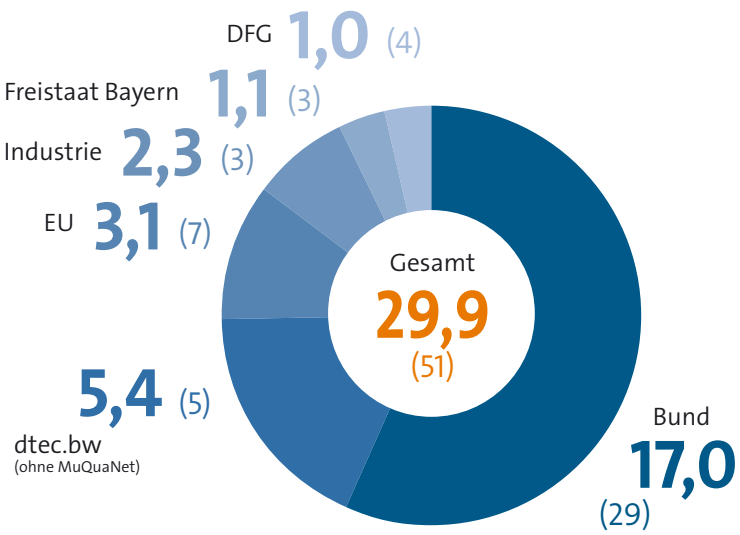

der Bundeswehr
Universität München
CODE
JAHRESBERICHT
2023
FI
CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Projektförderung

2023 wurden insgesamt 51 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

Hon.-Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Florian Alt
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 2023 aus 16 Ländern.

Kooperationspartner***

Im Jahr 2023 arbeitete das FI CODE mit 130 Partnern in 35 Ländern zusammen.

Legende

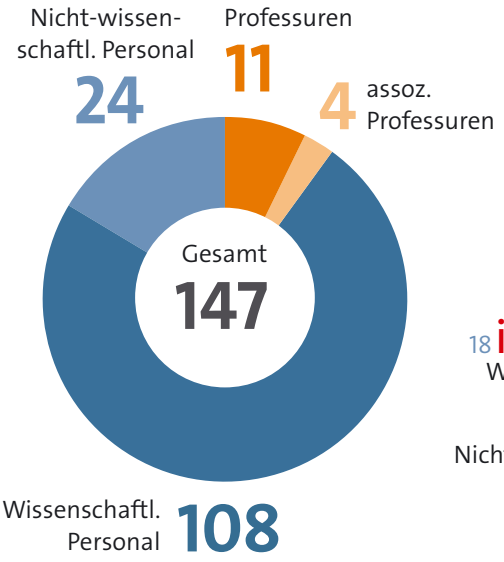
- Standort FI CODE
- 1 — Anzahl von CODE-Mitarbeitenden aus den Herkunftsländern
- 1 — Anzahl internationaler Kooperationspartner im betreffenden Land
- Länder mit Kooperationspartnern und Mitarbeitenden

*** Weitere Informationen zu Kontakten und Kooperationspartnern finden Sie ab S. 96.

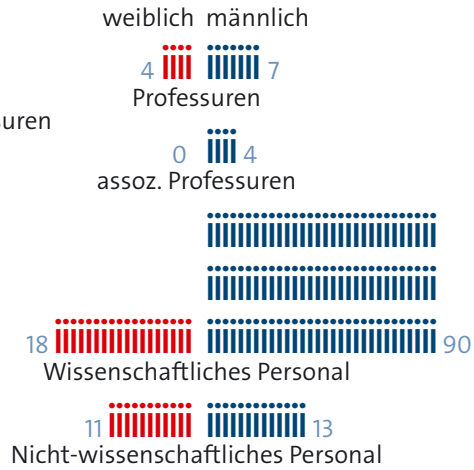
Personalstruktur

Das FI CODE hatte 2023 insgesamt 147 Mitarbeitende. Der Frauenanteil betrug 22 %.

Mitarbeitende



Geschlechteranteil



22 % **78 %**

Forschungsarbeit

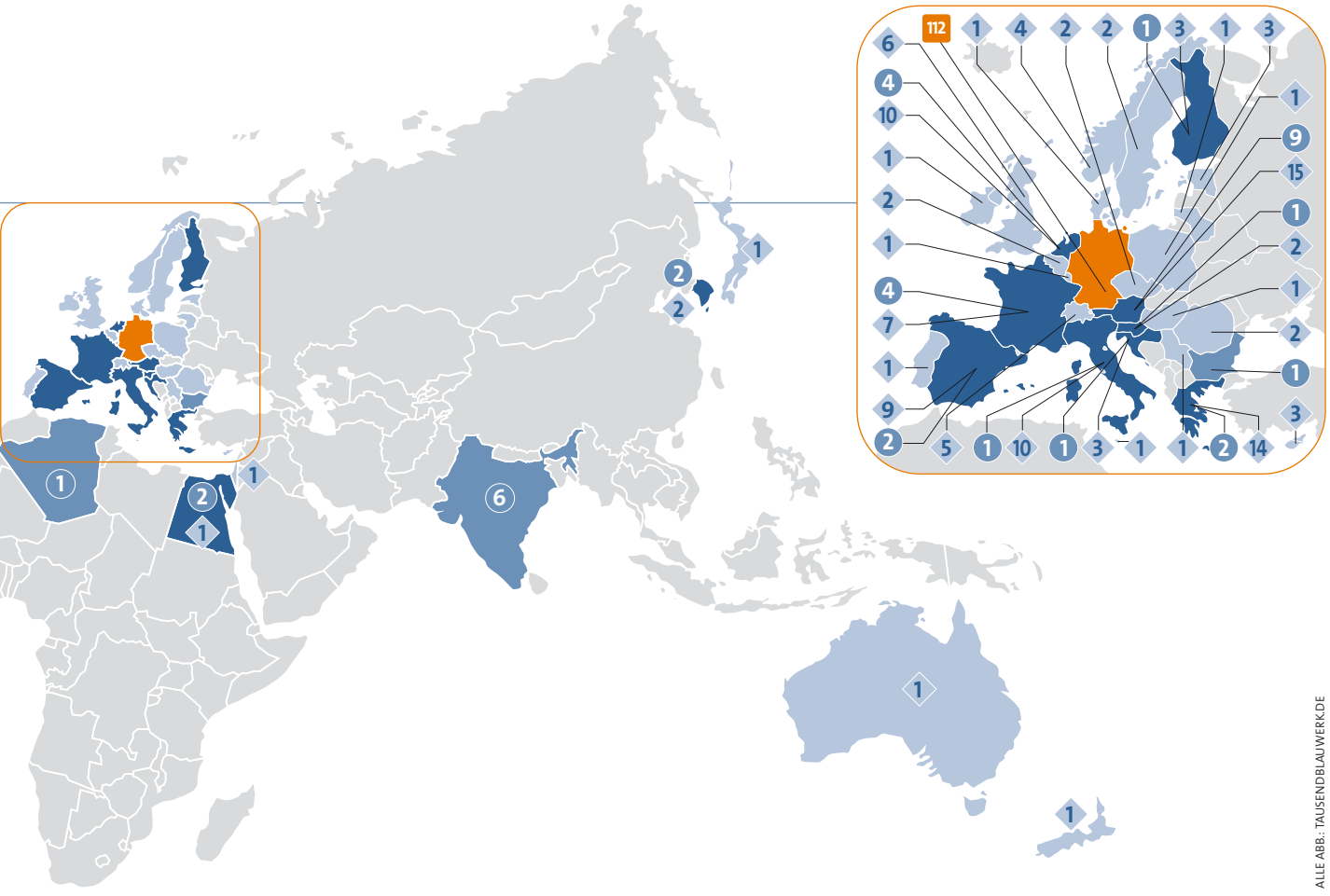
Übersicht der Promotionen und Publikationen am FI CODE 2023

Promotionen

6

Publikationen

107



ALLE ABB.: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
JAHRESBERICHT
2023

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Vorwort der Präsidentin

Das Jahr 2023 stand ganz im Zeichen des historischen Jubiläums „50 Jahre Universität der Bundeswehr München“, welches wir ausgiebig in zahlreichen Veranstaltungen gefeiert haben. Dazu passte hervorragend das zehnjährige Bestehen von CODE.

Seit der Gründung im Jahr 2013 ist es das Ziel von CODE, technische Innovationen und Konzepte zum Schutz von Daten, Software und Systemen in einem interdisziplinären Ansatz sowohl grundlagenorientiert als auch anwendungsnah zu erforschen und zu entwickeln. Dafür bündelt CODE seit nunmehr zehn Jahren wissenschaftliche Kompetenzen aus unterschiedlichsten Bereichen und arbeitet eng mit Partnern aus Bundeswehr, Behörden, Forschung und Wirtschaft zusammen. Damit passt CODE bestens zum Profil der Universität der Bundeswehr München „Sicherheit und Nachhaltigkeit in Technik und Gesellschaft“. Angesichts der großen Herausforderungen durch die Zeitenwende ist es mir ein zentrales Anliegen, unsere Universität noch mehr als strategische Ressource für das Bundesministerium der Verteidigung und die Bundeswehr zu etablieren.

Bereits seit 2021 ist das Forschungsinstitut CODE (FI CODE) ein verlässlicher Partner im nationalen Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS). Das NKCS ist eine gemeinsame Kooperationsplattform von BMWK, BMI, BMVg und BMBF sowie einzelner nachgeordneter Bereiche (BSI und FI CODE und DLR-PT). 2023 war für das FI CODE ein wichtiges Jahr bei der Weichenstellung für die weitere Entwicklung im NKCS. Im Rahmen einer Ausschreibung des Digital Europe Programme (DIGITAL) der Europäischen Kommission hat ein Konsortium bestehend aus BSI, dem Projektträger beim Deutschen Zentrum für Luft- und Raumfahrt e.V. und dem FI CODE das Projekt „NCC-DE – Capacity Building for the German National Coordination Centre for Cybersecurity in Industry, Technology and Research“ eingeworben.

Auch beim Thema Quantencomputer nimmt das FI CODE eine Vorreiterrolle ein. Auf dem vom Munich Quantum Valley, der LMU München sowie dem FI CODE gemeinsam organisierten Symposium „Quantum Computing Meets Cyber Security” in Garching diskutierten Expertinnen und Experten aus verschiedenen Bereichen über Cybersicherheitsrisiken im Zeitalter der Quantencomputer.

Das FI CODE ist eine Erfolgsgeschichte, auf die wir an unserer Universität zu Recht stolz sein dürfen. Ich gratuliere allen, die in den vergangenen zehn Jahren zum Aufbau und den Errungenschaften des FI CODE beigetragen haben und wünsche auch für die Zukunft alles Gute und weiterhin viel Erfolg und gutes Gelingen! In diesem Sinne nun eine spannende Lektüre dieses besonderen Jubiläums-Jahresberichts!

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,

auch für uns stand 2023 nach außen ganz im Zeichen des Doppeljubiläums aus 50 Jahren Universität der Bundeswehr München und zehn Jahren CODE. Diesem Jubiläum war auch ein Teil unserer Jahrestagung gewidmet – samt Geburtstagstorte. Doch auch im Inneren hat sich am Forschungsinstitut CODE Vieles weiterentwickelt. Der vorliegende Jahresbericht gibt Ihnen in mittlerweile vertrauter Manier einen Einblick in ausgewählte Highlights, die spannende Arbeit unserer Forschungsgruppen und das breite Spektrum unserer Aktivitäten im zurückliegenden Jahr.

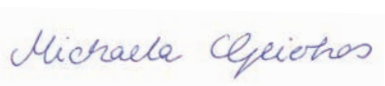
2023 konnten wir uns über weiteren Zuwachs und tatkräftige Unterstützung freuen. So stießen im Oktober Prof. Dr. Marta Gomez-Barrero und im November Prof. Dr. Daniel Slamanig zum FI CODE und übernahmen die Professuren für Maschinelles Lernen bzw. Kryptologie. Dank des Aufwuchses unserer bestehenden Forschungsgruppen stieg die Anzahl der CODE-Mitarbeitenden auf über 140 an. Erstmals wurden über 50 drittmittelfinanzierte Projekte parallel in unseren Forschungsgruppen bearbeitet. Eine Auswahl dieser Forschungsprojekte wird Ihnen im Hauptteil dieses Jahresberichts näher vorgestellt.

Erfolgreiche Forschung inkludiert auch den Transfer in die Praxis, den wir durch enge Vernetzung mit Expertinnen und Experten aus Bundeswehr, Behörden und Industrie stimulieren. Im Jahr 2023 führten wir mit ausgewählten Kooperationspartnern und handverlesenen Teilnehmenden, zahlreiche inhaltlich gewinnbringende und die Zusammenarbeit fördernde Veranstaltungen durch. Die Veranstaltungsthemen erstreckten sich dabei von der Schnittstelle zwischen Quantencomputern und Cybersicherheit bis zum Themenkomplex Open Source Intelligence. Eine kurze Zusammenfassung zu den Veranstaltungen finden Sie ebenfalls im vorliegenden Bericht.

Als universitäre Einrichtung freuen wir uns insbesondere über den zunehmenden Stellenwert, der einer kontinuierlichen, fachlichen und persönlichen Weiterbildung zukommt. Mit dem Ausbau unserer Cyber Range und den dort durchgeführten Hands-on-Trainings für die Bundeswehr und Landeskriminalämter, der Übernahme der Federführung bei der Weiterentwicklung des international populären E-Learning-Werkzeugs CrypTool durch die Forschungsgruppe von Prof. Dr. Arno Wacker und die Teilnahme von rund 60 Teams an unserem „Capture the Flag“ Event leistet CODE einen fachlich fokussierten und qualitativ hochwertigen Beitrag zur Thematik des lebenslangen Lernens.

Bei der Lektüre unseres Jahresberichts 2023 wünschen wir Ihnen interessante Einblicke und neue Erkenntnisse und freuen uns auf die weitere Zusammenarbeit!

Prof. Dr. Wolfgang Hommel



Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Leitung des Forschungsinstituts CODE

ABB.: UNIBW M; A. WAGENER FOTOGRAFIE

Inhalt

ABB.: ADOBE STOCK / KILLYKOON

Highlights
Aus dem Institut

Forschung
Porträts und Projekte

Weitere 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 Technologieentwicklung**
- **Wissenstransfer sowie Beratung von Entscheidungsträgern**
- **Aus- und Weiterbildung**

Wir betreiben sowohl Grundlagen- als auch anwendungsnahe Forschung und Technologieentwicklung 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 dem Organisationsbereich 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 / AU

Highlights

Aus dem Institut

Happy birthday, CODE!

Meilensteine unserer Entwicklung in den ersten zehn Jahren

Der erste runde Geburtstag von CODE ist auch Anlass für einen Rückblick auf die zurückliegenden zehn Jahre. Dieser Beitrag fasst die Entstehungsgeschichte von CODE als zunächst universitätsinternem Forschungszentrum, den Aufwuchs zum ressorteigenen Forschungsinstitut und weitere Meilensteine auf dem Weg zum aktuellen Leistungsspektrum zusammen. Besonderer Dank gilt dabei unseren Wegbereitern aus Universität und Bundeswehr sowie langjährigen Kooperationspartnern.

SEIT DER PRÄSIDENTSCHAFT (2005 – 2022) von Prof. Dr. Merith Niehuss prägt das Leitmotiv „Sicherheit und Nachhaltigkeit in Technik und Gesellschaft" die Forschung an der Universität der Bundeswehr München (UniBw M). Das Ziel der wissenschaftlichen Profilbildung mit gesellschaftlicher Verantwortung wird dabei maßgeblich auch durch die universitätsinternen Forschungszentren erreicht. CODE wurde 2013 nach Zustimmung des Senats und der Hochschulleitung als viertes Forschungszentrum auf Initiative von Prof. Dr. Gabi Dreo Rodosek, der Sprecherin des Forschungszentrums CODE (FZ CODE) und die erste Leitende Direktorin des späteren FI CODE, sowie des damaligen Dekans der Fakultät für Informatik, Prof. Dr.-Ing. Mark Minas, gegründet.

10 Jahre CODE

Anfangsjahre und Aufwuchs zum Forschungsinstitut

Unter der Prämisse angetreten, Forschung rund um Cyber Defence sowohl hochschulintern als auch mit externen Kooperationspartnern zu bündeln und in die Anwendung zu bringen, fand im September 2013 die Auftaktveranstaltung des noch jungen FZ CODE statt. Aus dieser entwickelte sich in den Folgejahren die Audimax-füllende CODE-Jahrestagung, in welche seit 2018 auch die Innovationstagung Cyber/IT des Bundesministeriums der Verteidigung (BMVg) integriert ist. Zu den bereits damals zahlreichen prominenten Vortragenden zählte auch Dr. Thomas Daum, Informatik-Alumnus der UniBw M und inzwischen Inspekteur Cyber- und Informationsraum (CIR).

Auftaktveranstaltung des FZ CODE im September 2013.

ABB.: FI CODE / A. WAGENER; FI CODE

Eröffnung des Cyber-Clusters UniBw M bei der CODE-Jahrestagung 2017 durch Bundesverteidigungsministerin Dr. Ursula von der Leyen.

Mit Cyber Defence als strategischem Forschungs- und Handlungsfeld der Universität widmete die Fakultät für Informatik der IT-Sicherheit von Software und Daten 2014 eine erste neue dedizierte Professur, auf die 2016 Prof. Dr. Wolfgang Hommel berufen wurde. Im Rahmen der parallelen Vorbereitungen zur Aufstellung des CIR als eigenständigem militärischem Organisationsbereich der Bundeswehr wurde unter BMVg-seitiger Federführung von Armin Fleischmann und Bernd Schlömer der Ausbau von CODE zur ressorteigenen Forschungseinrichtung geplant. Unter Prof. Klaus Buchenrieder, Ph.D., damals Dekan der Fakultät für Informatik sowie in der Folgezeit erster Technischer Direktor des FI CODE sowie der damaligen Senatsvorsitzenden, Prof. Dr.-Ing. habil. Dr. mont. Eva-Maria Kern, MBA, erhielt CODE eine Satzung als Forschungsinstitut mit personeller und materieller Grundausstattung. Der Aufwuchs von CODE zum Forschungsinstitut ging einher mit der Einführung des Masterstudiengangs Cyber-Sicherheit. Das entstandene bundesweit einzigartige Cyber-Cluster UniBw M wurde im Rahmen der CODE-Jahrestagung 2017 feierlich von der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, eröffnet.

Enge Kooperation mit ZITiS

Mit dem FI CODE wurde neben elf neuen W3-Professuren auch eine Geschäftsstelle eingerichtet, deren Leitung Volker Eiseler übernahm. Um den zusätzlichen Bedarf an Büro- und Laborflächen für die neuen Forschungsgruppen zu decken, wurde 2016 mit der Planung eines Neubaus auf dem Campus der Universität begonnen. 2017 erfolgte der Umzug in angemietete Flächen im „Cascada“, einem Bürohaus im campusnahen Münchner Süden. Hier konnte auch der Aufstellungsstab der ebenfalls 2017 errichteten Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) untergebracht werden. Die von Anfang an enge

Seit 2017 Heimat des FI CODE: Das „Cascada“-Bürogebäude im Südosten von München.

Vizeadmiral Dr. Thomas Daum, Inspekteur CIR, (4. v. l.) besucht die Cyber Range des FI CODE 2021.

Zusammenarbeit zwischen FI CODE und ZITiS zeigte sich dabei nicht nur darin, dass der geplante Neubau auf dem Universitätscampus gemeinsam genutzt werden sollte, und der Forschung, sondern auch in der Lehre. So ist der Masterstudiengang Cyber-Sicherheit einer der ersten Studiengänge an der UniBw M mit einer dedizierten Kapazität für zivile Studierende. Diese wurden zu einem erheblichen Teil von der ZITiS entsandt. Für diese Studierenden wurde 2020 daher eine spezialisierende Vertiefungsrichtung mit maßgeschneidertem Absolventenprofil eingeführt.

Transfer von Forschungsergebnissen in die Praxis

Auch vor dem Hintergrund des Personalbedarfs in Kommando, Organisationsbereich und Dimension CIR wird die Weiterentwicklung von Forschung und Lehre im FI CODE eng verfolgt und begleitet. Zu regelmäßigen Gästen des Forschungsinstituts gehörten und gehören unter anderem Ludwig Leinhos, erster Inspekteur CIR, Jürgen Setzer, Stellvertreter Inspekteur CIR, und Michael Vetter, Abteilungsleiter BMVg CIT I. Zur Sicherstellung einer vorausschauenden Forschungsausrichtung und organisatorischen Weiterentwicklung wurde ein Beirat ins Leben gerufen, dem neben Wolfgang Sachs, Referatsleiter CIT I 2, auch Vertreter aus Industrie und Wissenschaft angehören. Für den engen Austausch und die Stimulation des Transfers von Forschungsergebnissen in die Praxis der Truppe wurde auf Initiative von Armin Fleischmann ein Verbindungselement eingerichtet; die Verbindungsoffiziere haben dabei explizit auch die Möglichkeit, sich direkt an Forschungsprojekten zu beteiligen und somit wissenschaftlich weiterzuqualifizieren.

Weiteres Wachstum und neue Forschungsfelder

Bereits mit dem Aufwuchs vom Forschungszentrum zum Forschungsinstitut wurden die Themen Künstliche Intelligenz und Anwendungen des Maschinellen Lernens – zusammengefasst unter dem Oberbegriff „Smart Data“ – zum zweiten großen CODE-Forschungsfeld. Mit Prof. Dr. Michaela Geierhos wurde 2020 die erste in diesem neuen CODE-Geschäftsbereich angesiedelte Professur, Data Science, besetzt. Im selben Jahr erreichte CODE erstmals die Marke von 100 Mitarbeitenden und Prof. Dr. Udo Helmbrecht, vormals Präsident des BSI und der ENISA, trat die Nachfolge von Prof. Klaus Buchenrieder, Ph.D., als Technischer Direktor an. Er bereitete zusammen mit Prof. Dr. Gabi Dreo Rodosek den Aufbau des dritten Geschäftsbereichs, Quantum Technology, vor. Dieser umfasst neben Quantencomputing auch die Absicherung von Kommunikation durch Quantum Key Distribution und Post-Quantum-Kryptographie. Nach dem Eintritt in

ABB.: FI CODE (2); UNIBW M / SIEBOLD

Besuch des Generalinspekteurs General Eberhard Zorn (3. v. l.) 2022.

den Ruhestand Anfang 2021 folgte Prof. Dr. Wolfgang Hommel als Technischer Direktor nach. Mitten in der Corona-Pandemie – auch die CODE-Jahrestagungen fanden 2020 und 2021 nur virtuell statt – begann der Aufbau des neuen Geschäftsbereichs Quantum Technology unter Leitung von Dr. Sabine Tornow. Ebenso wurde der Grundstein für die Beteiligung des FI CODE am Nationalen Koordinierungszentrum für Cybersicherheit (NKCS) gelegt, die mittlerweile von Priv.-Doz. Dr. Corinna Schmitt verantwortet wird.

Personelle Wechsel und Weiterentwicklungen

Ende 2021 folgten größere personelle und organisatorische Veränderungen. Prof. Dr. Wolfgang Hommel wurde der Leitende Direktor, Prof. Dr. Michaela Geierhos die Technische Direktorin. Marcus Knüpfer folgte als Geschäftsführer Volker Eiseler, der seinerseits in Nachfolge von Bernd Schlömer als Referent ins BMVg CIT I 2 wechselte. Mit der Einrichtung eines CODE-internen Lenkungskreises wurde dem anhaltenden Wachstum des Forschungsinstituts – 2022 waren bereits 15 Forschungsgruppen beteiligt – Rechnung getragen. Neben einem deutlich verbreiterten Forschungsspektrum und der Weiterentwicklung des Masterstudiengangs Cyber-Sicherheit wurden die Jahre 2022 und 2023 durch die Öffnung vormals interner Leistungen für die Bundeswehr und Kooperationspartner geprägt. So werden die Cyber Range des FI CODE mittlerweile von Bundeswehr, Cyber-Reserve und Landeskriminalämtern genutzt und interessierte Dienststellen der Bundeswehr werden gezielt bei der bei der Analyse des Anwendungspotenzials von und dem Experimentieren mit Quantencomputern unterstützt.

Die Erfolgsgeschichte geht weiter

Zum Ende des Jubiläumsjahres 2023 ist CODE auf über 140 Mitarbeitende und über 50 parallel bearbeitete, drittmittelfinanzierte Projekte angewachsen, als ressorteigenes Forschungsinstitut fest etabliert und mit zahlreichen Partnern im In- und Ausland eng vernetzt. Wir danken allen Unterstützern und freuen uns auf die gemeinsame Zukunft! ■

Mehr Informationen zum FI CODE

https://www.unibw.de/code

code@unibw.de

ABB.: UNIBW M / SIEBOLD

Überblick

Leitung des Forschungsinstituts CODE	
Leitende Direktoren	
Prof. Dr. Wolfgang Hommel	seit 2021
Prof. Dr. Gabi Dreo Rodosek	2017-2021
Technische Direktoren	
Prof. Dr. Michaela Geierhos	seit 2021
Prof. Dr. Wolfgang Hommel	2021
Hon.-Prof. Dr. Udo Helmbrecht	2020-2021
Prof. Klaus Buchenrieder, Ph.D.	2017-2020
Geschäftsführer	
Marcus Knüpfer	seit 2022
Volker Eiseler	2017-2021

Beiratsmitglieder des FI CODE 2023	
Prof. Klaus Buchenrieder, Ph.D.	UniBw M
Dr. Norbert Gaus	Siemens
Prof. Dr. Ulrike Lechner	UniBw M
Prof. Dr.-Ing. Helmut Mayer	UniBw M
Prof. Dr. Johann Pongratz	TU Dortmund
Prof. Dr. Oliver Rose	UniBw M
Wolfgang Sachs	BMVg CIT I 2
Prof. Dr. Gunnar Teege	UniBw M
Dr. Ralf Wintergerst	BITKOM

Masterstudiengang Cyber-Sicherheit (MCYB)	
Vorsitzende des Prüfungsausschusses	
Prof. Dr. Harald Baier	seit 2022
Prof. Dr.-Ing. Mark Minas	2021
Prof. Dr. Stefan Brunthaler	2018-2021
Studiengangskoordination	
Michael Sattelmayer	seit 2020
Stefanie Molnar	2018-2020

Mitglieder der Studiengangkommission MCYB

Prof. Dr. Harald Baier, Prof. Dr. Michaela Geierhos, Prof. Dr. Peter Hertling (Studiendekan), Prof. Dr. Wolfgang Hommel, Prof. Dr.-Ing. Mark Manulis, Stefanie Molnar, Prof. Dr. Eirini Ntoutsi, Michael Sattelmayer, Prof. Dr. Gunnar Teege sowie Vertreter der wiss. Mitarbeitenden und der Studierenden

Professuren und Forschungsgruppen am FI CODE	
Prof. Dr. Florian Alt *Usable Security and Privacy*	seit 05/2018
Prof. Dr. Harald Baier *Digitale Forensik*	seit 09/2020
Prof. Dr. Stefan Brunthaler *Sichere Softwareentwicklung*	seit 10/2017
Prof. Klaus Buchenrieder, Ph.D. *Eingebettete Systeme / Rechner in Technischen Systemen*	
Prof. Dr. Gabi Dreo Rodosek *Kommunikationssysteme und Netzsicherheit*	
Prof. Dr. Michaela Geierhos *Data Science*	seit 04/2020
Prof. Dr. Marta Gomez-Barrero *Maschinelles Lernen*	seit 10/2023
Hon.-Prof. Dr. Udo Helmbrecht *Quantenkommunikation*	
Prof. Dr. Wolfgang Hommel *IT-Sicherheit von Software und Daten*	
Prof. Dr. Ulrike Lechner *Wirtschaftsinformatik*	
Prof. Dr.-Ing. Mark Manulis *Privacy und angewandte Kryptographie*	seit 03/2022
Prof. Dr.-Ing. Helmut Mayer *Visual Computing*	
Prof. Dr. Maximilian Moll *Operations Research – Prescriptive Analytics*	
Prof. Dr. Eirini Ntoutsi *Open Source Intelligence*	seit 08/2022
Prof. Dr. Stefan Pickl *Operations Research*	
Priv.-Doz. Dr. Corinna Schmitt *Secure Communication Systems*	
Prof. Dr. Daniel Slamanig *Kryptologie*	seit 11/2023
Prof. Dr. Gunnar Teege *Verteilte Systeme*	
Prof. Dr. Arno Wacker *Datenschutz und Compliance*	seit 06/2018

Bericht zur CODE-Jahrestagung 2023

CODE feiert zehnjähriges Jubiläum

Zehn Jahre CODE – zehn Jahre Spitzenforschung im Bereich Cybersecurity, Smart Data und Quantum Technologies. Im Zeichen dieses Jubiläums stand die Jahrestagung des Forschungsinstituts CODE am 11. und 12. Juli 2023. Über 400 Teilnehmerinnen und Teilnehmer aus Militär, Industrie, Wissenschaft und Behörden trafen sich auf dem Campus der Universität der Bundeswehr in Neubiberg.

DEN AUFTAKT DES ersten Veranstaltungstages machte die Präsidentin der Universität der Bundeswehr München, Prof. Dr. Eva-Maria Kern mit ihrer Begrüßungsrede sowie Staatssekretärin Siemtje Möller, die ihre Grüße via Videobotschaft aus dem Bundesministerium der Verteidigung (BMVg) sendete. Gemäß dem Tagungsmotto „10 Jahre CODE“ ließ der Leitende Direktor des FI CODE, Prof. Dr. Wolfgang Hommel, in seinem Beitrag die letzte Dekade Revue passieren. Auf seiner unterhaltsamen Zeitreise durch die letzten zehn Jahre gab er dem Publikum nicht nur Einblicke in die Geschichte und Entwicklung von CODE, sondern erzählte auch die ein oder andere amüsante Anekdote aus dieser Zeit. Im Anschluss trat Vizeadmiral Dr. Thomas Daum ans Rednerpult. Der Inspekteur Cyber- und Informationsraum verwies unter anderem auf die Leistungsfähigkeit von Künstlicher Intelligenz. Dies zeigte er anhand eines eindrucksvollen Beispiels: Der Einstieg seiner Keynote war vollständig von ChatGPT verfasst, wie der Vizeadmiral im Laufe seiner Rede aufklärte.

Dass gerade Cybersicherheitsforschung nur zusammen gelingen kann, war Thema des Vortrags von Barbara Kluge aus dem Bundesministerium des Innern und für Heimat (BMI). Besonders hob sie die enge Zusammenarbeit vom BMI und dem FI CODE bei diesem Thema hervor. Zwischen den Redebeiträgen des Vormittags unterhielt „At Ease“, die Big Band der UniBw M, mit beschwingten Musikeinlagen das Publikum. Zum Besten gaben sie dabei Klassiker der Filmmusik, so zum Beispiel „Happy“ oder „Golden Eye“.

Vizeadmiral Dr. Thomas Daum, Inspekteur Cyber- und Informationsraum: „Technologie der Zukunft wird bei CODE zur Technologie der Gegenwart“.

V. l. n. r.: Marcus Knüpfer (Geschäftsführer FI CODE), Michael Dreher (IBM), Prof. Dr. Michaela Geierhos (Technische Direktorin FI CODE), David Faller (IBM), Prof. Dr. Wolfgang Hommel (Leitender Direktor FI CODE) und Prof. Dr. Geralt Siebert (Vizepräsident UniBw M).

ABB.: UNIBW M / SIEBOLD (2); FI CODE

Nach einer kurzen Kaffeepause wurde das Programm fortgesetzt mit Vorträgen von Staatssekretär Bernd Schlömer und ZITiS-Präsident Wilfried Karl. Schlömer sprach über die Perspektiven des Bundeslands Sachsen-Anhalt bei der Digitalisierung und Informationssicherheit in der ebenenübergreifenden Zusammenarbeit von Land und Kommunen. Auch Karl griff den Aspekt der Zusammenarbeit auf und nannte Kooperation und Wissen „das Fundament der Cybersicherheit". Kurz vor der Mittagspause folgte ein weiteres Highlight. IBM und die UniBw M verlängerten ihre Partnerschaft im Bereich Quantencomputing um weitere fünf Jahre. In einer feierlichen Zeremonie fand die Vertragsunterzeichnung durch Vertreterinnen und Vertreter beider Seiten statt. Als Quantum Innovation Center eröffnen sich insbesondere für das FI CODE damit auch weiterhin Möglichkeiten der Forschung und Lehre in diesem zukunftsträchtigen Bereich.

Staatsminister Dr. Herrmann lobt Arbeit des FI CODE

Nach der Mittagspause folgten weitere Vorträge, unter anderem von Prof. Dr. Harald Baier und Prof. Dr. Eirini Ntoutsi, die in ihren Beiträgen zu Digitaler Forensik bzw. Responsible AI Einblicke in die aktuelle Forschung am FI CODE gaben. Im letzten Veranstaltungsblock des Nachmittags stand das Thema „Software-defined Defence" im Fokus. In seinem einleitenden Vortrag ging Michael Kiefer von Dassault Systems Deutschland noch einmal auf die Bedeutung und Aktualität des Themas ein. Im Anschluss diskutierte Jens Ohlig vom Tagesspiegel Background zusammen mit Vertreterinnen und Vertretern aus Militär, Industrie und Interessensverbänden über das Thema im Rahmen einer Paneldiskussion. Zum Abschluss des ersten Veranstaltungstages fand im UniCasino das Social Event statt, in dessen Rahmen der Bayerische Staatsminister für Bundesangelegenheiten und Medien, Dr. Florian Herrmann, eine Dinner Speech hielt. „Das Forschungsinstitut CODE ist ein Aushängeschild der Bundeswehr in Bayern. Seit 2013 ist CODE das perfekte Beispiel, wie gute, vernetzte Zusammenarbeit im Bereich Cyber-Security funktioniert", lobte der Staatsminister. Er betonte: „Verteidigung ist immer eine Teamaufgabe. Wir setzen auch weiterhin auf die enge Zusammenarbeit mit CODE, die mit ihrer exzellenten Forschungsarbeit entscheidend zur Sicherheit im digitalen Raum beitragen."

Tag Zwei der CODE-Jahrestagung begann nach der Begrüßung durch die Technische Direktorin des FI

Vor dem Hintergrund der zunehmenden Bedeutung von Cybersicherheitsfragen lobte Staatsminister Dr. Florian Herrmann in seiner Dinner Speech insbesondere die Arbeit des FI CODE.

ABB.: UNIBW M / PLANK; FI CODE / B. BELLGRAU

Sieger der Innovationstagung Cyber/IT wurde Dr. Michael Kissner (m.). Brigadegeneral Armin Fleischmann (l.) und Prof. Dr. Wolfgang Hommel (r.) gratulierten zum Erfolg.

CODE, Prof. Dr. Michaela Geierhos, mit zwei Keynotes. Brigadegeneral Armin Fleischmann, Unterabteilungsleiter Cyber-/Informationstechnik I des BMVg, griff das Thema Software-defined Defense noch einmal auf und verdeutlichte, welche Vorteile aber auch welche Herausforderungen eine größere Fokussierung auf die Software bei der Fähigkeitsentwicklung mit sich bringt. In einer zweiten Keynote unterstrich Prof. Dr. Achim Walter von der Universität Kiel die Wichtigkeit von Aufmerksamkeit und aktiven Rahmenbedingungen, um Innovation bestmöglich zu fördern und „zum Leben zu erwecken". Der inspirierende Vortrag war thematisch ein passender Vorgriff auf den Nachmittag. Der weitere Vormittag bot die Möglichkeit für tiefgreifenden Diskussionen und Vorträge: In den fünf parallel durchgeführten Workshops beschäftigten sich die Teilnehmenden unter anderem mit Cyber Range Trainings im Kontext Kritischer Infrastrukturen, den Herausforderungen und Chancen der Künstlichen Intelligenz oder mit Quantentechnologien.

Auf der in Zusammenarbeit mit dem BMVg ausgerichteten Innovationstagung Cyber- und Informationstechnik wurden am Nachmittag vorab eingereichte, innovative Ideen vorgestellt, die besonders im Geschäftsbereich des BMVg Verwendung finden könnten. Der mit 15.000 Euro dotierte erste Platz ging in diesem Jahr an Dr. Michael Kissner von der Akhetonics GmbH, der die Jury und das Publikum mit einem rein-photonischen, universellen Hochleistungsprozessor für homomorph verschlüsselte Daten überzeugen konnte. Aber auch die anderen Beiträge an diesem Tag verdeutlichten, welche Anwendungsmöglichkeiten es für Innovationen in der Bundeswehr gibt. In den einleitenden Worten verdeutlichte Brigadegeneral Fleischmann: „Alle Vorträge am heutigen Tag sind bereits Gewinner."

Die Jahrestagung endete mit einer Zusammenfassung und einem Schlusswort von Prof. Dr. Michaela Geierhos. Sie dankte allen Teilnehmerinnen und Teilnehmern für ihren Besuch, insbesondere denjenigen, die in unterschiedlichster Form zur Jubiläumstagung beigetragen haben – sei es auf oder hinter der Bühne. ■

Mehr Informationen zur CODE-Jahrestagung

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

Bericht von der CRITIS 2023

Die neue Realität von Safety & Security

Die CRITIS 2023 war die 18. internationale Konferenz zur Sicherheit kritischer Infrastruktur und fand vom 13. bis 15. September 2023 an der Universität Laurea in der Metropolregion Helsinki in Finnland statt. Nach der erfolgreichen Kooperation 2022 in München, wurde die CRITIS auch 2023 wieder in wissenschaftlicher Zusammenarbeit mit CODE, mit Herrn Prof. Dr. Udo Helmbrecht als Ehrenvorsitzender und Prof. Dr. Stefan Pickl als Programm Co-Vorsitzender, organisiert.

ZIEL DER CRITIS 2023 WAR erneut, Forscher, Akademiker, Betreiber kritischer Informationsinfrastrukturen, Industrie sowie Regierungsorganisationen zusammenzubringen, die auf dem Gebiet der Sicherheit komplexer Infrastruktursysteme und insbesondere im Kontext von Operations Research zusammenarbeiten. Vor diesem Hintergrund befasste sich die CRITIS 2023 in erster Linie, aber nicht ausschließlich, mit Forschungsthemen, die sich mit der komplexen Analyse im Kontext von Safety & Security sowie der Sicherheit von Informationsinfrastrukturen auf verschiedene Weise befassen. Gleichzeitig wurden Themen im Zusammenhang mit hybriden Bedrohungen vorangetrieben und die Sicherheit kritischer Infrastrukturen von verschiedenen Seiten optimiert.

Safety & Security und Operations Research

Darüber hinaus zielte CRITIS 2023 darauf ab, junge und engagierte Forscher in diesem anspruchsvollen multidisziplinären Forschungsbereich der Sicherheit zu fördern und zu inspirieren, insbesondere in Verbindung mit Operational Analysis und Systemanalyse.

Die CRITIS 2023-Konferenz setzte die Tradition fort, innovative Forschung auf dem Gebiet des Schutzes kritischer Informationsinfrastrukturen (C(I)IP) vorzustellen, Ideen zu repräsentieren, die sich mit den Herausforderungen der Resilienz und der gesellschaftlichen Sicherheit befassen, und den Dialog mit den Beteiligten zu fördern. Eröffnet wurde die Konferenz von der Generalvorsitzenden und Direktorin des LAURA-Sicherheitsforschungsprogramms, Päivi Mattila.

Die neue Realität der Sicherheit

Prof. Dr. Bernhard M. Hämmerli, ehemaliger Präsident der Information Security Society Schweiz ISSS, begrüßte die Kolleginnen und Kollegen und richtete einen besonderen Dank des Lenkungsausschusses an die Organisatoren. Er bedankte sich auch dafür, dass Prof. Dr. Udo Helmbrecht von CODE erneut als Honorary Chair von CRITIS 2023 fungierte. Er bedankte sich auch bei CODE für die hervorragende wissenschaftliche internationale Zusammenarbeit.

Prof. Dr. Stefan Pickl mit der lokalen Organisatorin Päivi Mattila und dem Plenarspeaker Prof. Dr. Kenji Watanabe (v. l. n. r.)

ABB.: ADOBE STOCK/ V. GALKINA ; FI CODE / S. PICKL

Plenarvortrag über Cyber-Physical Security in kritischen Infrastukturen

Anschließend eröffnete die FEI-Vizepräsidentin Mari Vuolteenaho offiziell die Konferenz und stellte den ersten Hauptredner, Prof. Dr. Jarno Limnéll vom finnischen Parlament, vor. Der Titel seines inspirierenden Vortrags lautete: „The new reality of security".

Auch Peter Sund, CEO des Finnish Information Security Cluster (FISC), Technology Industries of Finland, sprach über künftige Herausforderungen im Bereich der Sicherheit sowie über den analytischen Bedarf und die Relevanz geeigneter Modelle im Kontext von Safety&Security.

Nach der Kaffeepause hielt Kenji Watanabe (Nagoya Institute of Technology) den ersten Plenarvortrag zum Thema „Herausforderungen für die operative Umsetzung der cyber-physischen Sicherheit in kritischen Infrastrukturen".

Er betonte die Bedeutung geeigneter Modelle, algorithmischer Ansätze sowie effizienter datengesteuerter Optimierungstechniken und OR-basierter Ansätze im speziellen Kontext kritischer Infrastrukturen.

Die nächste Sitzung wurde durch den Beitrag „Towards an ecosystemic analysis for essential and important entities" von Nicolas Mayer eröffnet.

Intelligente Tools zur Entscheidungsfindung – Hybride Bedrohungen

Ein „Entscheidungsunterstützungssystem für die Überwachung und Risikoanalyse von nationalen kritischen Einrichtungen" wurde von Roberto Setola entwickelt und beschrieben. Die Ergebnisse des interessanten MEDEA-Projekts wurden von Genny Dimitrakopoulou in ihrem Vortrag „Hybride Cyber-Angriffe auf kritische Infrastrukturen" präsentiert.

Die andere parallele Sitzung befasste sich mit Risikomanagement und Risikoanalyse: Hiroshi Sasaki demonstrierte, wie er ein einfaches Instrument zur Risikobewertung für die Cybersicherheit von Fabrikanlagen entwickelt hat. José Martí analysierte einen Risikorahmen für den Klimawandel in Bezug auf ein komplexes, voneinander abhängiges kritisches System/komplexe, voneinander abhängige kritische Systeme. Roberto Setola präsentierte die Bewertung der Auswirkungen des Mangels an wichtigen Arbeitskräften auf die Wirtschaftssektoren während einer Pandemie. Die Rolle einer komplexen Spektrumanalyse wurde im Vortrag „Evasion attack against multivariate singular spectrum analysis-based IDS" von Vikas Maurya diskutiert.

Energiesicherheit und Vorhersage des Seeverkehrs – JRC

Nach der Kaffeepause stand die Energiesicherheit im Mittelpunkt der Konferenz: Der erste Plenarvortrag

Plenarvortrag von Generalmajor a.D. Dr. Dr. Dieter Budde

wurde von Vytis Kopustinskas (Joint Research Centre of Europe) zum Thema „Lessons learned from tabletop exercises“ gehalten: „Kohärente Resilienz der Energieversorgung in den baltischen Staaten“. Der zweite Plenarvortrag wurde von Jukka Heikkonen (Universität Turku) zum Thema „AI for anomaly detection with examples in maritime“ gehalten.

Beide Plenarsitzungen wurden in der anschließenden Mittagspause eingehend diskutiert. Nach der Mittagspause wurden die folgenden Beiträge in parallelen Sitzungen behandelt: „Surveillance of offshore installations with patrol routine“ von Bartosz Skobiej, „Vulnerability analysis of an electric vehicle charging ecosystem“ von Roland Plaka und „GNSS signal monitoring and security of supply of GNSS-based services“ wurde von Mika Saajasto vorgestellt. Optimierungsprobleme bei Vorhersageversuchen wurden von Farshad Farahnakian in seinem Vortrag „Kurz- und langfristige Vorhersage von Schiffsbewegungen für den Seeverkehr“ behandelt.

Netztopologie und kritische Energieinfrastruktur

„Mapping and analysis of common vulnerabilities in popular web servers“ war der Titel des Vortrags von Matyas Barocsai. In ihrem Vortrag „Adaptable smart distribution grid topology generation for enhanced resilience“ nutzte Natasa Gajic eine bestimmte Netztopologie zur Optimierung der Ausfallsicherheit.

Nach der Kaffeepause hielt Peter Burgherr vom Paul-Scherrer-Institut einen Plenarvortrag mit dem Titel „Hybride Bedrohungen und kritische Energieinfrastrukturen im Kontext der Energiewende“. Der folgende Plenarvortrag konzentrierte sich dann auf die ethische Dimension des Schutzes kritischer Infrastruktur: In seinem Vortrag „Ethik und die Bedrohung von Infrastrukturen“ charakterisierte Dr. Dr. Dieter Budde verschiedene ethische Dimensionen und differenzierte Ansätze.

Business Continuity Resilience und KI-basierte Antizipation

In diesem speziellen Kontext präsentierten Stefano Panzieri den Ansatz „Managing uncertainty using CISIApro 2.0 Model“ und Eveliina Hytönen „Business continuity building dynamic resilience“. Der andere Stream drehte sich um BCM-Modelle und OR-bezogene Lösungskonzepte: Eröffnet wurde der Stream durch den Vortrag „Relationships between security management and technical security“ von Øyvind Toftegaard. „Business Continuity Building Dynamic Resilience“ wurde von Eveliina Hytönen aus verschiedenen Perspektiven diskutiert. David Prette gab einen Überblick über die „Notfallresilienz aus der Sicht der Bürger“. Die letzte Sitzung wurde durch zwei sehr interessante Plenarvorträge eröffnet. Christian Després, Ministerium für ökologische Transformation, Frankreich, konzentrierte sich in seinem Vortrag „Anticipating future crises situations and adapting the means to respond to them“ auf Antizipationskonzepte. Er verwies dabei auf die besondere Zusammenarbeit und Forschungsaktivitäten zwischen der Forschungsgruppe COMTESSA und SANCTUM Labo Crise. Evaldas Bružė vom litauischen Cyber Crime Center of Excellence for Training, Research & Education betonte die stärkere Berücksichtigung von menschlichem Verhalten in Analysemodellen.

Strategische Entscheidungsunterstützung im Kontext des internationalen Forschungsverbundes SANCTUM+.

Zwei Industrievorträge stellten die Verbindung zwischen Cyber Security und Operational Analysis her: Mikaeli Langinvainio, CEO von Inclus Ltd., beleuchtete Künstliche Intelligenz und verbessertes Risikomanagement. Der letzte Vortrag befasste sich mit dem Cybersicherheitsindex und dem Bedarf an spezifischeren analytischen Konzepten in diesem Zusammenhang. Dieser Vortrag wurde von Pietari Sarjakivi, NIXU Corporation, gehalten: Sicherheit und Schutz könnten zu wichtigen Themen für OR-Analysten werden.

Nach diesen interessanten Vorträgen wurde die CRITIS 2023 mit einer Preisverleihung abgeschlossen. Die nächste CRITIS-Konferenz wird 2024 von Stefano Panzieri an der Universität Rom organisiert, erfreulicherweise wieder in enger Zusammenarbeit mit CODE. ■

Mehr Informationen zu CRITIS

https://www.laurea.fi/en/current-topics/events/critis-2023/

stefan.pickl@unibw.de

BEIDE ABB.: FI CODE / S. PICKL

Bei der „Cyber Phoenix“ übten Beteiligte aus drei Nationen u. a. die Abwehr von Cyberangriffen auf Einrichtungen der kritischen Infrastruktur.

ABB.: BUNDESWEHR / PIZ CIR

Bericht von der Reserveübung „Cyber Phoenix“ am FI CODE

Drei Nationen trainieren für den Ernstfall

Bei der zweiten Auflage der Übung „Cyber Phoenix“ trainierten Ende August Soldatinnen und Soldaten sowie Reservedienstleistende aus Deutschland, den Niederlanden und Australien gemeinsam auf der Cyber Range des FI CODE für den Ernstfall. Fünf Tage lang standen Einzel- und Gruppenübungen zur Abwehr von Cyberangriffen auf dem Programm.

NACH DER ERFOLGREICHEN Durchführung und den positiven Erfahrungen aus dem Vorjahr führte der Organisationsbereich Cyber- und Informationsraum (CIR) in der Woche vom 28. August bis 1. September zum zweiten Mal die Reserveübung „Cyber Phoenix“ durch. Neben Reservistinnen und Reservisten aus Deutschland und den Niederlanden, nahmen erstmals auch australische Soldatinnen und Soldaten an der Übung teil. Schauplatz des Geschehens war erneut das „Camp CODE“ – genauer gesagt die moderne Cyber Range ICE & T am Forschungsinstitut CODE.

Nach mehrmonatiger intensiver Vorbereitung begann für die 36 Teilnehmenden am Montagmorgen im Briefing Room die „Cyber Phoenix“. CODE-Geschäftsführer Marcus Knüpfer begrüßte die Soldatinnen und Soldaten der drei beteiligten Nationen und stellte das Trainerteam vor. Nach einer Einweisung in das Übungsszenario und die Räumlichkeiten bezogen die Übungsteilnehmenden dann ihre Arbeitsplätze in der Cyber Range, um sich zunächst mit der technischen Ausstattung und der Arbeitsumgebung vertraut zu machen.

In der virtualisierten Netzwerkumgebung der Cyber Range trainierten die multinationalen Teams während fünf Tagen in verschiedenen Szenarien die Abwehr von Cyberangriffen auf Einrichtungen der kritischen Infrastruktur. Im Mittelpunkt der Einzel- und Gruppenübungen standen dabei vor allem die Zusammenarbeit bei der Untersuchung und Analyse von Angriffsmustern sowie die schnelle Wiederherstellung der betroffenen Systeme und Dienste. Darüber hinaus sollten geeignete Präventivmaßnahmen ergriffen werden, um eine Wiederholung des Angriffs zu verhindern.

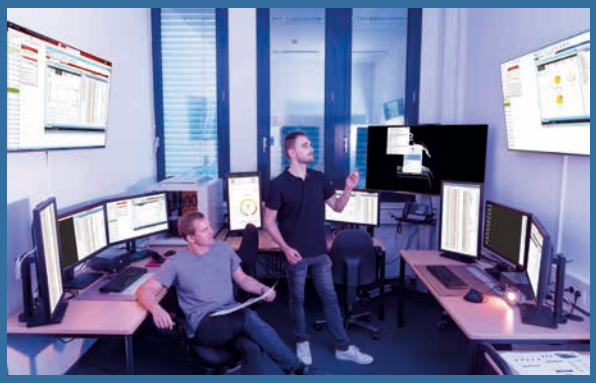
Beeindruckt zeigten sich auch die Vertreterinnen und Vertreter der beteiligten Nationen, die sich im Rahmen des „Distinguished Visitors Day“ über den Verlauf und die Fortschritte der Übung informierten. Sie lobten die hervorragende Zusammenarbeit der Soldatinnen und Soldaten und unterstrichen erneut die Bedeutung solcher Cyber-Übungen. Auch die Teilnehmenden zogen ein durchweg positives Fazit: Die monatelange intensive Vorbereitung hat sich einmal mehr gelohnt und dazu beigetragen, dass die Übung auch 2023 ein voller Erfolg wurde. ■

Mehr über Cyber Phoenix

https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/trinationale-vorbereitung-auf-den-digitalen-ernstfall-5681178

Die Kursräume von ICE & T sind für Training im Team konzipiert.

ICE & T Cyber Range am FI CODE



Trainer analysieren die Übungen und greifen unterstützend ein.

Die Cyber Range IT Competence Education & Training (ICE & T) am Forschungsinstitut CODE ist eine umfassende und flexible Lösung für praxisnahe Cybersicherheitstrainings. Sie bietet eine Plattform zum Erlernen und Vertiefen von Kompetenzen im Bereich Cyber Network Operations und legt einen starken Fokus auf Teamwork. Darüber hinaus ermöglicht ICE & T die Evaluierung neuer Cybersicherheitsprodukte und -verfahren.

Während der Trainings werden Cybersicherheitsszenarien in einer virtualisierten Umgebung bearbeitet. Die derzeit bei ICE & T verfügbaren Szenarien sind in die Kategorien Cyber Incident & Response Management (CIRM) Level 0–2, Supervisory Control and Data Acquisition (SCADA) und Penetration Testing (PT) unterteilt. Die Teilnehmenden lernen, verschiedene Angriffsmuster zu analysieren und abzuwehren oder PT-Methoden in realen Systemverbünden anzuwenden.

ICE & T ist auf einem Server-Cluster unter Verwendung des VMware ESXi Hypervisors vollständig virtualisiert. Mehr als 400 virtuelle Maschinen werden eingesetzt, um mehrstufige Szenarien sowie über 80 individuelle Übungen und Backoffice-Dienste zu

abzubilden. Die modulare Architektur ermöglicht außerdem die Integration physischer Hardwarekomponenten wie IoT und SCADA-Geräte.

Weitere Informationen

ICE T
IT Competence
Education & Training

code@unibw.de

Informationsflyer „Cyber Range”: https://go.unibw.de/84

ALLE ABB.: UNIBW M / SIEBOLD

Quantentechnologien

Auf dem Weg zur Fehlertoleranz

„Die jüngsten Fortschritte in der Quantentechnologie bringen uns einem tiefgreifenden Wandel in Wissenschaft und Technologie näher – einem Wandel, der weitreichende Auswirkungen auf unsere Wirtschaft, Sicherheit und Verteidigung haben wird. Diese Technologien könnten die Sensorik, die Bildgebung, die präzise Positionierung, Navigation und Zeitmessung, die Kommunikation, die Datenverarbeitung, die Modellierung, die Simulation und die Informationswissenschaft revolutionieren.“

NATO Summary of NATO's Quantum Technologies Strategy

Der IBM Quantum Heron Chip mit 133 Qubits.

DIE EXPERIMENTELLE KONTROLLE von Quantensystemen ermöglicht die Verarbeitung von Quanteninformationen, insbesondere durch Ausnutzung der Quanteneigenschaften der Superposition, Interferenz und Verschränkung.

Dabei bildet die Quanteninformationsverarbeitung das Rückgrat der Quantentechnologien: Quantendaten aus Quantensensoren können verarbeitet und in Quantenspeichern kurz zwischengesichert werden. Quantencomputer lassen sich über Quantennetze in verteilten Systemen zusammenschließen und mit klassischen Computern verbinden.

Die heutigen Quantencomputer sind jedoch in ihrer Leistungsfähigkeit noch eingeschränkt, da verschiedene Rauschquellen zu Fehlern führen.

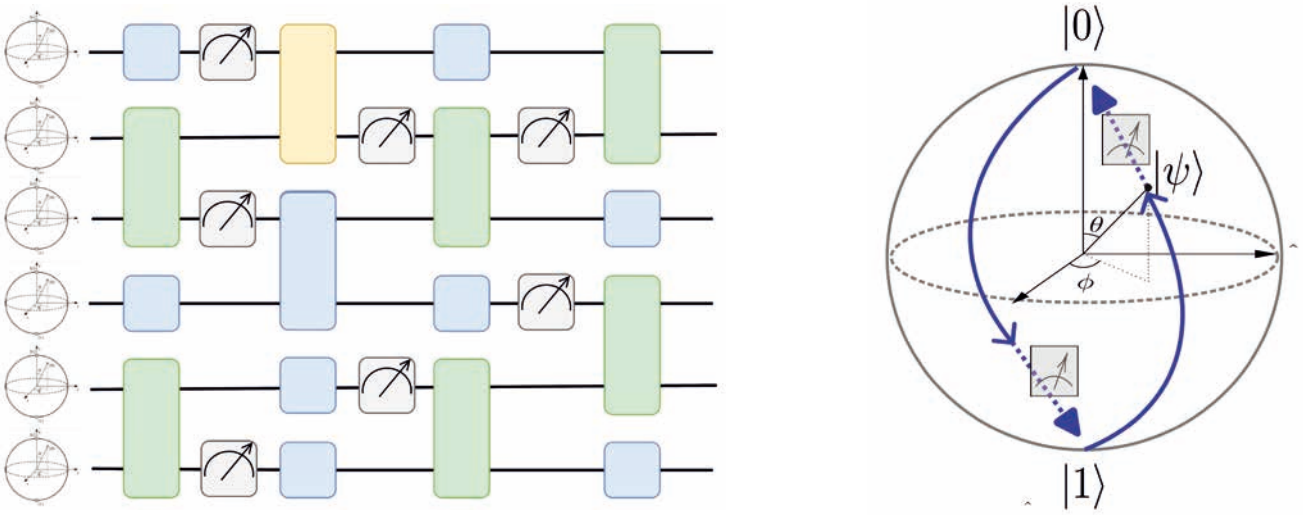
Im Allgemeinen ist das Ziel daher ein fehlertoleranter, universeller Quantencomputer, der eine Vielzahl von wichtigen Problemen lösen kann. Während wir auf dieses Ziel hinarbeiten, können wir auf dem Weg dorthin bereits nach nützlichen Anwendungen, neuen Algorithmen und Fehlerminderungstechniken suchen. Hierbei können wir, wenn wir die Fehler besser verstehen und beheben, damit beginnen, leistungsfähigere Quantenalgorithmen zu entwickeln. Dies erlaubt es uns mit jeder neuen Generation von Quantencomputern an relevanteren Anwendungen zu arbeiten.

Derzeitige Quantencomputer sind wertvoll für die wissenschaftliche Erforschung und Entwicklung, welche die vier grundlegenden Bereiche beinhaltet.

Erstens, die Ausnutzung des Quantencomputers als „Testbed“ für die Fragestellungen zur Quanteninformationsverarbeitung – beispielsweise der durch Zwischenmessung induzierte Phasenübergang der Verschränkungsdynamik oder die Verarbeitung von Quantendaten. Diese Kenntnisse können dann bei der Quantenalgorithmenentwicklung verwendet werden. Zweitens, die Untersuchung von Fehlerminderungstechniken und Fehlerkorrekturmethoden. Drittens, die Entwicklung neuer Algorithmen wie beispielsweise die Randomisierung mit Zwischenmessungen für Simulation, Optimierung und maschinelles Lernen. Viertens, die Identifizierung von möglichen Anwendungsfällen.

ABB.: IBM; MUNICH QUANTUM VALLEY / MIKKA STAMPA

Über Chancen und Risiken von Quantencomputern sprach Prof. Dr. Wolfgang Hommel im Mai 2023 vor den Teilnehmenden des Symposiums „Quantum Computing Meets Cyber Security” in Garching.



Quantenschaltkreise mit Zwischenmessungen: Der Schaltkreis besteht also aus einer deterministischen unitären Zeitentwicklung und einer stochastischen Messung, die zufällig auf einen Quantenzustand |0> oder |1> projiziert.

Anwendungsfälle für Fragestellungen in der Cybersicherheit wurden in einem von uns im Mai 2023 zusammen mit dem Munich Quantum Valley organisierten Workshop „Quantum Computing Meets Cyber Security" von Expertinnen und Experten aus den Bereichen Cybersecurity und Quantentechnologie thematisiert. Insbesondere wurden mögliche Cyberangriffe mithilfe von Geräten, die Quantentechnologien verwenden, diskutiert.

Darüber hinaus wurden Themen aus der angewandten Forschung mithilfe praxisorientierter Lehrveranstaltungen an Münchner Hochschulen, durch die Betreuung von Abschlussarbeiten und auf Workshops an Studierende und Mitarbeitende von bundeswehrnahen Dienstleistern weitergegeben sowie durch Vorträge auf Konferenzen und Seminaren vorgestellt. So konnten die Studierenden zum Beispiel Experimente zur Quantenteleportation selbst auf den Quantencomputern ausführen.

Experimente zu Fragestellungen der Quanteninformationsverarbeitung auf dem Quantencomputer

Für Quantenberechnungen ist es typischerweise erforderlich in einem Quantenschaltkreis Qubits zu initialisieren, kontrollierte Qubit-Wechselwirkungen durchzuführen (eine unitäre Zeitentwicklung mithilfe von Gattern) und die daraus resultierenden Quantenzustände zu messen. Es ist aber auch möglich, Quantenschaltkreise mit periodischen oder zufälligen Messungen von Qubits in der Schaltkreismitte auszuführen und zeitgleich die daraus resultierenden klassischen Informationen zu verarbeiten. In dem zuletzt genannten Fall besteht der Schaltkreis also aus einer deterministischen unitäre Zeitentwicklung und der stochastischen Messung, die zufällig auf einen Quantenzustand projiziert.

So können neue Algorithmen entwickelt werden oder Quanten-Vielteilchensysteme untersucht werden. Schaltkreise mit unitärer Zeitentwicklung mit Zwischenmessungen weisen eine Vielzahl dynamischer Phasen auf, die bei einer rein unitären Zeitentwicklung mit Messung am Ende nicht auftreten. Es kann so ein messinduzierter Verschränkungs-Phasenübergang realisiert werden.

Quantenfehlerminderungstechniken

Die derzeitige Quantenhardware unterliegt verschiedenen Rauschquellen, von denen die bekanntesten die Dekohärenz der Qubits, individuelle Gatterfehler und Messfehler sind. Diese Fehler begrenzen die Tiefe der Quantenschaltungen, die wir implementieren können. Doch selbst bei kurzen Schaltkreisen kann Rauschen zu fehlerhaften gemessenen Erwartungswerten führen. Glücklicherweise bietet die Quantenfehlerminderung eine Reihe von Werkzeugen und Methoden, die es uns ermöglichen, genauere Erwartungswerte aus verrauschten Quantenschaltungen mit geringer Tiefe zu ermitteln. Die Fehlerminderungstechniken müssen auf der Hardware getestet werden, um die beim Ausführen von Quantenalgorithmen auftretenden Hardwarefehler zu reduzieren. Bestimmte Algorithmen wie die „Probabilisitic Error Cancelation" funktionieren beispielsweise ähnlich wie die Rauschunterdrückung in Kopfhörern.

Mit klassischer Nachbearbeitung und kontrollierten Approximationen kann dann die Ausgabe des ursprünglichen Schaltkreises rekonstruiert werden. Mit diesem quantenklassischen Ansatz können kleine Quantencomputer einen Algorithmus ausführen, der mehr Qubits benötigt als verfügbar sind, und es können Laufzeit und Genauigkeit optimiert werden, bis es möglich ist, eine Quantenfehlerkorrektur anzuwenden.

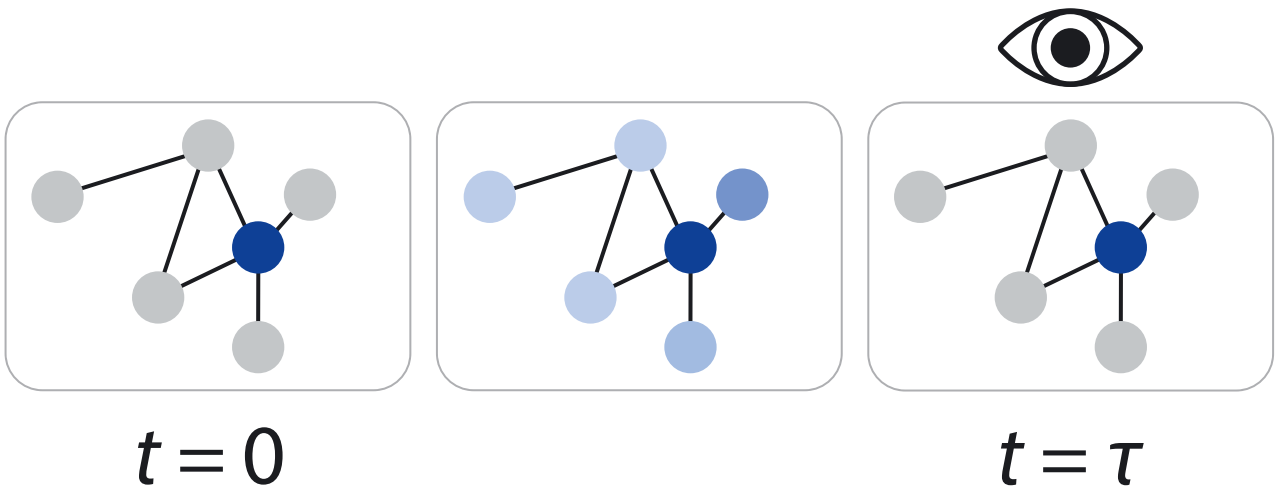
Die Skalierung der Anzahl der Qubits eines Quantencomputers ist ein aktuell noch zu überwindendes Problem. Eine Zwischenlösung ist ein skalierbarer hybrider Berechnungsansatz, der klassische Computer und verschiedene Quantencomputer durch „Distributed Quantum Computing“ kombiniert. Quantenschaltkreise werden in kleinere Einheiten zerlegt, sodass sie auf kleineren Quantenchips ausgeführt werden können.

Algorithmen und Anwendungen

Eine wichtige Technik zur Entwicklung von Quantenalgorithmen sind die sogenannten „Quantum Walks”. Sie haben sich in den letzten zehn Jahren zu einem universellen Berechnungsmodell entwickelt und wurden ursprünglich als Quantenversion klassischer „Random Walks” entwickelt, bei denen die Richtung des nächsten Schritts durch das Werfen einer Münze bestimmt wird. Random Walks finden in vielen Bereichen Anwendung, von der Biologie über die Informatik bis hin zum Finanzwesen, was auch für die Quantum Walks gilt. Die Gesetze der Quanteninformation besagen, dass die Entwicklung eines isolierten Quantensystems deterministisch ist. Der Zufall tritt nur dann in Erscheinung, wenn das System gemessen wird und man klassische Informationen erhält. Wir untersuchen die mögliche Anwendung für Probleme aus Optimierung und Graphentheorie, wenn Quantum Walks in verschiedenen Geometrien, durch wiederholte stroboskopische Messungen beeinflusst werden. Diese neue Möglichkeit, während der Berechnung Messungen durchzuführen („mid-circuit measurements“), z. B. auf IBM-Quantencomputern, eröffnet neue Perspektiven im Bereich der Algorithmenentwicklung. Auf Zwischenmessungen basierende Quantenschaltkreise haben wichtige Anwendungen, z. B. in der Quantenfehlerkorrektur, im topologischen Quantencomputing, bei Techniken zum Zerlegen („cutting and knitting“) von Schaltkreisen, Reservoir Computing oder zur Vorbereitung von Ressourcenzuständen im fehlertoleranten Quantencomputing. Darüber hinaus ist es mit Mid-Circuit-Messungen und Feed-Forward-Operationen möglich, bestimmte Beschränkungen der Schaltungstiefe und der Konnektivität der Qubits auf dem Qubit-Chip zu überwinden.

Eine große Anzahl von Problemen aus Logistik, Lieferketten-Management oder Kryptoanalyse kann in eine Optimierungsaufgabe umgewandelt werden, deren Ergebnis ein Zustand, eine Bitfolge oder eine Verteilung ist. Für viele dieser Probleme können nur Näherungslösungen mithilfe von Höchstleistungsrechnern gefunden werden. Quantenvariationsalgorithmen ermöglichen einen lernbasierten Ansatz. Die Parameter des Schaltkreises (Gatter- oder Puls-Parameter) werden durch Optimierung einer Kostenfunktion gefunden. Die Quantenvariationsalgorithmen werden kontinuierlich in Theorie und experimenteller Umsetzung verbessert, aber auch neue heuristische oder auf Approximationen basierende Algorithmen werden entwickelt.

Das maschinelle Lernen mithilfe von Quantencomputern ist ein Forschungsbereich, in dem das Zusammenspiel von Ideen aus dem Quantencomputing und dem maschinellen Lernen untersucht wird. Wir können zum Beispiel herausfinden, ob sich durch Quantencomputer die Zeit verkürzen lässt, die zum Trainieren oder Bewerten eines maschinellen Lernmodells benötigt wird. Andererseits können wir Techniken des maschinellen Lernens nutzen, um Quantenfehlerkorrektur-Codes zu entschlüsseln, die Eigenschaften von Quantensystemen abzuschätzen oder neue Quantenalgorithmen zu entwickeln. Mithilfe von Quantenvariationsalgorithmen können „Quantum Machine Learning“ Anwendungen realisiert werden, sowohl für klassische Daten als auch für Quantendaten, beispielsweise aus Quantensensoren. Dazu gehören konkret Quantum Clustering, Quan-



Visualisierung der Rückkehrzeit bei einem „Monitored Quantum Walk”.

ALLE ABB.: FI CODE

tum Boltzmann Machines, Kernel Methods, Quantum Convolutional Neural Networks, Quantensupport-Vektormaschinen, Quanten-Autoencoder oder generative adversarische Quantennetze. Kernel-Maschinenlernverfahren sind in der Mustererkennung allgegenwärtig, wobei „Support Vector Machines“ die bekannteste Methode für Klassifizierungsprobleme sind und auch als Quantenalgorithmus verwendet werden können. Die Codierung klassischer Daten in Quantenzustände (Quantenschaltkreis) wird Quantenmerkmalskarte genannt. Diese Merkmalskarte eröffnet die Möglichkeit, die Vorteile der Quanteninformationsverarbeitung in Algorithmen des maschinellen Lernens zu integrieren. Es ist davon auszugehen, dass wir einen Quantenvorteil erhalten können, wenn wir eine Quantenmerkmalskarte wählen, die mit einem klassischen Computer nicht leicht zu simulieren ist.

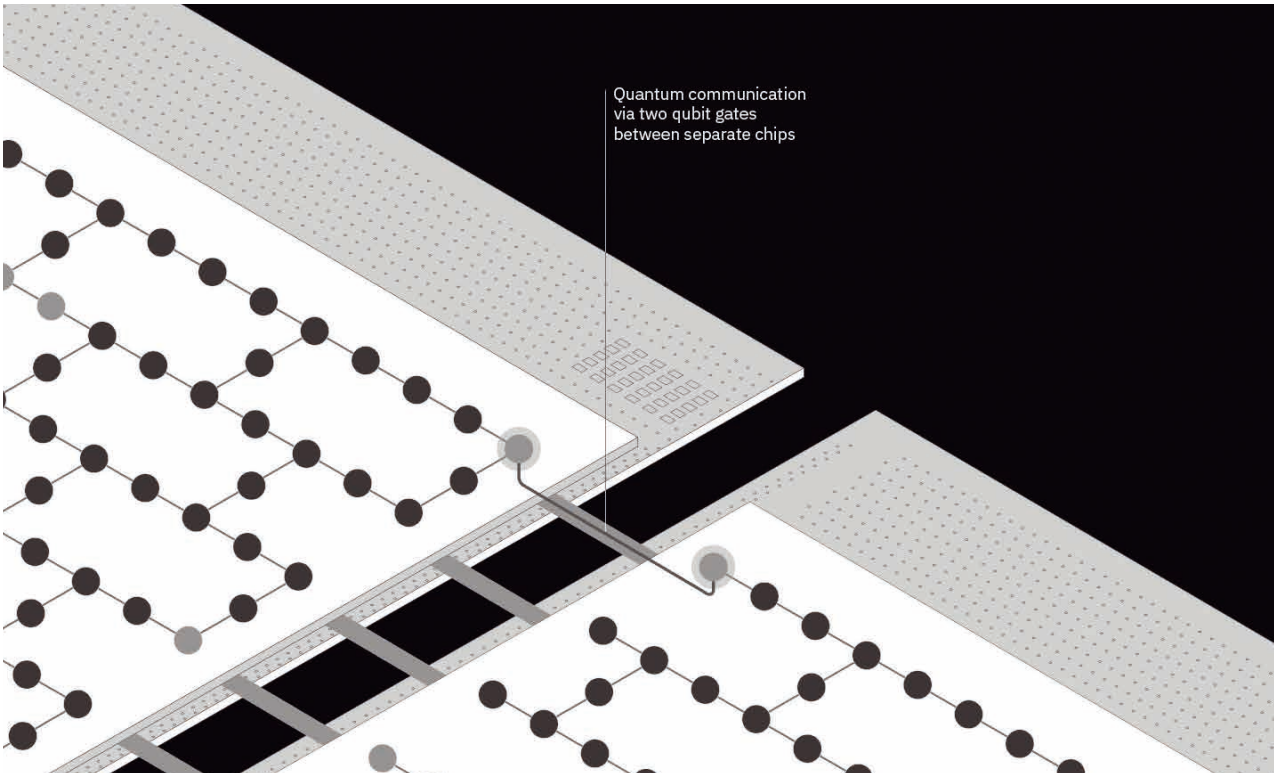
Wir untersuchen die Vorhersagekraft verschiedener Kombinationen von Quantenschaltkreisarchitekturen für die Quantenmerkmalskarten. Einen Quantenvorteil für die Klassifizierung von realen Daten zu finden ist eine große Herausforderung, vor allem, wenn es um heterogene Daten oder große Datensätze geht, die mehr Qubits benötigen, als auf aktuellen Quantencomputern verfügbar sind. In unserer Forschung untersuchen wir Quantenschaltkreisarchitekturen für Daten aus verschiedenen Quellen (Data Fusion), und die Möglichkeit Quantenchips zu kombinieren, um größere Datensätze zu verarbeiten.

Es wurde bereits ein exponentieller Vorteil im Bereich des Quantum Machine Learnings mit Quantendaten gezeigt. Anstelle der Verarbeitung der Quantendaten mit einem klassischen Computer kann man diese kurzzeitig in einen Quantenspeicher übertragen und von einem Quantencomputer auswerten lassen. Für die Charakterisierung des Quantenzustands des Sensors braucht man dann exponentiell weniger Daten im Vergleich zur herkömmlichen Verarbeitung. Eine weitere wichtige Anwendung ist die Simulation von Quantenmaterialien.

Quantensysteme sind jedoch nicht die einzigen Systeme, die schwer zu simulieren sind. Es gibt viele wichtige klassische Prozesse, die möglicherweise effizienter auf einem Quantencomputer simuliert werden könnten. Wenn durch den erfolgreichen Einsatz der Fehlerkorrektur Fehlertoleranz erreicht wird, sind bereits Algorithmen vorhanden, die dies ermöglichen könnten.

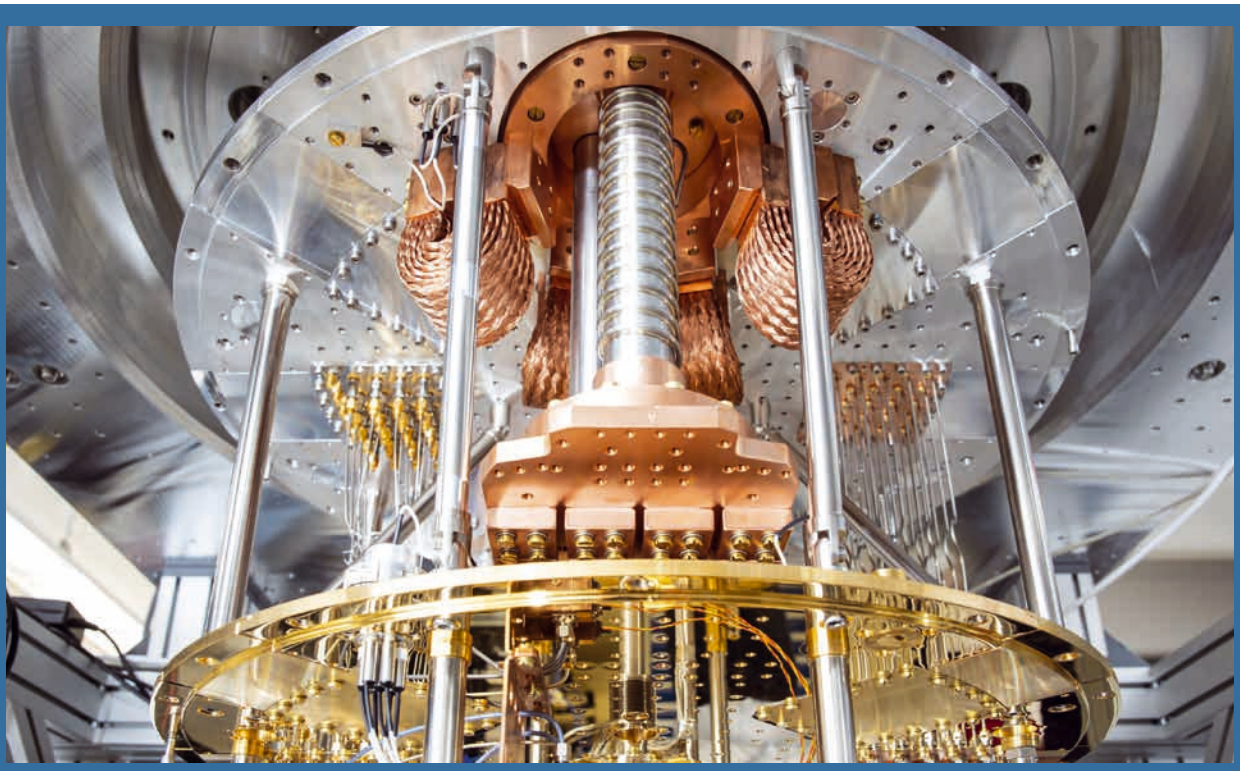
Ausblick

Die Unterdrückung und Mitigation von Fehlern ist eine der zentralen Herausforderungen für die realistische Anwendungen in der Quanteninformatik. Fehlerkorrigiertes Quantum Computing, das neue Anwendungen ermöglicht, zeichnet sich bereits ab. Erst kürzlich wurde in bahnbrechenden Experimenten eine skalierbare Fehlerkorrektur sowie die Möglichkeit der Quanteninformationsverarbeitung mit logischen Qubits demonstriert. Das Zeitalter der Fehlertoleranz zeichnet sich ab. ■



Quantenkommunikation zwischen zwei Quantenchips.

ABB.: IBM, FZ JÜLICH / SASCHA KREKLAU



Quantencomputing

QUANTENCOMPUTING ist ein Paradigma, das bei bestimmten Rechenproblemen exponentielle Geschwindigkeitssteigerungen gegenüber dem klassischen Rechnen ermöglicht. Die Rechenoperationen werden dabei mit Qubits durchgeführt. Ein Qubit ist die kleinste Informationseinheit eines Quantencomputers. Es ist ein quantenmechanisches Zweizustandssystem, das sich in einem Superpositionszustand (Überlagerungszustand) von 0 und 1 befinden kann. Die Superposition ermöglicht Interferenzeffekte, die zentral für die Quantenalgorithmen sind. Erst bei einer Messung geht das Qubit in einen der beiden Zustände (0, 1) über. Das Messergebnis kann dann in einem klassischen Bit gespeichert werden. Mit jedem zusätzlichen Qubit verdoppelt sich die Größe des für einen Quantenalgorithmus verfügbaren Zustandsraumes. Diese exponentielle Skalierung ist die Grundlage für die Leistungsfähigkeit von Quantencomputern. Theoretische Arbeiten haben gezeigt, dass – verglichen mit den besten bekannten klassischen Algorithmen – bestimmte strukturierte Probleme mit Quantenalgorithmen exponentiell schneller berechnet werden können.

Quantencomputer versprechen ein enormes Potenzial für die effiziente Lösung einiger der schwierigsten Probleme in den Natur-, Wirtschafts- und Computerwissenschaften, etwa Faktorisierung, Optimierung oder Modellierung von komplexen Systemen. Diese Probleme sind für jeden heutigen oder zukünftigen klassischen Computer unlösbar.

Bei vielen praktischen Berechnungsproblemen kommen heute heuristische Algorithmen zum Einsatz, deren Wirksamkeit empirisch nachgewiesen wurde. Analog dazu wurden auch heuristische Quantenalgorithmen vorgeschlagen. Empirische Tests sind jedoch nicht möglich, bevor die entsprechende Quantenhardware verfügbar ist. Mit den jüngsten bemerkenswerten technologischen Fortschritten besteht nun die Möglichkeit, Quantenalgorithmen und Quantenheuristiken auf kleinen Quantencomputern zu testen.

Kontaktpersonen zum Quantencomputing am FI CODE

Dr. Sabine Tornow
sabine.tornow@unibw.de
+49 89 6004 7370

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

Quantum Computing trifft Cybersicherheit

Beim Symposium „Quantum Computing Meets Cyber Security" trafen sich Mitte Mai 2023 in Garching Expertinnen und Experten aus verschiedenen Bereichen, um über Cybersicherheitsrisiken im Zeitalter der Quantencomputer zu diskutieren. Organisiert wurde die Veranstaltung vom Munich Quantum Valley, der Ludwig-Maximilians-Universität München sowie dem Forschungsinstitut CODE.

QUANTENCOMPUTER SOLLEN in Zukunft in der Lage sein, Probleme zu lösen, die weit über die Leistungsfähigkeit heutiger Computer hinausgehen. Mit den neuen Möglichkeiten gehen aber auch neue Risiken einher – insbesondere im Hinblick auf die Sicherheit der Kommunikation und Informationsverarbeitung. Solche Einsatzmöglichkeiten von Quantentechnologien, zum Beispiel für Cyberangriffe, müssen daher bereits bei der Entwicklung berücksichtigt werden.

Interdisziplinäre Vorträge und Diskussionen

In insgesamt elf Vorträgen wurden Fragen der Cybersicherheit sowie die Bedrohung durch und die Abwehr von quantenbasierten Cyberangriffen aus verschiedenen interdisziplinären Perspektiven beleuchtet. Darunter waren Beiträge von Expertinnen und Experten aus den Bereichen Informatik, Mathematik, Cybersicherheit und Quantenphysik. Die Sicht eines Sicherheitsforschers auf die Risiken und Chancen von Quantencomputern stellte Professor Dr. Wolfgang Hommel vor. In seinem Vortrag skizzierte der Leitende Direktor des FI CODE grundlegende Sicherheitsparadigmen, Anforderungen und Methoden im Zusammenhang mit Quantencomputern, die eines Tages in komplexere IKT-Infrastrukturen integriert werden sollen, und gab denjenigen, die Quantencomputer entwickeln und konstruieren, einen Einblick in die Hoffnungen und Befürchtungen der Sicherheitsgemeinschaft.

Darüber hinaus diskutierten die rund 100 Teilnehmenden Anwendungen aus dem Bereich der Quantenkryptographie für sichere Kommunikationstechnologien sowie Fragen der Post-Quantenkryptographie und die Notwendigkeit von "Security-by-Design"-Hardware. Alle Anwesenden waren sich einig, dass für eine sichere Quanteninfrastruktur weiterhin eine enge Zusammenarbeit zwischen den verschiedenen Fachdisziplinen notwendig ist.

Reger Austausch und Vernetzung

Auch die Pausen im Programm wurden von den Teilnehmenden produktiv genutzt. Bei einem Kaffee wurden die Gespräche fortgesetzt und dabei neue Kontakte für zukünftige Kooperationen geknüpft oder alte Bekanntschaften aufgefrischt. ■

Über Chancen und Risiken von Quantencomputern sprach Prof. Dr. Wolfgang Hommel in seinem Vortrag vor den rund 100 Teilnehmenden des Symposiums in Garching.

BEIDE ABB.: MQV / MIKKA STAMPA

Bild rechts: Oberst i. G. Beck (l.) überreichte Professor Florian Alt und Professorin Michaela Geierhos als Andenken jeweils ein kunstvolles Porträt von Albert Einstein.

JSEC veranstaltet erstes Cyber-Awareness-Training

Am 16. März 2023 fand in der Wilhelmsburg-Kaserne in Ulm beim Joint Support and Enabling Command (JSEC) das erste Cyber-Awareness-Training statt. Unter der Leitung von Professor Dr. Florian Alt und Professorin Dr. Michaela Geierhos vom Forschungsinstitut CODE wurden insgesamt knapp 250 NATO-Angehörige weiterqualifiziert.

IN DIESEM JAHR lag der Schwerpunkt auf nutzerzentrierter Authentifizierung und Social-Engineering-Angriffen sowie der Erkennung von Fake News und Desinformationskampagnen. Ziel der Veranstaltung war es, die internationalen Teilnehmerinnen und Teilnehmer für die alltägliche Bedrohung durch gezielte Manipulation zu sensibilisieren. Während es beim Social Engineering um die zwischenmenschliche Beeinflussung geht, um Menschen zu bestimmten Verhaltensweisen zu bewegen, z. B. zur Preisgabe vertraulicher Informationen, können Desinformationskampagnen auch dazu führen, dass das Vertrauen in die Demokratie und ihre rechtsstaatlichen Prinzipien sowie das Vertrauen in die Meinungsfreiheit massiv geschwächt wird.

Anhand sehr anschaulicher Praxisfälle konnten die Professoren Alt und Geierhos den Soldatinnen und Soldaten neben aktuellen Themen aus ihrer Forschung, was technisch möglich ist, auch wertvolle Hinweise geben, worauf zu achten ist, um sich dienstlich und privat davor zu schützen.

Als Andenken an ihren Besuch erhielten die beiden CODE-Professoren ein Porträt von Albert Einstein mit dem E^3-Logo des JSEC. Das Leitmotiv „Effective – Efficient – Enablement“ verkörpert die Vision des JSEC. Die drei Komponenten bedingen sich gegenseitig und erzeugen ein hohes Maß an Synergie, die sich mathematisch in Anlehnung an Ulms berühmtesten Sohn und seine Formel $E=mc^2$ am besten mit der dritten Potenz, also $E \times E \times E = E^3$ beschreiben lässt. ■

BEIDE ABB.: BUNDESWEHR / SEEGERT

Forschungsvermittlung und Awareness im Bereich Cybersecurity

Prof. Dr. Arno Wacker, Prof. Dr. Bernhard Esslinger und Prof. Dr. Michaela Geierhos (v. l. n. r.) bei der Urkundenübergabe des CrypTool-Projekts.

Das Open-Source-Projekt CrypTool – nach Meinung von Experten die weltweit am meisten genutzte Kryptografie-Lernsoftware – findet nach 25 Jahren seine neue Heimat am Forschungsinstitut CODE der Universität der Bundeswehr München. Prof. Bernhard Esslinger von der Universität Siegen übergab im Rahmen des zweitägigen CrypTool-Symposiums die Projektleitung an Prof. Dr. Arno Wacker und Dr. Doris Behrendt.

AM 30. UND 31. MÄRZ 2023 kamen mehr als 40 Teilnehmerinnen und Teilnehmer zum CrypTool-Symposium am Forschungsinstitut CODE zusammen. In zahlreichen interessanten Vorträgen wurden aktuelle Fragestellungen sowie die zukünftige Weiterentwicklung von CrypTool diskutiert.

Zu den Highlights des abwechslungsreichen Programms zählten der Vortrag von Dr. Lasry, dessen Name kürzlich durch die Presse ging als der Entschlüsseler der Briefe von Maria Stuart, aber auch die Beiträge von Prof. Dr. Gregor Leander und von Prof. Dr. Jürgen Fuß. Prof. Dr. Leander von der Ruhr-Universität Bochum sprach in seinem Vortrag über das Exzellenzcluster CASA und eine besondere Form von KI-Methoden zur Kryptoanalyse. Herr Prof. Dr. Fuß (FH Oberösterreich) gab Einblicke in die aktuelle Forschung zu Quanten- und Post-Quanten-Kryptografie.

Das CrypTool-Projekt (www.cryptool.org) ist eine Sammlung von Softwareanwendungen, Lehr- und Lernmaterial zum Thema Kryptografie. Dabei stehen historische Verfahren ebenso im Fokus wie Anwendungen, die in modernen IT-Umgebungen verwendet werden. Zusätzlich ist die Krypto-Challenges-Seite MysteryTwister (www.mysterytwister.org), die ihre Basis an der Ruhr Universität Bochum hat, an das Projekt angedockt.

CrypTool wurde von Prof. Dr. Esslinger ursprünglich als Awareness-Tool während seiner Zeit bei der Deutschen Bank ins Leben gerufen. Unter seiner Leitung und unter Mitwirkung zahlreicher Freiwilliger, Studierenden, Forschenden und Challenge-Solvern aus der ganzen Welt fand seitdem eine stetige Weiterentwicklung statt. CrypTool zeichnet sich besonders durch seine hohe fachliche Qualität und den Open-Source-Ansatz aus, der es den Usern ermöglicht, die Software kostenlos zu nutzen.

Bereits im Jahr 2019 war die technische Infrastruktur von CrypTool von Kassel nach München umgezogen. Nun wurde auch die inhaltliche Regie an das Forschungsinstitut CODE und dort an die Professur für Datenschutz und Compliance von Herrn Prof. Dr. Wacker übergeben. Frau Dr. Behrendt wird zukünftig die Weiterentwicklung und Pflege des CrypTool-Projektes übernehmen. ■

Prof. Dr. Gregor Leander sprach auf dem Symposium über das Exzellenzcluster CASA und KI-Methoden zur Kryptoanalyse.

BEIDE ABB.: FI CODE / B. BELLGRAU

CODE veranstaltet erstes OSINT-Forum

Am 8. und 9. November 2023 trafen sich rund 60 OSINT-Interessierte zum Austausch in München und sprachen über aktuelle technische Fragestellungen und Einsatzmöglichkeiten.

OPEN SOURCE INTELLIGENCE (OSINT) gewinnt zunehmend an Bedeutung angesichts der Herausforderung, eine ständig wachsende Menge an Informationen zu verarbeiten, die öffentlich zugänglich und für verschiedenste Fragestellungen relevant sein können. Für eine sinnvolle Integration von OSINT sind nicht nur technische Lösungen zur Verarbeitung der Datenmengen erforderlich. Auch braucht es ausgebildetes Fachpersonal zur Auswertung der Daten und zur Etablierung entsprechender Prozesse und Verfahren.

Aufgrund der Relevanz und Komplexität des Themas veranstaltete das Forschungsinstitut CODE in Kooperation mit der ESG Elektroniksystem- und Logistik-GmbH und der PD – Berater der öffentlichen Hand GmbH in diesem Jahr zum ersten Mal ein OSINT-Forum. Ziel dieser Veranstaltung war der Austausch und die Vernetzung von zivilen und militärischen Sicherheitsexpertinnen und -experten mit OSINT-Fachleuten aus Forschung und Industrie.

Eröffnet wurde das OSINT-Forum am 8. November in München durch Prof. Dr. Michaela Geierhos, Technische Direktorin von CODE und Inhaberin der Professur für Data Science. Gemeinsam mit ihrer Kollegin Prof. Dr. Eirini Ntoutsi, seit August 2022 Professorin für Open Source Intelligence an der Universität der Bundeswehr München, vertrat sie die wissenschaftliche Sicht auf das Thema. „Die Gewinnung verwertbarer Informationen aus offenen Daten ist ein enormes Potenzial von OSINT, das wir nutzen müssen“, so Geierhos. Die Anwendungsfelder von OSINT im öffentlichen Sektor, aber auch in der Industrie, seien ebenso vielfältig wie seine Einsatzmöglichkeiten. Es liege daher nahe, dass das Fachwissen gebündelt und die Vernetzung über die Organisationsstrukturen hinweg verbessert werden müsse. „Deshalb ist es ein zentrales Anliegen von CODE, ein Forum zu schaffen, auf dem in Zukunft regelmäßig und in exklusiver Runde die drängenden Fragen im Bereich OSINT diskutiert werden können“, ergänzte die Technische Direktorin.

> „Die Gewinnung verwertbarer Informationen aus offenen Daten ist ein enormes Potenzial von OSINT, das wir nutzen müssen.“
>
> *Prof. Dr. Michaela Geierhos, Technische Direktorin des FI CODE*

Das erste OSINT-Forum eröffneten Stefan Vollmer (ESG), Prof. Dr. Michaela Geierhos (FI CODE) und Louis Jarvers (PD) (v. l. n. r.)

ABB.: FI CODE

Abteilungsleiter CIT besucht CODE

Generalleutnant Michael Vetter, Abteilungsleiter Cyber-/Informationstechnik (CIT) und Chief Information Officer im Bundesministerium der Verteidigung (BMVg) traf bei seinem Besuch in München am 20. November 2023 mit Wissenschaftlerinnen und Wissenschaftlern von CODE zusammen und informierte sich über aktuelle Fortschritte in der Cybersicherheits- und Quantentechnologieforschung.

NACH GESPRÄCHEN mit der CODE-Leitung gaben ausgewählte Professuren und Arbeitsgruppen Generalleutnant Vetter einen Einblick in ihre Forschungsthemen. Mit Prof. Dr. Marta Gomez-Barrero und Prof. Dr. Daniel Slamanig stellten sich auch zwei neu berufene CODE-Professoren vor. Gomez-Barrero hat seit Oktober die Professur für Maschinelles Lernen inne. Slamanig hat Anfang November die Professur für Kryptologie übernommen. Darüber hinaus gab es ein Update zu den Entwicklungen im Bereich Quantentechnologien sowie zu den neuesten Aktivitäten im Bereich Software-Defined Defence, an denen CODE beteiligt ist.

Einblicke in CODE-Labore und Cyber Range

Auch das dtec.bw-Forschungsprojekt MuQuaNet, das unter anderem den Aufbau und Betrieb eines quantensicheren Netzwerks zum Ziel hat, wurde dem Generalleutnant vorgestellt. Bei einem Rundgang durch das MuQuaNet-Labor konnte sich Vetter vom Stand der Arbeiten überzeugen. Ebenso besichtigte er das BehaVR Lab von Professor Dr. Florian Alt, der dort mit seinem Team unter anderem zu Fragen der Verhaltensbiometrie forscht. Der Rundgang durch das Forschungsinstitut endete in der Cyber Range, wo das Trainerteam dem Gast aus dem BMVg einen Einblick in die neuesten Entwicklungen und Übungsszenarien gab, mit denen am FI CODE das Fachpersonal ausgebildet wird.

Zeit für persönliche Gespräche

Von der hohen Qualität der Aus- und Weiterbildung, die bei CODE stattfindet, konnte sich Generalleutnant Vetter beim Besuch der zeitgleich stattfindenden Übung „Army Cyber Spartan 2023“ überzeugen. Neben zahlreichen internationalen Teams nahm auch in diesem Jahr wieder ein rein studentisches Team der UniBw M aus dem Reachback am FI CODE remote an der Cyber-Defence-Übung der British Army teil. Eine Woche lang trainierte die zehnköpfige Gruppe vor allem Live-Fire-Verteidigung sowie Threat Hunting und erreichte am Ende eine Platzierung unter den ersten Vier. Im Anschluss an die Übungsbesichtigung nahm sich der General Zeit für persönliche Gespräche mit den Übungsteilnehmenden sowie weiteren Soldatinnen und Soldaten aus dem Bereich Cyber- und Informationsraum. ■

Ausgewählte Professuren und Arbeitsgruppen gaben Generalleutnant Vetter einen Einblick in ihre aktuellen Forschungsthemen.

Nach der Übungsbesichtigung nahm sich Vetter Zeit für persönliche Gespräche mit den Soldatinnen und Soldaten.

BEIDE ABB.: UNIBW M / SIEBOLD

Timothy Povich, General Sverre Diessen, Jackie Eaton, Donna Wood, Stefan Pickl, Oberst Matthias Kinkel und Altan Ozkil (v. l. n. r.)

ABB.: FI CODE / PICKL

Stefan Pickl erhält Excellence Award für seine Arbeit im NATO Thinktank

Die NATO Science and Technology Organization (STO) hat Prof. Dr. Stefan Pickl von der Universität der Bundeswehr München (UniBw M) Ende Mai 2023 in Harstad (Norwegen) für seinen umfassenden Forschungsbeitrag zu den zukünftigen Auswirkungen von COVID-19 auf die NATO-Allianz ausgezeichnet. Prof. Dr. Pickl arbeitete über zwei Jahre in der internationalen Arbeitsgruppe „STO Specialist Team SAS169" mit, die sich mit speziellen Vulnerabilitäts-Analysen und Prozessoptimierungen im Kontext der Corona-Pandemie befasste.

MIT DEM Excellence Award würdigt die STO jedes Jahr herausragende Beiträge in ausgewählten Panelforschungsaktivitäten. So auch 2023: Prof. Dr. Stefan Pickl vom Institut für Theoretische Informatik, Mathematik und Operations Research der UniBw M sowie des Forschungsinstituts CODE erhielt den Excellence Award für seine Arbeit im speziellen SAS-Panel „The future impacts of COVID-19 on the Alliance".

Prof. Dr. Stefan Pickl ist zudem deutscher Repräsentant im SAS-Board der NATO und arbeitet regelmäßig in internationalen Arbeitsgruppen mit. Schon zum zweiten Mal wird eine Arbeitsgruppe mit seiner Beteiligung ausgezeichnet.

„Diese Auszeichnung freut mich besonders, da die Arbeitsgruppe sich sehr schnell konstituieren musste, und nicht zuletzt aufgrund der Pandemie nur unter erschwerten Bedingungen international zusammenarbeiten konnte", resümiert Prof. Dr. Pickl.

Die Arbeitsgruppe von Prof. Dr. Pickl arbeitet seit mehreren Jahren mit der WHO eng zusammen, Pickl ist zudem im wissenschaftlichen Beirat des „Healthcare System Engineering"-Programms der University of Central Florida tätig.

Im Rahmen des Science for Peace Programs der NATO entwickelte seine Arbeitsgruppe COMTESSA im Kontext des internationalen MASSAI-Projektes (Management of Mass Casualty via an Artificial Intelligence-Based Platform) eine IT-basierte Entscheidungsunterstützungsplattform, dessen Konzeption ebenfalls in die weitreichenden Analysen der SAS Arbeitsgruppe einfloss. ■

ABB.: ADOBE STOCK / ESI

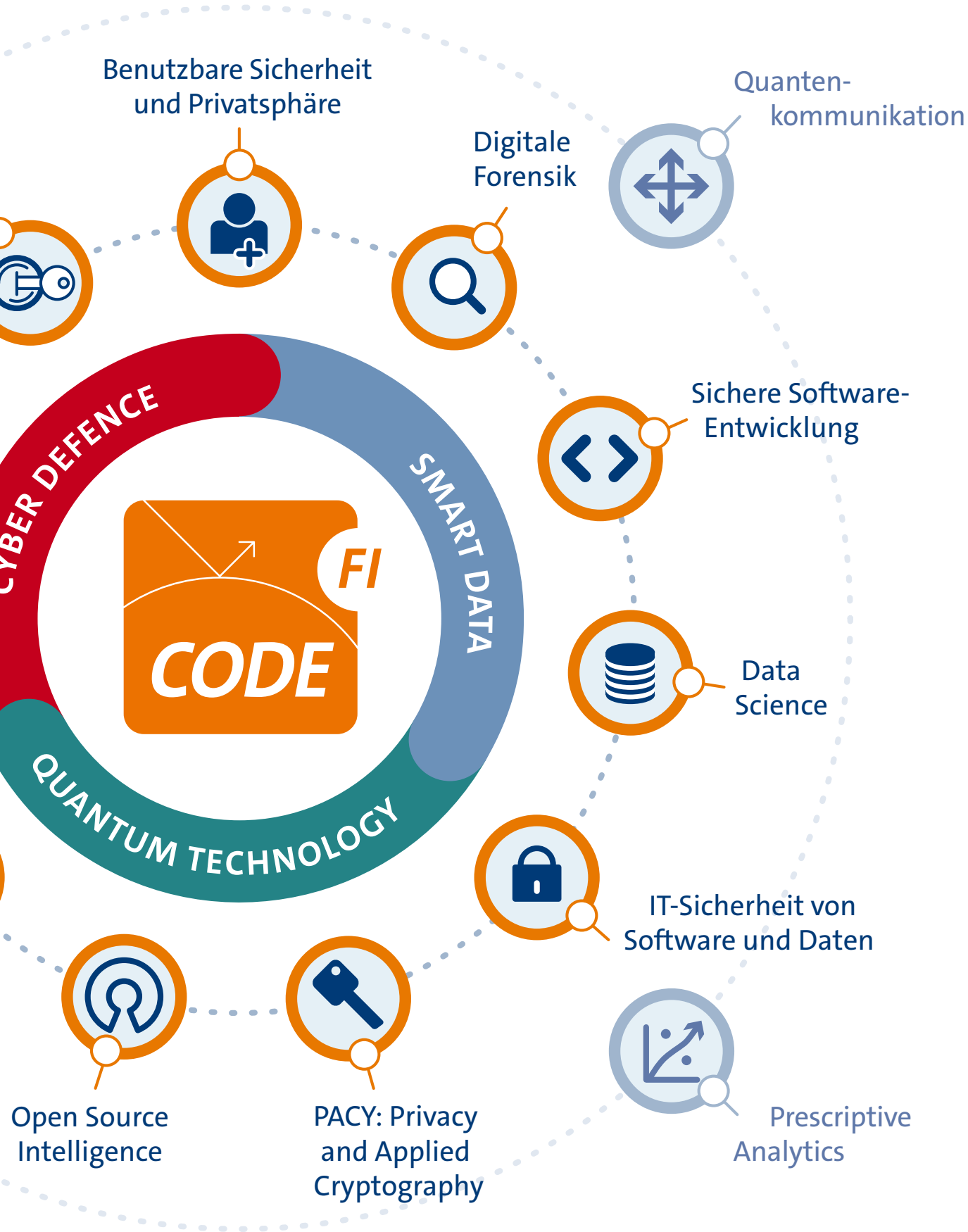
Forschung

Porträts und Projekte

Die Forschung am FI CODE

Am Forschungsinstitut CODE werden derzeit 51 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


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

Prof. Dr. Florian Alt

Forschungsgruppe für Benutzbare Sicherheit und Privatsphäre

Die Forschungsgruppe für Benutzbare Sicherheit und Privatsphäre von Prof. Dr. Florian Alt erforscht menschliches Verhalten in Bezug auf sichere Systeme. Ihre Forschung umfasst die Rolle von Sicherheit und Privatsphäre in benutzerorientierten Design-Prozessen und wie solche Systeme besser an die Interaktion, das Verhalten und den physiologischen Zustand von Nutzern angepasst werden können.

DIE PROFESSUR FÜR Benutzbare Sicherheit und Privatsphäre wurde 2018 gegründet und forscht an der Schnittstelle zwischen Mensch-Computer-Interaktion, IT-Sicherheit und Datenschutz. Prof. Dr. Florian Alt erforscht mit seinem Team, sowohl wie Wissenschaftler, Designer und Produktentwickler dabei unterstützt werden können, Sicherheits- und Datenschutz Bedürfnisse bereits im Designprozess zu berücksichtigen mit dem Ziel, Sicherheits- und Datenschutz Mechanismen besser in die Art und Weise zu integrieren, als auch wie Nutzer im Alltag mit Technologie interagieren.

Forschungsgebiete und Methoden

Die Forschungsgruppe beschäftigt sich mit einer Vielzahl verschiedener Forschungsthemen. Hierzu gehört die Untersuchung von menschlichem Verhalten und physiologischen Reaktionen in sicherheitskritischen Situationen, die Entwicklung neuer sowie die Verbesserung bestehender Sicherheits- und Datenschutz Mechanismen basierend auf menschlichem Verhalten und menschlicher Physiologie, die Untersuchung neuartiger Bedrohungen welche durch ubiquitäre Technologien entstehen sowie die Entwicklung entsprechender Schutzmechanismen, und das Erforschen von Ansätzen um das Verständnis und das Verhalten von Benutzern in sicherheitskritischen Situationen zu verbessern. Spezifische Anwendungsbereiche sind intelligente Wohnumgebungen, Social Engineering, Verhaltens-Biometrie und Mixed Reality.

Im Rahmen ihrer Forschung greift die Gruppe auf Forschungsmethoden zurück, die allgemein aus der Mensch-Computer-Interaktion bekannt sind, und entwickelt diese stetig weiter. Dazu gehören unter anderem nutzerzentriertes Design und iteratives Prototyping. Die Arbeit ist stark auf den Menschen ausgerichtet, was empirische Ansätze zu einem grundlegenden Bestandteil der Forschung der Gruppe macht. Um Verhalten zu verstehen und neue Ansätze zu evaluieren, werden sowohl Studien im Labor als auch im Feld durchgeführt.

Infrastruktur und Publikationen

Die Gruppe verfügt über ein Labor für Mensch-Maschine-Interaktion, welches mit einem hochmodernen Indoor-Positionierungssystem, stationären und mobilen High-End-Eye-Trackern sowie anderen physiologischen Sensoren, Wärmekameras und Augmented sowie Virtual Reality Headsets ausgestattet ist. Darüber hinaus baut die Gruppe derzeit eine Testumgebung auf, in der das Verhalten und die physiologischen Reaktionen von Benutzern in sicherheitsrelevanten Situationen in der realen Welt untersucht werden können.

Zusammen mit seinem Team hat Prof. Dr. Florian Alt über 300 in DBLP gelistete wissenschaftliche Beiträge veröffentlicht und 18 Auszeichnungen auf führenden Tagungen seines Fachgebiets gewonnen. Die Forschung der Gruppe wurde durch die Deutsche Forschungsgemeinschaft (DFG), das Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw), das Bundesministerium der Verteidigung (BMVg), das Bayerische Staatsministerium für Bildung und Wissenschaft, die Humboldt-Stiftung, den DAAD, Google und die BMW Group gefördert.

Entwicklung der Forschungsgruppe im Jahr 2023

Das Forschungsgruppe Usable Security and Privacy hat 2023 neben Prof. Dr. Florian Alt 13 Mitarbeiter und fünf wissenschaftliche Hilfskräfte. Unter den wissenschaftlichen Mitarbeitern der Forschungsgruppe befanden sich sieben Promovierende und vier Postdoktoranden, die 2023 an 23 Publikationen mitgewirkt haben.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

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

Die Professur für Benutzbare Sicherheit und Privatsphäre war 2023 zahlreich auf der ACM CHI Conference on Human Factors in Computing Systems – der größten und bekanntesten HCI Konferenz – vertreten.

ABB.: ISTOCK / PHOTOTECHNO; FI CODE / ALT

Projekt PriMR

Nutzungsschnittstellen zur Kommunikation und Kontrolle von Datenschutz-Aspekten in Mixed Reality

Mixed Reality Headsets erheben Daten über ihre aktiven Nutzer (z. B. Nutzungsdaten, Bewegungsdaten, die Herzfrequenz) und über Menschen in der Umgebung (passive Nutzer). PriMR beschäftigt sich damit, wie aktive und passive Nutzer für die Auswirkungen von MR-Technologie auf ihre Privatsphäre sensibilisiert werden können und wie sie bei Entscheidungen bezüglich der Datenerfassung, -verarbeitung und -weitergabe unterstützt werden können.

Datenerhebung und -schutz in Mixed Reality

Mixed Reality (MR) Headsets ermöglichen zahlreiche neue Anwendungen, unter anderem in den Bereichen Freizeit, Arbeit, Bildung und Marketing. Mit MR können die Nutzer in eine virtuelle Welt eintauchen oder ihre Sicht auf die reale Welt mit virtuellen Inhalten erweitern. Um dies zu erreichen, verwenden MR-Headsets eine Reihe von Sensoren, welche sensible Daten erfassen, verarbeiten und mit Dritten teilen können. Moderne Headsets ermöglichen den Zugriff auf Verhaltensdaten (Hand- und Körperbewegungen, Blick), physiologische Daten (EEG, Herzfrequenz), und Kontextdaten (Tracking-Raum, passive Nutzer).

PriMR beschäftigt sich damit wie Nutzer für die Auswirkungen von Mixed Reality Technologie auf ihre Privatsphäre sensibilisiert werden können.

Aus solchen Daten lassen sich Informationen über Demografie, Gesundheitszustand und Behinderungen ableiten. Es ist offensichtlich, dass solche Daten sensibel sind. Zwar sind Sensoren erforderlich, um das Tracking und Interaktion zu ermöglichen, doch können die erfassten Daten missbraucht werden. Dies stellt eine Herausforderung dar, da der Zugang zu den Daten notwendig ist, um eine immersive Benutzererfahrung zu schaffen. Gleichzeitig ist es wichtig, aktive und passive Nutzer in die Lage zu versetzen, ihre Daten vor einer unbeabsichtigten Nutzung zu schützen.

PriMR: Kommunikation und Kontrolle durch den Nutzer

Im Projekt PriMR wird untersucht, wie Benutzerschnittstellen zur Kontrolle des Datenschutzes für MR entwickelt werden können. Die Kern-Herausforderungen sind (1) wie aktive und passive Nutzer für die Auswirkungen der Nutzung von MR-Technologie auf die Privatsphäre sensibilisiert und (2) wie sie bei sinnvollen Entscheidungen bezüglich der Datenerfassung, -verarbeitung und -weitergabe unterstützt werden können. Da MR in zahlreichen Umgebungen genutzt, eine wachsende Zahl von Anwendungen (Spiele, Büro, Bildung) unterstützt wird, kontinuierlich neuartige Sensoren integriert sowie Nutzer mit unterschiedlichen Fähigkeiten einbezieht, stellen sich unter anderem folgende Fragen: Wie können MR-Benutzerschnittstellen das Bewusstsein dafür schärfen, welche Daten erhoben, verarbeitet und weitergegeben werden? Wie können passive Nutzer von MR-Nutzern über ein laufendes Tracking informiert werden und wie kann ihnen die Kontrolle über ihre Daten gewährt werden? Wie können MR-Benutzerschnittstellen die effiziente Zustimmung zu Datenschutz unterstützen? Wie können Forscher und Praktiker bei der datenschutzgerechten Gestaltung von MR-Anwendungen unterstützt werden?

Das PriMR-Projekt ist ein wichtiger Schritt, um Datenschutz zu einem integralen Aspekt bei der Entwicklung von MR-Anwendungen zu machen.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

https://www.unibw.de/usable-security-and-privacy/research/projekte/primr_dfg

Gefördert durch:
Deutsche Forschungsgemeinschaft (DFG)

ABB.: ISTOCK / METAMORWORKS

Projekt User-Centered Biometric Interfaces

Verbesserung der Kompetenz und der Handlungsfähigkeit von Nutzern biometrischer Authentifizierung

Die maschinellen Lernmodelle, die biometrischen Authentifizierungsmethoden (z. B. Fingerabdruck, Gesichtserkennung oder Verhaltensbiometrie) zugrunde liegen, wirken auf die Nutzer wie eine Blackbox, was ihre Funktionsweise schwer verständlich macht. Im Rahmen dieses Projekts werden Nutzerschnittstellen zu biometrischen Systemen vorgeschlagen, um den Nutzern das Verstehen zu erleichtern und ihnen Kontrolle zu ermöglichen.

Usability-Probleme der Geheimnis Basierten Authentifizierung

Authentifizierung ist zu einem Bestandteil unseres täglichen Lebens geworden. Beispiele sind die Verwendung von Authentifizierungstoken wie Schlüssel, oder die Verwendung von Passwörtern, PINs, und Entsperrmustern für den Zugriff auf digitale Konten und Geräte. Allerdings führt die ständig wachsende Zahl der erforderlichen Authentifizierungen mit solchen Mechanismen zur Überforderung der Benutzer.

Biometrische Authentifizierungsmechanismen

Biometrische Verfahren nutzen einzigartige Muster in der Physiologie oder im Verhalten des Benutzers für die Authentifizierung. Sie erfordern keine geistige Anstrengung, können nicht gestohlen oder vergessen werden und arbeiten im Hintergrund. Biometrische Verfahren haben jedoch auch Nachteile: Die zugrundeliegenden maschinellen Lernmodelle sind für den Benutzer meist undurchsichtig, während sie gleichzeitig anfällig für fluktuierende Erkennungsleistungen sind. Die Nutzer erhalten dabei kaum Einblick in die Entscheidungen des Modells oder Kontrolle über den Authentifizierungsmechanismus, der ihre Daten schützen soll.

Verbesserung von Verständnis und Handlungsfähigkeit

Dieses Projekt verfolgt einen nutzerzentrierten Ansatz, um sowohl bestehende Schnittstellen mit biometrischen Systemen zu verbessern als auch neue vorzuschlagen, um 1) das Verständnis der Nutzer und 2) die Kontrolle über den Erkennungsprozess zu erleichtern. Wir beantworten insbesondere die Fragen: Welche Bedürfnisse haben die Nutzer und wie können sie durch die Gestaltung biometrischer Schnittstellen berücksichtigt werden? Wie können biometrische Schnittstellen den Nutzer dabei unterstützen ihre Funktionalität zu verstehen? Wie können biometrische Schnittstellen die Handlungsfähigkeit der Nutzer unterstützen?

Nutzerzentrierte Biometrische Schnittstellen

Wir haben mehrere Studien durchgeführt, um die Präferenzen und Bedürfnisse von Nutzern zu verstehen. Wir schlagen außerdem Lösungen vor, die den Nutzern helfen, personalisierte Einblicke in die Leistung eines biometrischen Systems zu gewinnen, kontextabhängige Faktoren, die das System beeinflussen, zu verstehen und darauf zu reagieren, und Modelle Entscheidungen vorwegzunehmen. Wir zeigen auch, dass es möglich ist, die Kontrolle über ein biometrisches Verfahren zu erlangen, das keine Schnittstellen hierfür bietet, und stellen Methoden vor, die diese Aufgabe dem Benutzer erleichtern. Zusammenfassend haben wir untersucht, wie biometrische Schnittstellen aussehen könnten, wie die Interaktion mit biometrischen Systemen verbessert werden könnte und ob sie zu einer informierten und sicheren Nutzung der biometrischen Authentifizierung beitragen können.

Die Funktionsweise von biometrischen Authentifizierungsmethoden (z. B. Fingerabdruck, Gesichtserkennung oder Verhaltens Biometrie) ist für Nutzer oft unverständlich.

Lukas Mecke

lukas.mecke@unibw.de

+49 89 6004 7323

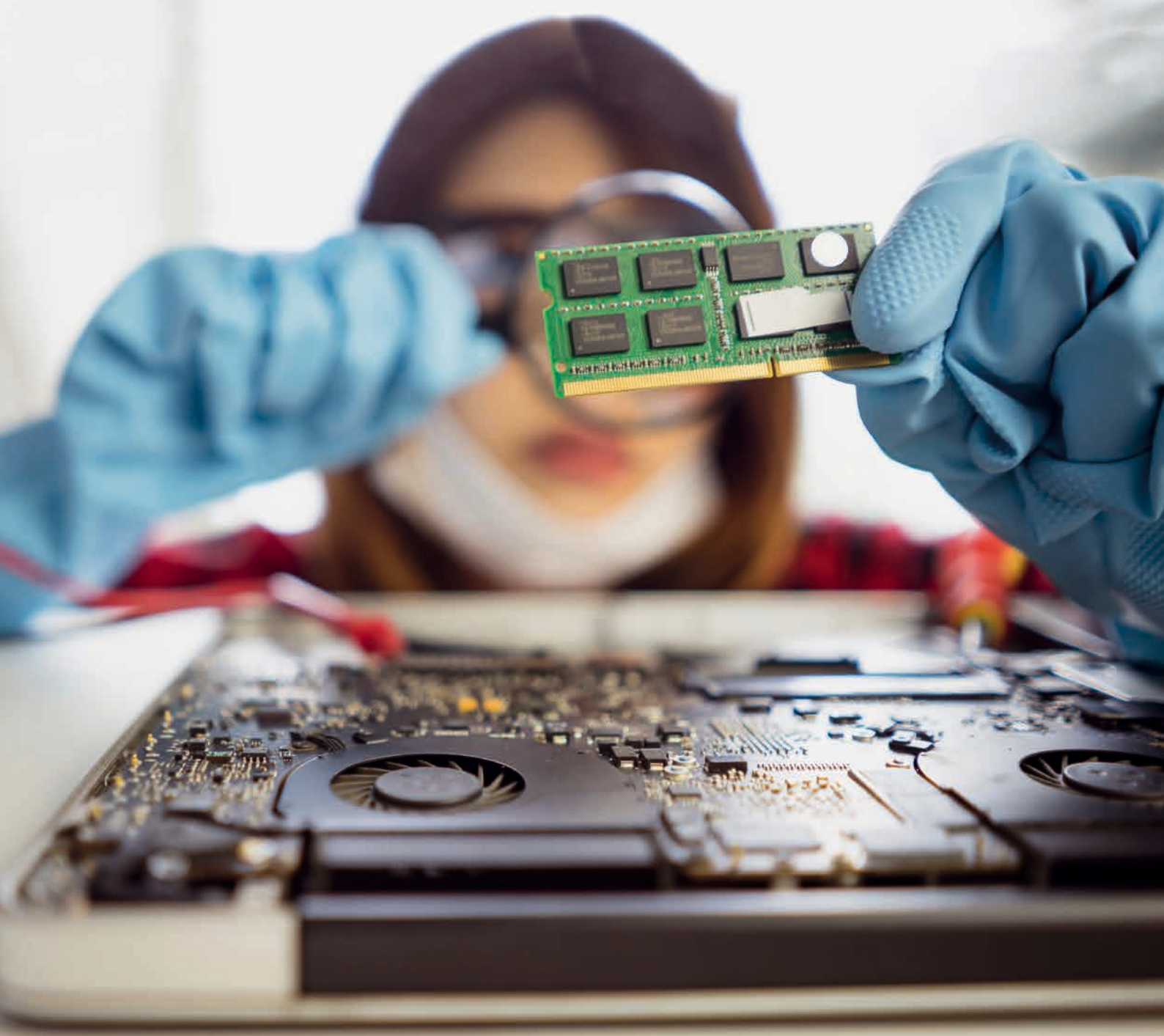
www.unibw.de/usable-security-and-privacy

ABB.: ISTOCK / BLUE PLANET STUDIO

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 „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 „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

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

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.

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.

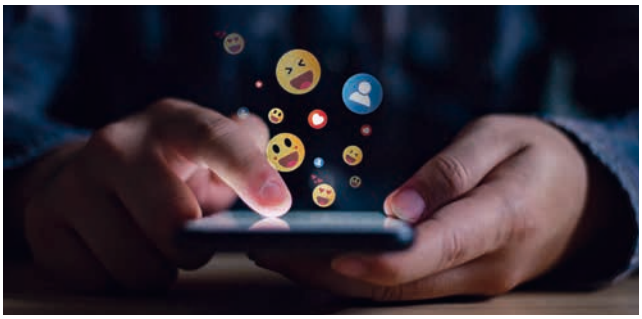
WhatsApp-Sticker sind eine beliebte Mischung aus Emojis und Bildern oder Videos, die von den Nutzern selbst erstellt werden können. Sie unterliegen daher keiner Kontrolle und verbreiten sich automatisch von Nutzer zu Nutzer. Dadurch können sie „viral gehen", nicht nur lustige, sondern auch illegale Sticker. 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) an der Professur „Sichere Softwareentwicklung“ beschäftigt sich mit der Erforschung und Entwicklung neuester Verteidigungstechniken, um fortgeschrittene, hochkomplexe und brandaktuelle Angriffe zu verhindern. Dabei bauen wir auf unsere Expertise im Programmiersprachen Bereich, insb. unser Compiler Know-How, um komplexe und anspruchsvolle Probleme im Querschnitt von Programmiersprachen und Computersicherheit zu lösen. In Anlehnung an Clausewitz, verstehen wir Sprachbasierte Sicherheit als Fortsetzung des Compilerbaus mit anderen Mitteln.

Das vergangene Jahr war für die µCSRL Forschungsgruppe in jeder Hinsicht erfolgreich, sodass wir die Sichtbarkeit erhöhen konnten und damit sicherstellen, dass wir auch in Zukunft anspruchsvolle Probleme in Angriff nehmen können.

Unsere Compiler-basierte Verteidigungstechnik gegen Address-Oblivious Code Reuse Angriffe (AOCR) wurde bei der prestigeträchtigen 18. Europäischen Konferenz zu Computer Systemen (EuroSys) publiziert. Die zugehörige Präsentation erfolgte bei der Konferenz im Mai 2023 in Rom.

Im September 2023 besuchte die ganze µCSRL Forschungsgruppe das 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung (KPS 2023) um dort eine Reihe von Vorträgen zu zentralen Forschungsthemen des Lehrstuhls abzuhalten. Diese Vorträge umfassten neben Fuzzing auch Arbeiten zur Interpreter-Optimierung von Web Assembly (WASM), erste Ergebnisse unserer internationalen Kooperation mit der KU Leuven und der EPFL im „Dependable Production Systems“ Projekt, als auch eine neue Verteidigungstechnik gegen Counterfeit Object-Oriented Programming (COOP) mittels Compiler-basierter Prüfung Objekt-Integrität für C++ Programme.

Neben dem KPS Kolloquium, besuchten wir in 2023 auch das EuroS&P Symposium in Delft und die ACM Computer and Communications Security Konferenz in Kopenhagen.

Im Dezember 2023 konnten wir auch unser vierjähriges Projekt mit Airbus Defense & Space nicht nur pünktlich, sondern auch äußerst erfolgreich abschließen: Alle geplanten Meilensteine wurden erreicht und zur vollsten Zufriedenheit des Projektpartners erfüllt.

Darüber hinaus sind wir sehr erfreut, durch weitere Mitarbeiter Akquise zum Aufwuchs von µCSRL und damit auch zum Wachstum des FI CODE beizutragen. Nach seinem erfolgreich beendeten Masterstudium an der TU Wien, hat er sich für ein Doktoratsstudium bei uns entschieden. Neben den Doktoranden haben wir 2023 auch mehrere Master- und Bachelor-Studierende betreut, unter anderem auch einen Masteranden, der seine Forschung an der University of California, San Diego durchführen konnte.

Im Jahr 2023 wurde Prof. Dr. Brunthaler eingeladen, als Mitglied des Programmkomitees folgender internationaler Top Konferenzen zu dienen: Symposium on Network and Distributed Systems Security (NDSS 2024 in San Diego, USA), ACM SIGPLAN International Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA 2024 in Pasadena, USA), das IEEE European Symposium on Security and Privacy (EuroS&P 2024 in Wien) und den 2024 Workshop on Principles of Secure Compilation (PriSC 2024, co-located with POPL 2024 in London, UK). Herr Prof. Dr. Brunthaler hat auch den Vorsitz des Bereichs „System Security“ im *Journal of Systems Research* (JSys) übernehmen.

µCSRL Projekte werden gefördert vom Bundesministerium der Verteidigung und der Österreichischen Forschungsförderungsgesellschaft.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

www.unibw.de/ucsrl

ABB.: ISTOCK / DE M10

Drohende Gefahr von Angriffen auf Lieferketten

Bestehende Abwehrmechanismen erweisen sich zunehmend als unwirksam

Angriffe auf die Lieferketten sind – analog zur Analyse und Kategorisierung kinetischer Angriffe – *indirekt*: Um ein Ziel zu treffen, greifen sie die zugrundeliegende Infrastruktur an oder untergraben sie, z. B. Compiler und Interpreter, oder bauen Toolketten auf. Sobald ein Opfer seine Infrastruktur aktualisiert, haben die Angreifer schon fast gewonnen.

Kein Vertrauen

1984 hielt Ken Thompson einen Vortrag mit dem treffenden Namen „Reflections on Trusting Trust“. Die Arbeit belegt eindrücklich das indirekte Angriffe nicht nur möglich, sondern gleichzeitig sehr mächtig sind. Thompson änderte einen Compiler so, dass er jedes Mal eine Hintertür einfügte, wenn er ein passwd-Programm kompilierte. Dies hatte zur Folge, dass jedes Mal, wenn dieses Programm kompiliert wurde, eine Hintertür vorhanden war, die die Authentifizierungsbarrieren des Betriebssystems durchbrach. Als zusätzliches Täuschungsmanöver beschrieb Thompson, wie man den Code zum Einfügen der Hintertür verstecken kann: Da ein Compiler benötigt wird, um sich selbst zu kompilieren, fügte Thompson zusätzlichen Code hinzu, der erkennt, wenn er sich selbst kompiliert und dann die Logik zum Einfügen der Hintertür unbemerkt injiziert. Folglich konnte der Quellcode zum Einfügen der Hintertür entfernt werden, was bedeutet, dass keine Untersuchung des Compiler Quellcodes jemals die vorhandene Hintertür entdecken könnte. Diese Überlegungen zum Thema „Vertrauen“ zeigen also deutlich die Grenzen des Vertrauens auf und verdeutlichen die immense Gefahr, die von indirekten Angriffen ausgeht.

Bedeutung im Jahr 2024

In den letzten paar Jahren haben Supply-Chain-Angriffee an Aufmerksamkeit gewonnen, vor allem durch eine Reihe bedeutender Angriffe, z. B. SolarWinds. Obwohl sich die bekannten Supply-Chain-Angriffe in ihrer inneren Funktionsweise unterscheiden, zeigen sie deutlich auf, wie porös moderne Software ist. Die Porosität stammt sowohl aus der Mischung von proprietären und quelloffenen Bibliotheken von Drittanbietern, als auch der Vielzahl von Systemabhängigkeiten für Hard- und Software.

Diese Gemengelage wird durch die starke Abhängigkeit der Entwicklungs- und Fertigungsunternehmen von ihren Zulieferern noch verschärft. Oft hat das Unternehmen, das die zugelieferten Komponenten integriert, keine Möglichkeit, spezifische Anforderungen durchzusetzen, z. B. welche Compiler oder Programmiersprachen zu verwenden sind.Die dadurch entstehende Angriffsfläche für indirekte Angriffe über Lieferketten ist riesig.

Um diese Probleme zu lösen, haben sowohl Industrie als auch Wissenschaft vorgeschlagen, ein Konzept aus der physischen Fertigung zu übernehmen, nämlich die so genannten Stücklisten (engl.: bill of material), in denen detailliert beschrieben wird, welche Komponenten sich in einer Maschine befinden. Das übernommene Konzept wird als Software-Stückliste bezeichnet, abgekürzt SBOM. Es gibt eine Vielzahl von SBOM Standards, die von Build-Tools erstellt werden, um zu spezifizieren welche Komponenten eine Software enthält.

Rückschlüsse aus diesen Beobachtungen

Aus beiden Perspektiven, den Überlegungen zum Vertrauen und dem anhaltenden Trend zu Software-Stücklisten, ergibt sich, dass SBOMs wahrscheinlich die derzeitige Situation verbessern werden, die jede Software als schwarzen Kasten betrachtet. Gleichzeitig folgt jedoch unweigerlich, dass SBOMs durch indirekte Angriffe im Sinne Thompsons erfolglos bleiben werden. Bei der Softwareerstellung oder dem Bau komplexer Softwarekomponenten ist das blinde Vertrauen in Tools nicht mit den potenziellen Problemen durch Angriffe in der Lieferkette vereinbar. In ähnlicher Weise müssen Zertifizierungsstellen, die Software für den Einsatz in kritischen Infrastrukturen zertifizieren, ihre Verfahren so aktualisieren, dass teure und zeitaufwändige Neuzertifizierungen überflüssig werden.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

www.unibw.de/ucsrl

Identifikation von Binärkomponenten

Das Reverse Engineering zur Identifizierung von Binärkomponenten in Programmen ist eine mühsame und fehleranfällige Aufgabe. Immer wieder müssen Ingenieure Programme analysieren, nur um festzustellen, dass ein bestimmtes Stück Binärcode einer bekannten Funktion entspricht. Die daraus resultierenden Reibungsverluste und die damit einhergehende Zeitverschwendung stellen ein erhebliches Hindernis für das Reverse Engineering dar.

Identifikation von Binärkomponenten

Ein Programm in binärer Darstellung ist lediglich eine scheinbar zufällige Sequenz von Nullen und Einsen. Obwohl diese Sequenz für den Computer, der das Programm ausführt, sinnvoll und – hoffentlich – vernünftig ist, sind die Nullen und Einsen für einen Menschen unverständlich. Um ein Programm in binärer Darstellung zu analysieren, führt der Mensch daher eine Reihe von Schritten durch, um Teilen des Programms schrittweise eine Bedeutung, also eine präzise Semantik, zuzuordnen. In einem ersten Schritt werden Binärprogramme in der Regel disassembliert, d. h. die Nullen und Einsen werden durch eine textuelle Darstellung der ursprünglichen Maschinenbefehle ersetzt, z. B. MOV RAX, RBX. Diese Darstellung ist zwar lesbar und aussagekräftig für einzelne Instruktionen, die Analysze größerer Teile anhand einzelner Instruktionen bleibt jedoch mühsam und zeitintensiv. Ein möglicher nächster Schritt ist die sog. Dekompilierung, um aus vielen einzelnen, isolierten Maschinenbefehlen High-Level-Quellcode, z. B. C-Code, zu erzeugen. Da die Dekompilierung selbst jedoch grundsätzlich unentscheidbar ist, gibt es Sequenzen, welche nicht effektiv nach C dekompiliert werden können. Der derzeitige Stand der Technik leidet auch an einer Menge anderer Probleme, wie die zuverlässige Analyse des Kontroll- und Datenflusses und der Wiederherstellung aussagekräftiger Typ Informationen. Alle diese Probleme sind nach wie vor schwierig, da ein Compiler bei der Kompilierung vom Quell- zum Binärcode wertvolle Informationen verwirft.

*µ*BKI

Für viele Aufgaben ist eine vollständige Dekompilierung aber nicht unbedingt erforderlich. Bei einem binären Blob kann es genügen, wenn man weiß, welche Teile im Programm enthalten sind. Zu diesem Zweck genügt es, alle binären Sequenzen des Programms mit einer Datenbank zu vergleichen, die bekannte, gutartige Sequenzen enthält. Wenn eine Sequenz des aktuell analysierten Programms mit einer in der Datenbank übereinstimmt, können wir die ursprüngliche Komponente leicht identifizieren, z. B. ihren Quellcode oder ihre Version.

Im Dezember 2023 wurde beispielsweise Ghidra, das Disassemblierungsprogramm der NSA, um eine solche Komponente erweitert, um die Identifizierung von Binärdateien zu erleichtern.

Unsere Forschung in diesem Bereich begann 2021 und geht das Problem auf eine neuartige Weise an. Dazu müssen wir zunächst eine große Datenbank mit bekanntem, gutem Binärcode erstellen. Zu diesem Zweck haben wir eine Kompilierfarm entwickelt, die große Mengen von Programmen mit verschiedenen Compilern und deren unterschiedlichen Versionen automatisch kompilieren kann. Da die daraus resultierenden Binärdateien enormen Speicherplatz benötigen, analysieren wir die Binärdateien mit einer Vielzahl verschiedener Hash-Verfahren und speichern nur die berechneten Hash Daten.

Sobald wir dann ein neues Programm analysieren, analysieren wir das Programm erneut mit denselben verschiedenen Hashing-Verfahren und suchen diese Hashes dann in unserer Datenbank der vorberechneten Hash-Daten. Wenn wir eine Übereinstimmung finden, können wir mit hoher Wahrscheinlichkeit davon ausgehen, dass die betreffende Binärsequenz gutartig ist und wir diese schon einmal gesehen haben. Folglich besteht keine Notwendigkeit, die Sequenz tatsächlich zu analysieren. Da wir einen solchen Lookup für alle Sequenzen eines Programms durchführen können, können wir alle bekannten Sequenzen herausfiltern, sodass sich die manuellen Reverse-Engineering-Bemühungen auf die unbekannten Sequenzen konzentrieren können. Auf diese Weise können die verfügbaren Ressourcen optimal genutzt werden, was zur deutlichen Verbesserung des Gesamtergebnisses führt.

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

Prof. Dr. Michaela Geierhos

Data Science

Das interdisziplinäre Team der Professur für Data Science vereint Kompetenzen aus den Bereichen Informatik, Computerlinguistik und Mathematik, 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 Mathematik, 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). Die Art der Daten ist dabei sehr vielfältig: Neben Texten werden auch Audiosignale und Bilder verarbeitet.

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. Auch die Erkennung von sogenannten Deepfakes mittels innovativer Methoden der Künstlichen Intelligenz (KI) gehört zum Anwendungsspektrum. Da die Datensynthese häufig für Desinformation, Betrug und andere böswillige Zwecke missbraucht wird, muss die Erkennung synthetischer Bilddaten in Zukunft zuverlässiger funktionieren.

Praxisorientierte Lehre

Ein Lehrkonzept, das Theorie und Praxis verbindet, liegt den Data Science-Veranstaltungen zugrunde. 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.

Praxisorientiert forschen: Data Science Use Cases

Auch in der Forschung werden Theorie und Praxis miteinander verknüpft. So unterhält das Data Science Team zahlreiche Kooperationen mit Partnern aus Militär, Wirtschaft und dem öffentlichen Sektor. Die Anwendungsgebiete reichen derzeit von der Erkennung von Desinformationskampagnen über die Rekonstruktion von Audiodaten bis hin zum Einsatz von vertrauenswürdiger KI in polizeilichen Anwendungen. Ein Ziel der aktuellen Forschung ist die prototypische Implementierung eines einzigen Frameworks, das in der Lage ist, unterschiedlich kodierte Audiosignale zu dekodieren. Ein besonderer Fokus liegt dabei auf der Sprachrekonstruktion. KI-Techniken, insbesondere Generative Adversarial Networks, kommen hier zum Einsatz.

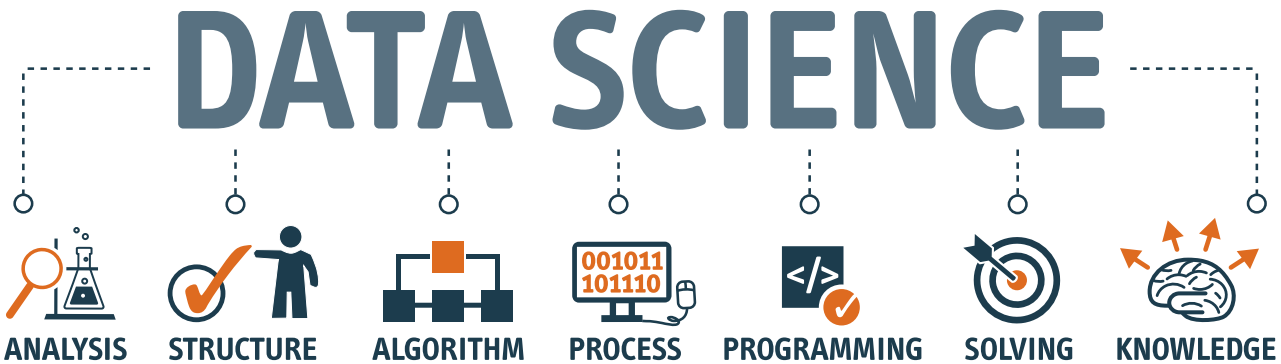
Jüngste technologische Entwicklungen im Bereich der KI ermöglichen ihre Anwendung in vielen Bereichen. Allerdings tauchen immer wieder Fragen zur Vertrauenswürdigkeit auf. Wir wollen daher die Erklärbarkeit vertrauenswürdiger KI-Modelle für den transparenten Einsatz bei Sicherheitsbehörden zur Textklassifikation sicherstellen. Polizeibehörden müssen verschiedenste Textformen in großen Mengen analysieren, so dass KI-Methoden entscheidende Unterstützung leisten können, um verdächtige Inhalte mit hoher Geschwindigkeit und Genauigkeit zu identifizieren. Die Entscheidungen eines KI-Modells sind jedoch nicht einfach zu erklären. Unser Ziel ist es daher, Lösungen zu entwickeln, die verständliche Erklärungen für verschiedene polizeiliche Szenarien liefern, um Vertrauen in die Entscheidungen zu schaffen.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

www.unibw.de/datascience



Aufgabenspektrum der Professur für Data Science.

ABB.: SHUTTERSTOCK / RYZHI; SHUTTERSTOCK / TRUEFFELPIX

Projekt SynData

Generierung und Detektion von synthetischem Bildmaterial

Künstliche Intelligenz (KI) in Anwendungen ermöglicht die Erzeugung synthetischer Bilddaten in wenigen Knopfdrücken. Dies führt dazu, dass Datensynthese häufig für Desinformation, Betrug und andere bösartigen Absichten missbraucht wird. Mit dieser Problematik beschäftigt sich das Projekt SynData, dessen Ziel es ist, sowohl den Generierungsprozess besser zu verstehen, als auch die Erkennung von synthetischen Bilddaten robuster zu machen.

Wie funktioniert die Synthese von Bildmaterial?

KI verarbeitet Bilder, Texte und andere Datentypen in numerischen Repräsentationen und trifft auf Basis dessen Vorhersagen. Heutzutage können Modelle ebenfalls für Aufgaben verwendet werden, die weitaus komplexer sind, wie beispielsweise automatisierte Robotik oder Datengenerierung. Letzteres erfordert komplexe Netzwerkstrukturen, sorgfältig kuratierte Datensätze und ein umfassendes maschinelles Training, um nutzbare Generatoren zu erzeugen. Einmal trainiert, können diese Modelle jedoch visuelle Daten erzeugen, die authentisch wirken (z. B. realistische Porträts von Gesichtern oder Videos).

Was ist Detektion und warum ist es relevant?

Die Synthese auf Basis von KI ist mittlerweile so fortgeschritten, dass man ohne vorherige Kenntnisse in diesem Bereich und spezieller Hardware täuschend echte Texte, Bilder und Videos in nur wenigen Knopfdrücken erstellen kann. Daher sind Detektionsalgorithmen, die numerisch vorhersagen, ob Daten synthetisiert sind, derzeit ein sehr aktuelles Forschungsthema. Viele der aktuell verwendeten Architekturen für Bildgeneratoren führen zu spezifischen Artefakten im Output. Diese Defekte können genutzt werden, um Detektoren zu entwerfen, die darauf trainiert sind, die Artefakte dieser Defekte in Bildern zu finden. Detektoren sind in der Regel neuronale Netze, die auf groß angelegten Datenbanken vortrainiert wurden. Diese werden dann verwendet, um Generierungsartefakte in spezifischen Datensätzen zu erkennen.

Was ist SynData?

Das Projekt SynData ist in zwei Teams unterteilt, wobei sich ein Team mit Synthese beschäftigt und das andere mit Detektion. Beide Teams haben umfassende Frameworks entwickelt, die es ermöglichen, State-of-the-Art-Modelle zu testen und neue Architekturen für spezifische Anwendungsfälle zu erstellen. Das Generierungsteam arbeitet daran, eine bessere Datensynthese bereitzustellen, die qualitativ hochwertigere Bilder erstellt, die schwerer zu detektieren sind. Das Detektionsteam zielt darauf ab, robuste Detektionsalgorithmen zu entwickeln, die synthetisches Bildmaterial zuverlässig erkennen. Die thematische Trennung in Synthese und Detektion ermöglicht Interaktion und Verbesserungen auf beiden Seiten, da eine Verbesserung für ein Team eine neue Herausforderung für das andere darstellt. Im Rahmen des Projekts haben beide Teams bereits neuartige Ansätze präsentiert. Diese Neuerungen verbessern die Merkmalsauswahl in der Bildsynthese und Adversarial Attacks, welche zur Evaluierung der Robustheit von Detektoren verwendet werden. Einige dieser Neuerungen wurden bereits auf hochrangigen Konferenzen veröffentlicht oder befinden sich derzeit in der Endphase der Evaluierung.

KI-generierte Bilder: Künstliche Intelligenz erlaubt das gezielte Ansteuern von Gesichtsmerkmalen im Generierungsprozess.

ABB.: ZITIS / A. MEISSNER

Amon Soares de Souza, M.Sc.
amon.soares@unibw.de
+49 89 6004 7342
https://go.unibw.de/syndata

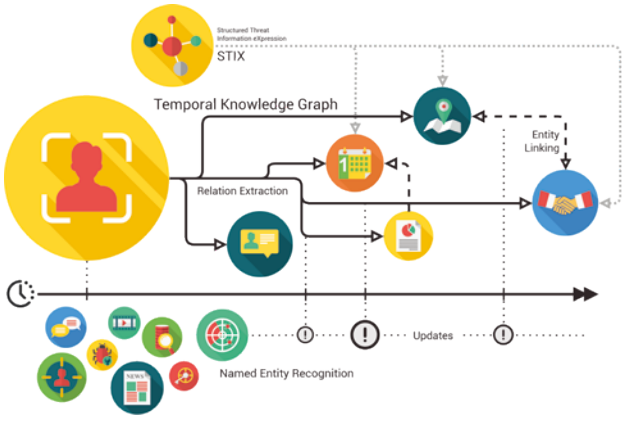
Projekt NAWI

News-Artikel und Wissen

Das Projekt NAWI widmet sich der Extraktion von strukturiertem Wissen aus Cyber-Threat-Intelligence (CTI)-Berichten mithilfe von Methoden der Relation Extraction, Named Entity Recognition und Entity Linking. Das entstehende Wissen soll in einen Graphen überführt werden, der eine zeitliche Analyse, sowie die Vorhersage von Zusammenhängen aufgrund von schon bestehendem Wissen im Bereich der Cybersicherheit ermöglicht.

Bedrohung durch Cyberangriffe und die Rolle von CTI-Berichten

Die heutige vernetzte Welt steht permanent der Gefahr von Cyberangriffen gegenüber, die nicht nur finanzielle Schäden verursachen, sondern auch die Integrität sensibler Daten und die Kontinuität von Prozessen gefährden können. In diesem Kontext spielen CTI-Berichte eine entscheidende Rolle. Sie liefern tiefgehende Einblicke in die Taktiken, Techniken und Verfahren (TTPs), die von Angreifern genutzt werden, sowie in die neuesten Bedrohungen und Schwachstellen. Dadurch stellen CTI-Berichte eine informationsreiche Quelle zur automatisierten Extraktion von Informationen dar.



Techniken zur Erzeugung von temporalen Wissensgraphen, die im STIX-Format strukturiert sind.

Verbesserte Vorbereitung durch Auswertung von CTI-Berichten

Insbesondere die in CTI-Berichten enthaltenen Informationen über vergangene Angriffe tragen dazu bei, eine bessere Vorbereitung auf zukünftige Angriffe zu ermöglichen. Durch die Analyse und Strukturierung dieser Daten können wertvolle Zusammenhänge und Beziehungen zwischen verschiedenen Vorfällen und Akteuren erkannt werden, um in zukünftigen Angriffen besser reagieren zu können. Um diesem Problem entgegenzuwirken, fokussiert sich das Projekt auf die Generierung eines Wissensgraphen aus CTI-Berichten. Mithilfe fortgeschrittener semantischer Analysetechniken wie Relation Extraction und Named Entity Recognition strebt das Projekt an, die Akteure, Tools, Methoden und ähnliches in den Berichten zu erfassen und die Zusammenhänge darzustellen.

Semantische Analyse von CTI-Berichten

Aus täglich entstehenden CTI-Berichten sollen relevante Informationen in das STIX Serialisierungsformat konvertiert werden, die die inhärenten Textzusammenhänge beschreiben. Hierbei wird die von STIX vorgegebene Ontologie genutzt. Durch Named Entity Recognition werden im Text Entitäten identifiziert, während gleichzeitig mithilfe von Relation Extraction die zugehörige Relation vorhergesagt wird.

Knowledge Graph im Bereich Cybersicherheit

Nach der Extraktion semantischer Informationen müssen die identifizierten Entitäten mithilfe von Entity Linking mit dem Wissensgraphen verknüpft werden, der kontinuierlich aktualisiert wird. Ein weiterer Schwerpunkt der Forschung liegt darin, die Kriterien zu ermitteln, die erfüllt sein müssen, damit neue Informationen in den Graphen integriert werden können. In einem späteren Schritt ermöglicht die Link Prediction die Vorhersage fehlender oder zukünftiger Informationen. Zudem kann das Projekt ermöglichen, bestehende Wissensgraphen zu erweitern.

Florian Babl, M.Sc.
florian.babl@unibw.de
+49 89 6004 7352
https://go.unibw.de/nawi

ABB.: FI CODE / F. BABL

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.

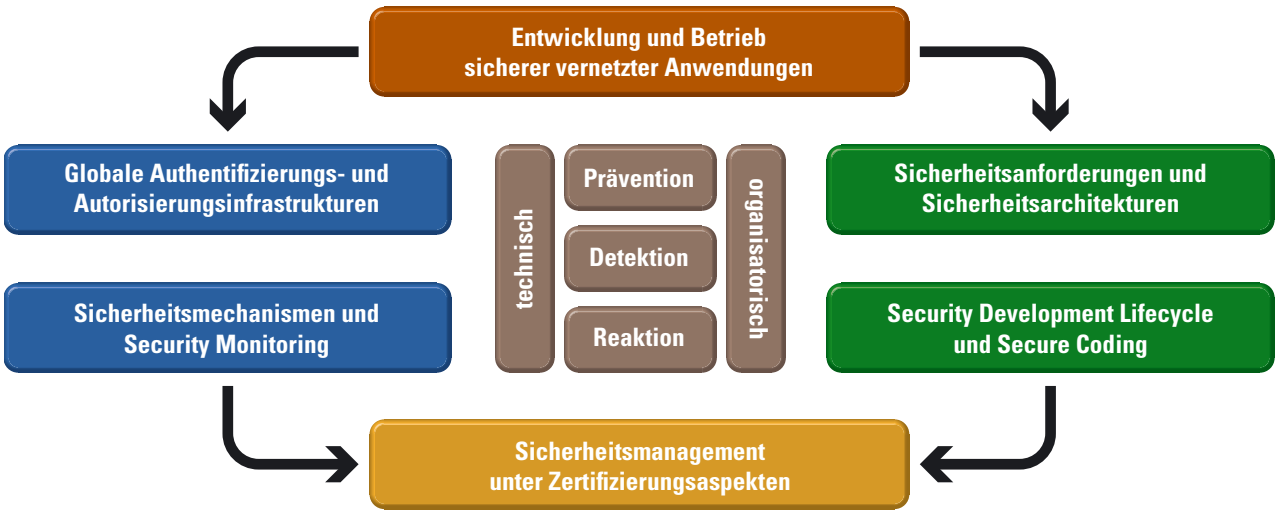
In laufenden Forschungsvorhaben und Projekten wurde 2023 unter anderem an der Verknüpfung dezentraler Identity-Management-Lösungen mit benutzerfreundlichen und datenschutzoptimierten Ansätzen zu Dokumentensignaturen gearbeitet. Innovative Ansätze zur Absicherung von Kommunikationsprotokollen, Security Monitoring und richtliniengesteuerten Automatisierungslösungen wurden auf das Management zukünftiger Energieversorgungsnetze angewandt. Die Adaption von Security Information & Event Management (SIEM) Systemen an Low-Latency-Anforderungen und neuartige Bedrohungen ist Gegenstand eines Projekts zur Analyse und Absicherung von 6G-Mobilfunknetzen. Ein Transfer der Forschungsergebnisse in die Praxis wurde auch im Rahmen von dtec.bw-Projekten erzielt: Beispielsweise wurden im Rahmen einer Kooperation mit dem Landkreis Bad Kissingen erste Komponenten eines Sturzflut-Frühwarnsystems in Betrieb genommen. In Zusammenarbeit mit der Gemeinde Neuhaus und Katastrophenschutz sowie Blaulichtorganisationen wurden die Eckdaten für eine abgesicherte Krisenkommunikationsinfrastruktur auf Basis von Commercial-off-the-Shelf-IoT-Komponenten festgelegt.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 7355

www.unibw.de/software-security



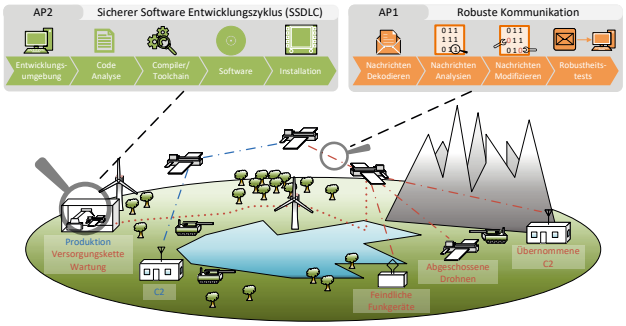
Forschungsschwerpunkte der Professur „IT-Sicherheit von Software und Daten“.

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

Projekt ACSE

Airborne Cybersecurity Enhancement

Das Projekt Airborne Cybersecurity Enhancement (ACSE) ist eine Forschungskooperation zwischen dem FI CODE und Airbus Defence and Space (Airbus). Unser Team befasst sich zum einen mit der Netzsicherheit für interne und externe Kommunikation von Luftfahrzeugen und zum anderen mit der sicheren Softwareentwicklung in der Avionik und steht dabei in engem Austausch mit aktuellen Airbus-Projekten.



In ACSE betrachtete Angriffsvektoren auf Luftfahrzeuge.

Sicherheit in Kommunikationsnetzen

Ziel des Teilprojektes ist es, eine Möglichkeit zu schaffen, Kommunikationsprotokolle, wie sie in der Avionik verwendet werden, hinsichtlich möglicher Schwachstellen zu analysieren und neue Protokolle zu prototypisieren.

Hinführend dazu wurde zuerst eine umfangreiche Analyse verschiedener aktuell verwendeter interner und externer Kommunikationsprotokolle durchgeführt, wobei im Anschluss auch Kommunikationsprotokolle, die potenziell in der Luftfahrt eingesetzt werden könnten, aus anderen Domänen einbezogen wurden. Dabei wurden die Protokolle nach einem einheitlichen System bewertet und Anwendungsgebiete sowie mögliche Schwachstellen herausgestellt. Basierend auf dieser allgemeinen Einordnung wurden dann Teile konkreter Avionik-Architekturen betrachtet und Vorschläge zu deren Härtung erarbeitet.

Mithilfe dieses Wissens sowie einer Untersuchung des State-of-the-Art zur Analyse und Interaktion mit Protokollen auf allen ISO-OSI-Ebenen für kabelgebundene und Funkkommunikation wurde ein Werkzeug entwickelt, das es erlaubt, mit verschiedensten Schnittstellen zu interagieren, um diese zu testen. Ein Hauptaugenmerk lag auf der Reduzierung des Initialaufwandes für die Integration neuer Protokolle durch das Ausnutzen von Airbus intern bereits vorliegenden Protokollspezifikationen. Durch die erreichte Flexibilität eignet sich das Werkzeug auch für die Prototypisierung von Protokolländerungen oder gänzlich neuen Protokollen.

Sicherheit in der Softwareentwicklung

In diesem Teilprojekt wurde untersucht, wie der Entwicklungsprozess von Software für Avionik-Systeme angepasst werden kann, um neben den bereits bestehenden umfangreichen Normen und Anforderungen der Luft- und Raumfahrt zusätzlich noch Cybersicherheit zu betrachten.

Auf konzeptioneller Seite wurde ein „Sicherer Softwareentwicklungslebenszyklus“ (SSDLC) entwickelt, der die existierenden, primär der Lufttüchtigkeit geschuldeten Anforderungen sowie die aktuellen Entwicklungsprozesse bei Airbus aufnimmt und mit Bausteinen zur Erhöhung der Cybersicherheit erweitert.

Ein konkreter Baustein zur Erhöhung der Cybersicherheit ist die Verwendung von Softwareanalysewerkzeugen. In diesem Teilprojekt wurde betrachtet, wie bestimmte in der Luft- und Raumfahrt verwendete Programmiersprachen sowie Programmierregeln mit solchen Werkzeugen geprüft werden können und welche Kategorien von Fehlern und einhergehenden Schwachstellen damit vermieden werden können.

Alexander Frank
+49 89 6004 2745
alexander.frank@unibw.de
https://go.unibw.de/acse

Gefördert durch:
Airbus Defence and Space

ABB.: FI CODE / ALEXANDER FRANK

Projekt 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 transdisziplinären Forschungsprojekts stehen für die Forschungsgruppe dabei die Themen selbstbestimmtes (engl. self-sovereign) Identitätsmanagement, elektronische Signaturen und die technische Unterstützung der Projektpartner im Mittelpunkt.

DIGITALE IDENTITÄTEN sind ein zentraler Baustein des zunehmend digitalisierten Alltags. In diesem Kontext trägt das Arbeitspaket im Projekt LIONS dazu bei, nicht nur technische Aspekte von Identitätsmanagementsystemen, sondern auch die Verknüpfung zu Themen aus der Psychologie und Mensch-Maschine-Interaktion zu betrachten.

Selbstbestimmtes Identitätsmanagement

Als Beitrag zu mehr Transparenz und Datenschutz im Umgang mit personenbezogenen Daten, werden durch das selbstbestimmte Identitätsmanagement die Nutzenden zentral in die Verwaltung ihrer Identitätsdaten eingebunden.

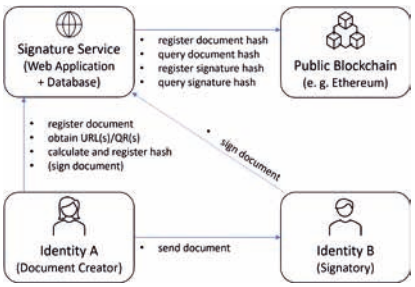
Dadurch entstehen sowohl technische Herausforderungen in der adäquaten Sicherung dieser Daten als auch organisatorische Hürden beim Austausch und der Akzeptanz von Identitätsdaten.

Zusätzlich werden Fragestellungen untersucht, die den Umgang der Nutzenden mit den Identitäts-Wallets analysieren.

Dabei werden die technischen Vorteile des Systems der fast vollständigen Übertragung der Verantwortung für die sichere Verwendung der Identitätsdaten auf die Nutzenden gegenübergestellt.

Elektronische Signaturen

Im Rahmen des Identitätsmanagements spielen digitale Signaturen als kryptografisches Beweismittel der Identität eine entscheidende Rolle. Gleichzeitig sind sie zusammen mit den Identitäten selbst Grundlage für elektronische Signaturen, welche für digitalisierte Geschäftsprozesse ein unverzichtbarer Bestandteil sind.



LIONS-Architektur für digitale Signaturdienste.

Im Rahmen des Projektes werden verschiedene Konzepte zum Austausch signierter Daten und Dokumente entwickelt, prototypisch entwickelt und demonstriert. Hierzu wurde der direkte Datenaustausch zwischen zwei Identitäten bzw. deren Mobilgeräten mittels einer Modifikation eines standardisierten Datenformats anhand von Szenarien aus dem Healthcare-, sowie aus dem militärisch-organisatorischen Bereich untersucht. Für beide Szenarien wurden die benötigten Anwendungen und Bibliotheken implementiert, getestet und auf Konferenzen vorgestellt.

Weiterhin wurde ein Konzept für ein Web- und Ethereum-basiertes System für elektronische Signaturen entwickelt und prototypisch implementiert, welches sich vor allem auf Aspekte wie Benutzerfreundlichkeit, Vertrauenswürdigkeit, Datenschutz und eine erhöhte Souveränität konzentriert. Bei diesem System wird die öffentliche Blockchain verwendet, um die Daten beweisbar zu machen, ohne dabei in Konflikt mit dem Datenschutz zu kommen. Dabei werden auch neue Methoden zur Signaturplatzierung auf dem Dokument evaluiert. In diesem Kontext wurde auch eine empirische Studie vorbereitet, die bestehende und neue Konzepte auf Vertrauenswürdigkeit und Akzeptanz untersuchen soll.

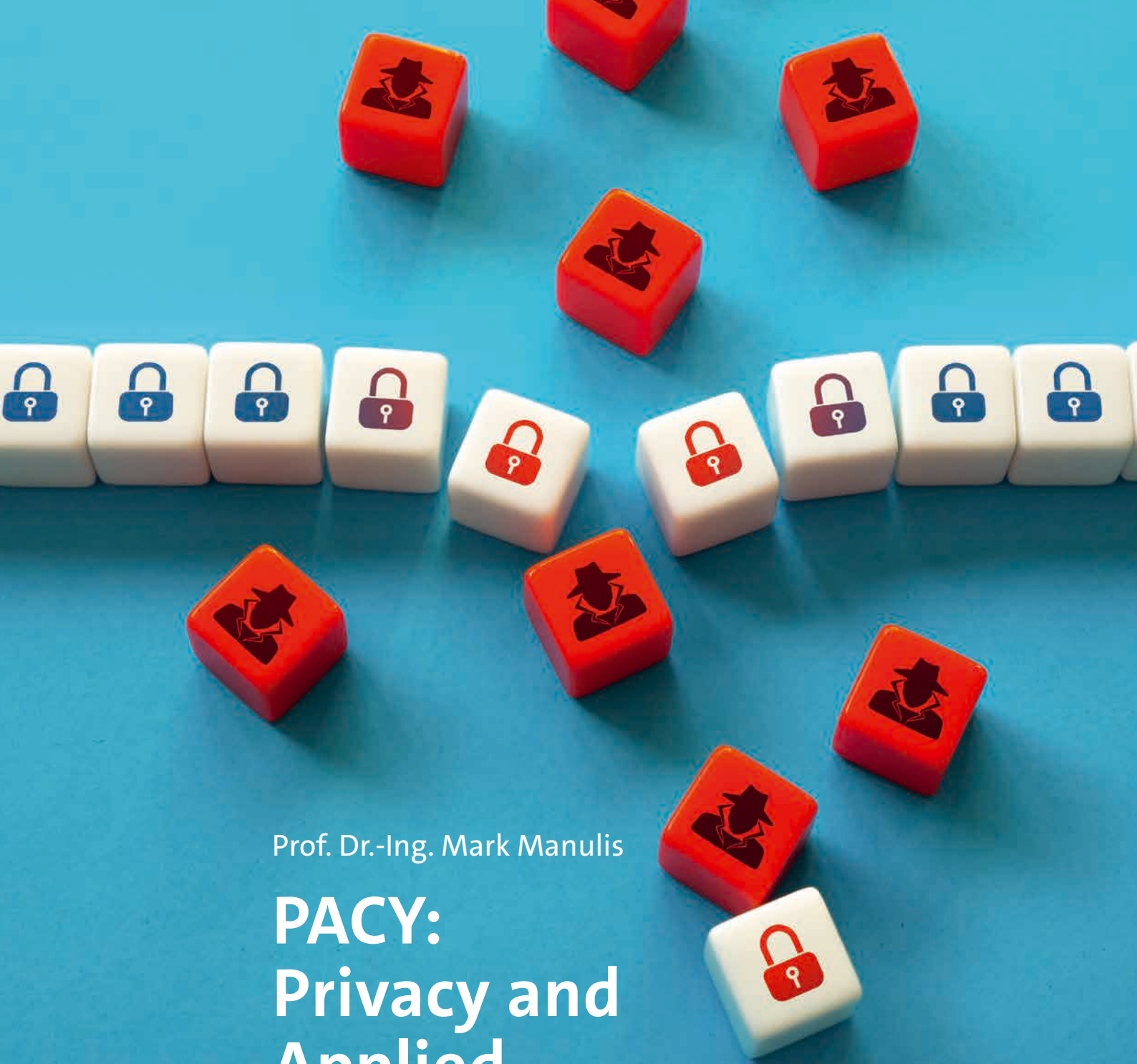
Dr. Michael Grabatin
michael.grabatin@unibw.de
+49 89 6004 3992
https://www.unibw.de/lions

Gefördert durch:

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

ABB.: FI CODE / MICHAEL HOFMEIER



Prof. Dr.-Ing. Mark Manulis

PACY: 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: Authentifizierung 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 Nicht-verfolgbarkeit 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

ARKG: Asynchrone Remote-Schlüsselerzeugung

Verkapselung von kryptographischen Schlüsselpaaren für Public-Key-Kryptosysteme

Die von PACY Lab in Zusammenarbeit mit Yubico im Jahr 2020 eingeführte Asynchronous Remote Key Generation (ARKG) wurde ursprünglich entwickelt, um die Sicherung von Sicherheitsschlüsseln für Webkonten zu ermöglichen, die durch den WebAuthn-/FIDO2-Standard geschützt sind. Seitdem hat sich ARKG als eigenständiger Baustein für andere Anwendungen der delegierten und Privatsphäre schützenden Authentifizierung bewährt.

Unterschied zwischen ARKG und Standard-Schlüsselkapselungsmechanismen

Bei traditionellen Schlüsselkapselungsmechanismen (KEM) verwendet der Sender den öffentlichen Schlüssel des Empfängers, um einen symmetrischen kryptographischen Schlüssel K zu kapseln. Der vorgesehene Empfänger kann K mit seinem eigenen privaten Schlüssel entkapseln. KEMs werden heute etwa beim Aufbau von sicheren Kanälen verwendet.

Im Gegensatz zu KEMs erlaubt ARKG dem Sender, das gesamte asymmetrische Schlüsselpaar (sk, pk) für den beabsichtigten Empfänger zu kapseln, so dass nur der Empfänger (und nicht der Sender) den privaten Schlüssel sk erfährt. Dadurch kann der Empfänger (sk, pk) als sein eigenes, frisch generiertes Schlüsselpaar in Public-Key-Kryptosystemen verwenden. ARKG hat sich bisher als vielseitiger Baustein erwiesen, der eine Reihe unterschiedlicher Anwendungen im Rahmen der delegierten oder verzögerten Authentifizierung ermöglicht.

ARKG für Pairing basierte und Postquantensichere Kryptosysteme

PACY Lab arbeitet weiter an neuen ARKG Designs. Die ursprüngliche

Version des ARKG-Protokolls war für diskrete logarithmusbasierte Schlüsselpaare konzipiert und konnte daher nur in einschlägigen Kryptosystemen wie ECDSA-Signaturen oder ElGamal-Verschlüsselung verwendet werden. Unsere letzten ARKG-Konstruktionen haben den Anwendungsbereich von ARKG auf andere Arten von Schlüsselpaaren erweitert, die in der modernen Kryptographie häufig verwendet werden.

Unsere Veröffentlichung in ACNS 2023 beschreibt einen allgemeinen Ansatz zur Erzeugung von ARKG-Schlüsselpaaren, die mit vielen Pairing basierten Kryptosystemen kompatibel sind. Beispielsweise können Instanzen unseres Protokolls Schlüssel generieren, die mit speziellen digitalen Signaturverfahren wie den Verfahren von Pointcheval und Sanders bzw. von Camenisch und Lysyanskaya kompatibel sind, die in Anonymen-Credential-Systemen verwendet werden. Eine weitere Instanz des Protokolls kann Schlüssel für Stealth-Adressen generieren, die auf BLS-Signaturen basieren und für die Empfängeranonymität in Blockchain-Transaktionen verwendet werden können.

Unser Veröffentlichung in IEEE EuroS&P 2023 stellt ein postquantensicheres ARKG-Protokoll vor, welches zur Erzeugung von Schlüsselpaaren verwendet werden kann, die mit einer Reihe von gitterbasierten Kryptosystemen kompatibel sind, darunter Kyber und Dilithium, die vom NIST als künftige Standards in der Post-Quantum-Kryptografie ausgewählt wurden.

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 durchsuchbare Verschlüsselung

Ermöglichung aussagekräftiger Suchanfragen über ausgelagerte verschlüsselte Daten.

Die durchsuchbare Verschlüsselung ermöglicht es Nutzern, vertrauliche Daten in verschlüsselter Form in einen Cloud-Speicher auszulagern und später private Suchvorgänge durchzuführen, ohne dem Cloud-Anbieter die Vertraulichkeit ihrer Daten anzuvertrauen.

Herausforderungen bei der Suche in verschlüsselten Daten

Die Auslagerung der Datenspeicherung bietet eine effiziente Möglichkeit für Kunden mit begrenzten Ressourcen, große Mengen verschlüsselter Daten zu verwalten und zu verbreiten. Herkömmliche Verschlüsselungsmethoden mit öffentlichen oder privaten Schlüsseln, die die Vertraulichkeit der Daten im Ruhezustand schützen können, behindern jedoch die Möglichkeit, bestimmte Datensegmente gezielt zu suchen und abzurufen.

Eine durchsuchbare Verschlüsselung (Searchable Encryption, SE) zielt darauf ab, diese Einschränkungen zu überwinden. SE ermöglicht es den Nutzern, verschlüsselte Daten sicher in einen Cloud-Speicher auszulagern und später Suchvorgänge in diesen Daten durchzuführen, ohne den Cloud-Anbieter über die gesuchten Inhalte zu informieren. SE kann als Teil des neuen Paradigmas Rechnens auf verschlüsselten Daten betrachtet werden, bei dem Cloud-Dienste mit Vertraulichkeit der Daten oder der Verwaltung privater Schlüssel nicht vertraut werden müssen.

Aufbau durchsuchbarer Verschlüsselungssysteme

Bei der Entwicklung moderner SE-Ansätze mit öffentlichen Schlüsseln ist die so genannte Key-Policy Attribute-Based Encryption (KP-ABE) ein wichtiger Baustein. In einem KP-ABE-Schema hat jeder private Schlüssel eine eingebettete Zugriffsrichtlinie und kann zur Entschlüsselung von Chiffretexten verwendet werden, die wiederum Attribute einbetten, für die die Zugriffsrichtlinie erfüllt ist. Beispielsweise kann ein Chiffretext, der die Attribute Offizier und Bundeswehr enthält, durch einen privaten Schlüssel mit eingebetteten Zugriffsregeln wie Offizier ODER Bundeswehr oder Offizier UND Bundeswehr entschlüsselt werden. KP-ABE kann zur Konstruktion eines SE-Schemas verwendet werden, indem in Chiffretexte eingebettete Attribute als Schlüsselwörter betrachtet werden, die von Suchanfragen verwendet werden können, während die Suchanfragen als in private Schlüssel eingebettete Zugriffsrichtlinien betrachtet werden können. Um sicherzustellen, dass die Schlüsselwörter vertraulich bleiben, muss eine spezielle Variante der so genannten anonymen KP-ABE-Verfahren verwendet werden.

ABB.: : GENERIERT BY DALL-E 3

PACY Lab erforscht effiziente SE-Verfahren, die in der Lage sind, aussagekräftige Suchanfragen zu verarbeiten, um den praktischen Einsatz in realen Anwendungen zu ermöglichen. In Zusammenarbeit mit der University of Surrey (GB) haben wir das bisher effizienteste anonyme KP-ABE-Verfahren entwickelt sowie ein schnelles und ausdrucksstarkes SE-Verfahren namens FEASE, welches eine bessere Leistung und Skalierbarkeit im Vergleich zu den modernsten SE-Verfahren mit öffentlichen Schlüsseln erreicht. Diese Arbeit wird auf Usenix Security 2024 veröffentlicht.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

Die Forschungsgruppe Artificial Intelligence & Machine Learning (AIML) unter der Leitung von Prof. Eirini konzentriert sich auf die Entwicklung intelligenter, datenbasierter Algorithmen zur Bewältigung gesellschaftlicher Herausforderungen. Aktuelle Forschungsrichtungen sind: a) kontinuierliches Lernen und Vergessen, b) verantwortungsvolle KI mit Schwerpunkten Fairness, Erklärbarkeit und Robustheit, und c) generative KI für bessere Datenqualität.

Kontinuierliches Lernen

Zahlreiche Anwendungen wie soziale Medien und Produktionsprozesse, erzeugen dynamische, kontinuierlich eintreffende Daten. Dies erfordert eine Weiterentwicklung traditioneller Trainingsroutinen hin zu kontinuierlichem Lernen, bei dem sich Modelle stetig anpassen, weiterentwickeln, und vergessen können. Der Schwerpunkt liegt auf der Entwicklung intelligenter Algorithmen und Modelle, die dabei Anforderungen beispielsweise hinsichtlich Speicherverbrauch und Reaktionszeit berücksichtigen. Die Forschungsgruppe befasst sich mit der Aktualisierung von ML-Modellen mit neuen Daten, der Verwaltung bestehender Informationen, um katastrophales Vergessen zu verhindern, und der Überwachung und Erklärung von Veränderungen im Laufe der Zeit. Diese Forschungsrichtung ist in Projekten wie OSCAR, das sich auf Textdatenströme konzentriert, und HEPHAESTUS, das sich auf Produktionsdatenströme konzentriert, vertreten.

Verantwortungsvolle KI

KI-gestützte Systeme werden heute in großem Umfang eingesetzt, um Entscheidungen mit weitreichenden Auswirkungen zu treffen, wodurch Fragen mit Bezug zu Menschenrechten aufgeworfen werden. Um eine verantwortungsvolle Entwicklung und den Einsatz solcher Systeme zum Wohle der Gesellschaft zu gewährleisten, sind traditionelle Algorithmen die ausschließlich für die Vorhersageleistung optimiert sind nicht ausreichend. Zusätzlich müssen ethische und rechtliche Grundsätze in das Design, das Training und den Einsatz von KI-Systemen integriert werden. Unsere Forschung konzentriert sich auf die Behandlung von Vorurteilen und Diskriminierung in KI-Systemen, erklärbare KI (XAI) und Robustheit. Beim fairnessbewussten Lernen erforschen wir Multi-Fairness unter Einbezug ungleicher Verfügbarkeit von Daten für verschiedene Teilgruppen. Im Bereich XAI untersuchen wir kontrafaktische Erklärungen und die Modellierung von Unsicherheiten, während wir im Bereich Robustheit die Generalisierung von Modellen verbessern und Modelle gegen feindliche Angriffe stärken. Diese Forschungsrichtung ist in Projekten wie NoBIAS und MAMMoth vertreten, die sich auf Fairness konzentrieren, sowie bei STELAR, das sich auf robustes Verhalten gegen Diskriminierungsursachen konzentriert.

Generative KI

KI kann mittlerweile neben der Analyse historischer Daten auch neuartige Texte, Bilder und Tabellendaten generieren. Generative KI hat das Potenzial, für die Gesellschaft von Nutzen zu sein, indem sie Ingenieure beim Produktdesign unterstützt, zu neuen Kreationen inspiriert und zur Generierung von Inhalten beiträgt. Allerdings müssen Herausforderungen wie Sicherheitsprobleme, vorurteilsbehaftete Inhalte, Urheberrechtsfragen, sowie Grenzen künstlicher Kreativität angegangen werden. Die Forschungsgruppe setzt generative KI ein, um Probleme der Datenqualität, etwa in Form vorhandener Ungleichgewichte und verzerrter Verteilungen, zu lösen. Darüber hinaus wird das Potenzial generativer KI zur Generierung neuer nützlicher Datensätze erforscht. Diese Forschungsrichtung ist in Projekten wie dem SFB1463 vertreten, welcher sich auf das Design von Offshore-Windturbinen durch eine Kombination von Simulation, analytischen und datengesteuerten Modellen konzentriert.

Entwicklung der Forschungsgruppe

Im Jahr 2023 hat sich die Forschungsgruppe um sechs Promovierende und einen Postdoc vergrößert, während einige Mitglieder in Berlin (an der Freien Universität) und Hannover (an der Leibniz Universität/L3S Research Centers) bleiben, wo Prof. Dr. Ntoutsi zuvor tätig war.

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

https://www.unibw.de/aiml

ABB.: ADOBE STOCK / PARRADEE; ADOBE STOCK / THITICHAYA

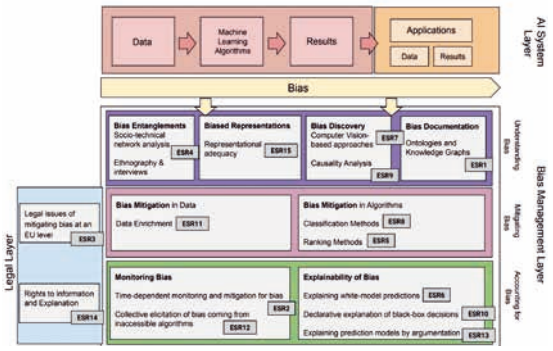
Projekt NoBIAS

Diskriminierungsfreie Künstliche Intelligenz

Im Rahmen von NoBIAS erforschen und entwickeln wir innovative Methoden für eine vorurteilsfreie KI-Entscheidungsfindung. Das Projekt zielt darauf ab, eine Kohorte von 15 Forschern darin zu befähigen, voreingenommene und diskriminierende KI-Entscheidungen zu erkennen, und Lösungen anzubieten, die das Potenzial von KI unter rigoroser Einhaltung rechtlicher und sozialer Normen maximal ausschöpft.

KI: Potenziale erschließen und Risiken mindern

KI-basierte Algorithmen werden in großem Umfang von Unternehmen, Regierungen und verschiedensten Organisationen eingesetzt, um Entscheidungen mit weitreichenden Auswirkungen auf Einzelpersonen und die Gesellschaft als Ganzes zu treffen. Während diese Algorithmen zwar Lösungen für Probleme bieten, bergen sie auch Risiken, da sie unter anderem zu Diskriminierung führen können, beispielsweise in der Stellenvergabe oder bei medizinischer Behandlung. Dokumentierte Diskriminierung verschiedener Bevölkerungsgruppen durch KI haben Bedenken hinsichtlich der gesellschaftlichen Auswirkungen der Technologie geweckt. Diese Bedenken müssen ausgeräumt werden, damit KI zum gesellschaftlichen Wohl beitragen und gleichzeitig ihr Potenzial ausschöpfen kann. Verantwortungsvolle Entwicklung und verantwortungsvoller Einsatz von KI spielen eine entscheidende Rolle bei der Gewährleistung ethischer Nutzung, dem Aufbau von Vertrauen und der Schaffung von Zurechenbarkeit beim Einsatz dieser leistungsstarken Technologie.



Überblick über die NoBIAS-Forschungsagenda.

Ein ganzheitlicher Ansatz zur Bekämpfung von Vorurteilen in KI-Systemen

Bei NoBIAS liegt das Hauptaugenmerk auf der Bekämpfung von Vorurteilen und Diskriminierung in KI-Systemen. Unsere Forschungsgruppe verfolgt einen ganzheitlichen Ansatz, der die gesamte KI-Entscheidungspipeline umfasst. Das übergeordnete Ziel ist es, Ursachen und Formen von Diskriminierung zu verstehen, und deren Auswirkungen zu mindern. Ermöglicht wird dies durch einen interdisziplinären Ansatz, der Informatik, Recht und Soziologie miteinander verbindet, sowie durch eine koordinierte Reihe von Einzelprojekten, die eine globale Vision für vorurteilsbewusste KI-Systeme verfolgen.

Hauptziele:

1. Verständnis der Entstehung von Voreingenommenheit in der Gesellschaft, ihres Einzugs in soziotechnische Systeme, ihrer Manifestation in den von KI-Algorithmen verwendeten Daten und ihrer Modellierung und formalen Definition.
2. Entwicklung von Methoden und Techniken zur Abschwächung von Voreingenommenheit von Daten, Algorithmen und Modellen in KI-Entscheidungsfindungsprozessen.
3. Nutzung proaktiver Methoden wie vorurteilsvermeidende Datenerfassung und rückwirkende Ansätze wie das Erklären von KI-Entscheidungen in menschlichen Begriffen (XAI), um gegen diskriminierende Ergebnisse anzugehen.

Das interdisziplinäre NoBIAS-Konsortium besteht aus acht, über fünf europäische Staaten verteilte Organisationen, inklusive einer nicht-akademischen, die über führende Expertise in KI, Recht und Soziologie verfügen. Ergänzt wird das Netzwerk durch verschiedene assoziierte nicht-akademische Partner aus unterschiedlichen Anwendungsbereichen wie Banken und dem Gesundheitswesen.

NoBIAS

Prof. Dr. Eirini Ntoutsi
eirini.ntoutsi@unibw.de
+49 89 6004 7420
https://nobias-project.eu/

ABB.: FI CODE / NTOUTS

Gefördert durch: European Union's Horizon 2020 research and innovation programme under the **Marie Skłodowska-Curie** grant agreement no. 860630.

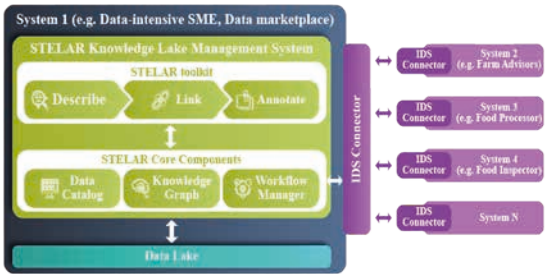
Projekt STELAR

Räumlich-zeitlich verknüpfte Datenwerkzeuge für den AgRi-Lebensmittel-Datenraum

STELAR entwickelt ein innovatives Knowledge Lake Management System (KLMS), um hochwertige, zuverlässig gelabelte, und vorurteilsvermeidende Daten bzw. Datenverarbeitung im Agrar- und Ernährungssektor zu fördern. Pilotprojekte betreffen Risikoprävention in der Lebensmittelversorgung, frühzeitige Vorhersage des Pflanzenwachstums, sowie zeitnahe Eingriffe im Rahmen von Präzisionslandwirtschaft.

KI in der Landwirtschaft

KI revolutioniert die Landwirtschaft, verbessert die Effizienz, die Präzision und die Entscheidungsfindung, leitet damit einen bedeutenden Wandel in diesem Sektor ein und ebnet den Weg für eine nachhaltigere und produktivere Zukunft. Trotz dieser Fortschritte stellt die Bewältigung der Komplexität des Agrar- und Ernährungssektors eine Herausforderung dar. Dazu gehören die Integration verschiedener Datenquellen, die Bewältigung verzerrter Datenerhebung und Probleme mit der Datenqualität, die Verwaltung großer Datenmengen, die von Sensoren, Satelliten und anderen Quellen erzeugt werden, und die enorme Vielfalt nachgelagerter Aufgaben und Anwendungen. Im Rahmen von STELAR wird ein Knowledge Lake Management Systems (KLMS) für den Agrar- und Lebensmittelbereich entwickelt, das eine intelligente Entdeckung, semantische Interoperabilität und die Bereitstellung KI-fähiger Daten ermöglicht und Anwendungen in der intelligenten Landwirtschaft und Lebensmittelsicherheit unterstützt.



Übersicht von STELAR KLMS.

Hauptziele:

1. Optimierung der Datenermittlung und -wiederverwendung durch Automatisierung der Extraktion detaillierter Metadaten, einschließlich bereichsspezifischer Indikatoren und Berichte, zur Verbesserung energieeffizienter Analysen großer Datenmengen.
2. Verbesserung der Verknüpfung von Daten, um Beschreibungen zu erweitern, Einheiten zu assoziieren und den Abgleich auf einer Schema- und Instanzebene, sowie einen räumlich-zeitlichen Abgleich zu ermöglichen.
3. Verbesserung der Datenannotation und der Generierung synthetischer Daten durch fortgeschrittene Lerntechniken und Mechanismen für Erklärbarkeit, Erkennung und Abschwächung von Datenverzerrungen sowie Behebung von Label- und Datenknappheit.

Das KLMS wird in Pilotversuchen an realen Anwendungsfällen in der Agrar- und Ernährungswirtschaft getestet, insbesondere zur Risikoprävention bei der Lebensmittelversorgung, zur frühzeitigen Vorhersage des Pflanzenwachstums und hinsichtlich frühzeitiger Interventionen in der Präzisionslandwirtschaft. Der Fokus liegt in erster Linie darauf, die KI-Datenqualität für verschiedene nachgelagerte Aufgaben zu verbessern und die Modellverallgemeinerung über verschiedene Kontexte (Raum, Zeit, Wetter, Kulturpflanzen usw.) hinweg zu erleichtern. Dies beginnt mit der Analyse von KI-Pipelines, um Quellen möglicher datengetriebener Verzerrungen zu identifizieren und ihre Auswirkungen auf nachgelagerte Aufgabenmodelle zu verstehen. Im Anschluss an diese Analyse wird generative KI zur Verbesserung der Datenqualität verwendet und erklärbare KI (XAI) eingesetzt, um sicherzustellen, dass die Modelle korrekte Informationen lernen.

Prof. Dr. Eirini Ntoutsi
eirini.ntoutsi@unibw.de
+49 89 6004 7420

Dr. Vivek Kumar
vivek.kumar@unibw.de
https://stelar-project.eu/

Gefördert durch: EU as part of the call for proposals HORIZON-CL4-2021-DATA-01-03 – Technologies for data management (IA)

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.

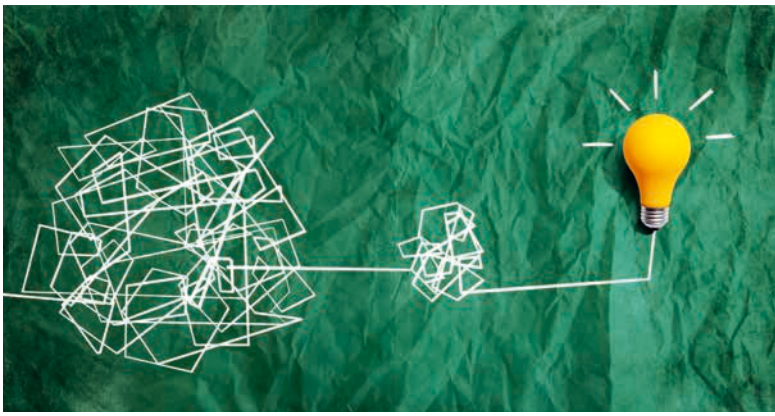
Stärkere Sicherheit – Quantencomputer und mehr

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 (sogenannte 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 2023 wurde Prof. Slamanig eingeladen in Programmkomitees folgender internationaler Top Konferenzen zu dienen: Annual International Cryptology Conference (CRYPTO 2024), Annual ACM Conference on Computer and Communications Security (ACM CCS 2023 und ACM CCS 2024), Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2023). An der ACM CCS 2023 erhielt er einen Top Reviewer Award, der die konstruktivsten 10% unter den Mitgliedern des Programmkomitees auszeichnet.

Entwicklung der Forschungsgruppe

Das QuSAC Lab wurde im November 2023 gegründet und die ersten beiden Doktoranden haben mit Dezember ihre Arbeit aufgenommen. Mit Februar 2024 wird das Lab zusätzlich durch einen Postdoktoranden verstärkt. Die Gruppe ist wissenschaftlich sowohl national wie auch international stark vernetzt und pflegt zahlreiche Kooperationen. Zudem sind zukünftige kooperative Projekte in Planung, die weiter zum Wachstum des QuSAC Labs beitragen werden.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

www.unibw.de/crypto

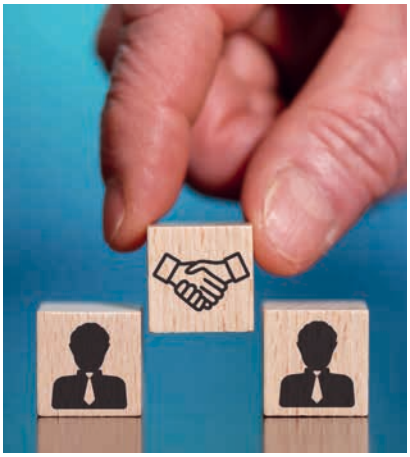
ABB.: ADOBE STOCK / ANNIKA; ADOBE STOCK / TIERNEY

Feingranulare Vorwärtssicherheit durch punktierbare Verschlüsselung

Wie lässt man kryptographische Schlüssel die Fähigkeit zum Entschlüsseln vergessen?

Verschlüsselung bietet nur dann Sicherheit, wenn geheime Schlüssel auch geheim gehalten werden. Da die sichere Verwaltung von Schlüsseln eine notorisch schwierige Aufgabe darstellt, ist es zu optimistisch, davon auszugehen, dass sie niemals bekannt werden. Zudem müssen sensible Informationen oft über einen langen Zeitraum geschützt werden. Hier können Verschlüsselungsverfahren mit stärkeren Sicherheitseigenschaften Abhilfe schaffen.

ZUR DEFINITION der Sicherheit von Verschlüsselungsverfahren gibt es einen gut untersuchten formalen Rahmen. Mit Methoden der beweisbaren Sicherheit können wir dann auch mathematisch deren Sicherheit beweisen.



Moderne Anwendungen stellen Verschlüsselungslösungen auf die Probe.

Verschlüsselung und das „Durchsickern" von Schlüsseln

Sie bieten jedoch nur dann Sicherheit, wenn die geheimen Schlüssel dem Angreifer nicht bekannt sind. Heutzutage werden verschlüsselte Daten über öffentliche Netze ausgetauscht und häufig auf Servern Dritter (z. B. in der Cloud) gespeichert. Da Speicherplatz günstig ist, muss man davon ausgehen, dass die Daten lange gespeichert werden (z. B. in Backups) oder sogar während der Übertragung aufgezeichnet werden, wie es die Snowden-Leaks nahelegen. Da die sichere Verwaltung von kryptographischen Schlüsseln eine notorisch schwierige Aufgabe ist, scheint es zu optimistisch anzunehmen, dass geheime Schlüssel niemals „durchsickern" werden. Vor allem da sensible Informationen oft mehrere Jahrzehnte lang geschützt werden müssen.

Das Schützen von Daten in die Zukunft

Die Eigenschaft die verschlüsselte Daten schützt, die vor dem Bekanntwerden eines geheimen Schlüssels erzeugt wurden, wird Vorwärtssicherheit genannt. Sie ist bei interaktiven Schlüsselaustauschprotokollen gut untersucht und in wichtigen Verschlüsselungsprotokollen wie TLS 1.3 obligatorisch. Sobald man jedoch Interaktion verbietet, ändert sich das Bild. Dies gilt z. B. für asymmetrische Verschlüsselung oder Schlüsselaustauschprotokolle die niedrige Latenz (so genannte 0-RTT) erfordern.

Punktieren von Schlüsseln

Vorwärtssicherheit bietet hier die so genannte punktierbare Verschlüsselung. Sie ermöglicht es, den geheimen Schlüssel sehr feingranular, d.h. auf Chiffretexte, zu punktieren. Ein Schlüssel, der für einen Chiffretext punktiert wurde, kann diesen nicht mehr entschlüsseln. Folglich gefährdet das Bekanntwerden des Schlüssels die geschützte Nachricht nicht. Mitglieder des QuSAC-Labs haben das erste effiziente Verfahren (Bloom Filter Encryption) und verschiedene algorithmische Optimierungen entwickelt. Zudem haben Sie einen generischen Ansatz, solche Schemata aus Post-Quantum-Annahmen zu konstruieren, sowie verschiedene Verallgemeinerungen dieser Verfahren entwickelt. Erwähnenswert ist zudem die Betrachtung so genannter aktualisierbarer Verschlüsselung, ein Ansatz zur Rotation von Schlüsseln für ausgelagerte verschlüsselte Daten, ohne dass alle Daten heruntergeladen, neu verschlüsselt und wieder hochgeladen werden müssen, aus der Perspektive der Punktierbarkeit. Letzteres ermöglicht die Konstruktion solcher Systeme mit starken Vorwärtssicherheitsgarantien. Trotz bedeutender Fortschritte gibt es noch viele interessante offene Fragen in diesem Feld.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

Stärken von nicht-interaktiven Zero-Knowledge-Beweisen

Nicht-interaktive Zero-Knowledge-Beweise fit für praktische Anwendungen

Zero-Knowledge-Beweise (ZKPs) ermöglichen es einer Partei (dem Prover) interaktiv eine andere Partei (den Verifier) von der Richtigkeit einer Aussage zu überzeugen, ohne Information darüber preiszugeben, z. B. den Beweis, dass man ein Sudoku-Rätsel gelöst hat, ohne dessen Lösung preiszugeben. In den letzten Jahren haben wir eine „kambrische Explosion" in der Forschung und Praxis erlebt, wobei letzteres zahlreiche Forschungsfragen aufwirft.

ZKPS WURDEN Mitte der 1980er Jahre entwickelt. Eine wichtige Variante sind nicht-interaktive ZKPs (NIZK). Hier besteht der Beweis aus einer einzigen Nachricht des Provers und kann von jedem verifiziert werden. Dieses Feature hat jedoch den Nachteil, dass eine vertrauenswürdige Instanz vorab Parameter generieren und allen Parteien bereitstellen muss.

Wachsendes Interesse an Zero-Knowledge-Beweisen

Lange Zeit waren ZKPs von theoretischem Interesse, und der praktische Nutzen begrenzt. Mit der wachsenden Popularität von Kryptowährungen und Blockchains hat sich dieses Bild drastisch geändert. Speziell für reale Anwendungen gilt das Interesse NIZK mit kompakten Beweisen, den sogenannten zk-SNARKs.

Zwei zentrale Eigenschaften von NIZK-Beweisen

Die Zero-Knowledge-Eigenschaft verlangt, dass Beweise keine Information über den so genannten Zeugen preisgeben, den der Prover benötigt, um den Verifier von seiner Aussage zu überzeugen. Die Soundness-Eigenschaft stellt sicher, dass ein Verifier keine Beweise für falsche Aussagen akzeptiert. Man benötigt aber typischerweise die stärkere Knowledge-Soundness Eigenschaft. Sie sagt aus, dass der Prover den Zeugen tatsächlich kennen und nicht nur seine Existenz beweisen muss. Aber wenn NIZK in der freien Wildbahn verwendet werden, reicht auch das nicht. Man benötigt die so genannte Simulation-Extractability (SE). Sie garantiert, dass aus existierenden Beweisen keine anderen gültigen Beweise erzeugt werden können. Dies ist wichtig für diverse Kryptowährungs-Anwendungen, da ein Angreifer sonst neue Coins aus dem Nichts generieren könnte. Eine weitere Anwendung sind Signaturverfahren, wo Mitglieder des QuSAC-Labs gezeigt haben, wie man quantensichere Verfahren aus bestimmten SE NIZK konstruieren kann.

Kenntnis von Puzzle-Lösungen beweisen, ohne sie zu verraten.

Formale Beweise der SE-Eigenschaft sind oft sehr aufwendig. Mitglieder des QuSAC Labs haben Methoden entwickelt, die es generisch ermöglichen, NIZK-Beweise oder zk-SNARKs, die nur (Knowledge-)Sound sind, in SE-Beweise zu „heben", ohne die Effizienz zu sehr zu beeinträchtigen. Letzteres ist besonders wichtig für zk-SNARKs, bei denen Kompaktheit und Effizienz eine wichtige Rolle spielen.

Die vertrauenswürdige Instanz in der realen Welt

Erfolgt die Erstellung der initialen Parameter in böser Absicht, verlieren NIZK ihre Sicherheit. In der Theorie kann man eine vertrauenswürdige Instanz annehmen. Jedoch gibt es in vielen praktischen Anwendungen keine solche Partei. Eine wichtige Forschungsfrage ist die Entwicklung von NIZK, deren Sicherheit bestehen bleibt, auch wenn die Parametergenerierung bösartig erfolgt. Hier haben Mitglieder des QuSAC Labs einen umfangreichen Beitrag geleistet. Es bleiben aber noch viele interessante Fragen offen.

Prof. Dr. Daniel Slamanig
daniel.slamanig@unibw.de
+49 89 6004 7430

ABB.: ADOBE STOCK/ GOKHAN

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 Pentesting, Datenschutz, Privacy Enhancing Technologies, 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 Kryptografie sowie Kenntnisse über die verschiedenen Verfahren zur sicheren Datenübertragung in modernen Kommunikationsnetzen.

Forschung

Ein 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 umfasst die Analyse 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; ISTOCK / PESHKOV

Das CrypTool-Projekt

Open-Source-Software zum Erlernen von Kryptografie und Kryptoanalyse

Das CrypTool-Projekt (www.cryptool.org) ist eine Sammlung von Softwareanwendungen, Lehr- und Lernmaterial zum Thema Kryptografie. Dabei stehen historische Verfahren ebenso im Fokus wie Anwendungen, die in modernen IT-Umgebungen verwendet werden. Seit März 2023 befindet sich die Gesamtprojektleitung an der Professur für Datenschutz und Compliance von Herrn Prof. Dr. Wacker.

CRYPTOOL (CT) kommt in erster Linie in der universitären Lehre zum Einsatz, wird aber auch von Schülern, Hobbykryptologen und Historikern verwendet. Das Decrypt-Projekt https://de-crypt.org beispielsweise arbeitet derzeit an einer Software-pipeline, um das Entschlüsseln alter Archivfunde automatisiert zu ermöglichen. CrypTool-Softwarekomponenten sind hier Teil der Pipeline. Außerdem ist die Krypto-Challenges-Seite MysteryTwister www.mysterytwister.org, die ihre Basis an der Universität Bochum hat, an das Projekt angedockt.

CT wurde im Jahr 1998 von Prof. Esslinger (Universität Siegen) ursprünglich als Awareness-Tool während seiner Zeit bei der Deutschen Bank ins Leben gerufen. Unter seiner Leitung und unter Mitwirkung zahlreicher Freiwilliger, Studierender, Forschender und Challenge-Solver aus der ganzen Welt fand seitdem eine stetige Weiterentwicklung statt. Die technische Infrastruktur war bereits im Jahr 2019 nach München an die Professur für Datenschutz und Compliance von Prof. Dr. Wacker umgezogen, heuer wurde schließlich auch die Hauptprojektverantwortung an ihn übertragen. Frau Dr. Behrendt kümmert sich seit März 2023 als Projektleiterin um die Weiterentwicklung und Pflege des CT-Projektes.

Neben einigen kleineren Teilprojekten konzentrierte sich unsere Arbeit im Jahr 2023 auf zwei Schwerpunkte:

Der erste Schwerpunkt lag auf der Umstellung der Webanwendung CrypTool-Online (CTO, https://www.cryptool.org/de/cto/) auf das Paradigma „mobile first“ unter Verwendung moderner Webtechnologien. CTO enthält ca. 50 Kryptografie-Apps, z. B. eine AES-Animation, die Msieve-Faktorisierung oder auch die Caesar-Verschlüsselung. Jede dieser Apps muss von der derzeitigen Infrastruktur, basierend auf einem Jekyll Rebuild des ursprünglichen CrypTool-Portals, das mit Joomla gebaut worden war, auf die neue Infrastruktur portiert werden. Die neue Infrastruktur verwendet u. a. Next.js, React und Chakra-UI.

Für Studierende besteht die Möglichkeit, im Rahmen ihrer Bachelor- oder Masterarbeit an der Professur von Herrn Wacker eine der CTO-Apps zu portieren und dabei von erfahrenen Full-Stack-Webentwicklern des CT-Projektes Unterstützung zu erhalten. Die ersten Arbeiten sind bereits im Entstehen.

Die Umstellung zum neuen CTO soll im Jahr 2024 erfolgreich abgeschlossen sein.

Der zweite Schwerpunkt besteht darin, neuere Verfahren, insbesondere aus den Bereichen Post-Quanten-Kryptografie und voll-homomorpher Verschlüsselung, in CTO zu implementieren. Hier konnten erste Prototypen gebaut werden, gleichwohl wurde deutlich, dass zum Verständnis mehr mathematische Grundlagen nötig sind.

Die Entwicklung solcher Grundlagen-Apps ist ein weiteres Ziel für das Jahr 2024.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

ABB.: FI CODE / A. WACKER

Detektion von Cookie-Bannern

Erkennung, Erfassung und Bewertung von Cookie-Bannern

In diesem Dissertationsprojekt wird die automatisierte Erfassung und Analyse von Cookie-Bannern auf Webseiten untersucht. Ziel ist es, eine möglichst genaue Methode zur Identifizierung und Bewertung von Cookie-Bannern zu entwickeln. Das Projekt soll einen umfassenden Überblick über die Einhaltung von Richtlinien bezüglich Cookie-Bannern auf Webseiten geben. Diese Richtlinien ergeben sich aus der Datenschutzgrundverordnung (DSGVO).

ABB.: FI CODE / A. WACKER; ISTOCK / WONGMBATULOYO

IM RAHMEN des Projekts werden verschiedene Techniken und Ansätze untersucht, um die effektivste Methode zur Erfassung und Klassifizierung von Cookie-Bannern zu ermitteln. Die Klassifizierung von Cookie-Bannern erfolgt danach, ob ein Cookie-Banner manipulativ ist oder nicht. Diese Einteilung hilft uns bei der Beurteilung, ob ein Cookie-Banner den Anforderungen der DSGVO entspricht oder nicht. Bei dieser Einteilung werden unter anderem die vom Cookie-Banner angebotenen Optionen (Ablehnen/Akzeptieren) und deren farbliche Gestaltung als Kriterien herangezogen. Auch das Setzen von Cookies durch die Webseite ist relevant, da nicht nur das Banner korrekt gestaltet sein muss, sondern auch das Setzen von Drittanbieter-Cookies im Hintergrund erst nach Zustimmung des Nutzers erfolgen darf.

Das manuelle Verfahren zur Bewertung von Cookie-Bannern ist präzise, aber langsam und aufwändig. Eine Bewertung anhand fester Begriffe oder Strukturen im HTML-Code scheidet ebenfalls aus. Aufgrund der Vielfalt und Flexibilität, mit der Cookie-Banner dargestellt werden können, z. B. durch Positionierung, unterschiedliche Formulierungen und Einbettung der Banner auf der Webseite, ist dieses Vorgehen keine Option. Daher wird der Fokus auf maschinelles Lernen (ML) gelegt und untersucht, wie ML eingesetzt werden kann, um Cookie-Banner automatisch zu erkennen, zu klassifizieren und ggf. relevante Informationen daraus zu extrahieren. Dies umfasst die Entwicklung und das Training von Modellen, das Testen verschiedener Verfahren und deren Optimierung.

Erste Ansätze mit ML zur Erkennung, ob ein Cookie-Banner vorhanden ist oder nicht, haben je nach Ansatz eine Genauigkeit von 70 bis 90 Prozent gezeigt.

Auch die sprachliche Formulierung des Textes ist für die Klassifizierung relevant, da ein Banner nach den Vorgaben der DSGVO für den Nutzer leicht verständlich gestaltet sein muss. Dies stellt für ML-Ansätze noch eine große Herausforderung dar. So müsste ein Modell trainiert werden, das beurteilen kann, ob ein vorgegebener Text zu einem Cookie-Banner für einen Menschen leicht verständlich ist oder nicht.

All diese Schritte, das Erkennen eines Banners, das Klassifizieren in verschiedene Möglichkeiten der Manipulation des Nutzers, werden aufeinander aufbauen. Daher wird es aller Voraussicht nach nicht möglich sein, ein einziges Modell zu entwickeln, das alle diese Schritte in einem Durchgang durchführt.

Als Ergebnis des Projektes soll eine Aussage darüber getroffen werden, wie die Verteilung von Webseiten im Internet in Bezug auf Cookie-Banner ist, ob diese den Nutzer korrekt informieren und sich auch beim Setzen von Cookies korrekt verhalten oder nicht.

Mathias Schlolaut, M.Sc.
mathias.schlolaut@unibw.de
+49 89 6004 7328
www.unibw.de/datcom

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, Erkennung, Bewertung und Mitigation von Cyberrisiken.

Projekt CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA war eines der Pilotprojekte zum Aufbau eines sicheren, widerstandsfähigen und vertrauenswürdigen europäischen Ökosystems mit führenden Kompetenzen in Forschung, Technologie, Industrie und Öffentlichkeit. Es hat Exzellenz und Führung kombiniert, um die Fragmentierung zu überwinden, indem es das Ökosystem zur Stärkung der europäischen digitalen Souveränität aufbaute.

MEHR ALS 21 Highlights, über 300 wissenschaftliche Veröffentlichungen, ein Multi-Stakeholder-Ökosystem, das Forschung, Industrie, Start-ups und öffentliche Einrichtungen zusammenbringt: All das und noch viel mehr hat CONCORDIA erreicht, das am 31. März 2023 endete. Das vierjährige, mit 16 Millionen Euro dotierte Projekt (plus 7 Millionen Euro zusätzlicher Industriemittel) deckte ein breites Themenspektrum ab, darunter Cyberangriffe auf kritische Infrastrukturen, Informationssicherheit und Datenschutz, Zertifizierung und Kompetenzaufbau. CONCORDIA hat sein Ziel, ein europäisches widerstandsfähiges, sicheres und vertrauenswürdiges Ökosystem aufzubauen, das flexibel, innovativ und offen ist, voll und ganz erreicht. Darüber hinaus werden die Ergebnisse von CONCORDIA nicht nur dem Europäischen Kompetenzzentrum für Cybersicherheit und dem Netzwerk der nationalen Cybersicherheitszentren und damit der gesamten europäischen Cybersicherheitsgemeinschaft wertvolle Impulse geben, sondern auch Forschung, Entwicklung und Innovation stärken und beschleunigen. CONCORDIA wurde auch im BMBF-Jahrbuch „Success Stories 2023“ erwähnt.

Ein des CONCORDIA Highlights ist die vorgeschlagene Roadmap für Cybersicherheit in Europa, eine Reihe von strategischen Empfehlungen und Prioritäten in Bezug auf Forschung und Innovation, Bildung, Wirtschaft und Investitionen, Recht, Zertifizierung und Standardisierung. Das CONCORDIA Service Board wurde festgelegt, um den Aufbau und die Verwaltung der Cybersicherheitsgemeinschaft zu ermöglichen. Die KYPO Cyber Range Plattform ist auf die Aus- und Weiterbildung von Cybersicherheitsexperten ausgerichtet, wurde von der Masaryk Universität entwickelt und 2020 als Open Source veröffentlicht. Die KYPO Cyber Range wurde im Jahr 2021 mit dem EU Innovation Radar Preis in der Kategorie Disruptive Tech ausgezeichnet. Die Abwehr von DDoS-Angriffen ist adressiert durch DDoS Clearing House und wurde erfolgreich in Italien und den Niederlanden getestet. Die gemeinsame Nutzung von Daten und Erfahrungen von Experten über Angriffen hilft Unternehmen, herauszufinden, welche Angriffe es gibt, damit sie sich im Voraus darauf vorbereiten können.

Die Entwicklung von CONCORDIA Cyber-Threat-Intelligence-Plattformen für den Telekommunikations- und Finanzsektor, einschließlich eines rechtlichen Rahmens („Code of Engagement“) und Sicherheitsmerkmale, sind weitere Projekterfolge. Die CONCORDIA Initiative Women in Cybersecurity hat Maßnahmen zur Förderung der Geschlechtervielfalt umgesetzt. Das CONCORDIA Governance Modell für ein europäisches Bildungsökosystem im Bereich Cybersicherheit wurde auf der Grundlage der Erfahrungen aus der CONCORDIA Schulung Becoming a Cybersecurity Consultant spezifiziert, dessen erfolgreiche Teilnehmer sich für das von CONCORDIA etablierte Zertifizierungssystem C3 für die Rolle des Cybersicherheitsberaters bewerben konnten. Diese Initiativen, einschließlich der Teach-the-Teacher Aktivität, haben sich mit der Mangel an Cybersecurity Fachleuten durch die Bereitstellung von Schulungen und die Zertifizierung von Cybersecurity-Fähigkeiten befasst. Ein Rahmen für die Risikoanalyse, das CONCORDIA Versicherungsmodell oder das Ökosystem für Start-ups sind weitere Beispiele von Projekterfolgen.

Das CONCORDIA-Konsortium begann mit 42 Partnern, die von der EU finanziert wurden. Am Ende des Projekts bestand das CONCORDIA-Konsortium aus 56 Projektpartnern aus Wissenschaft, Industrie und öffentlichen Einrichtungen, die 21 EU-Mitgliedstaaten und mit Horizont 2020 assoziierte Länder vertraten, wobei die Partner eigene Ressourcen zur Erreichung der Projektziele beitrugen.

Prof. Dr. Gabi Dreo Rodosek

gabi.dreo@unibw.de

+49 89 6004 7360

https://www.concordia-h2020.eu/

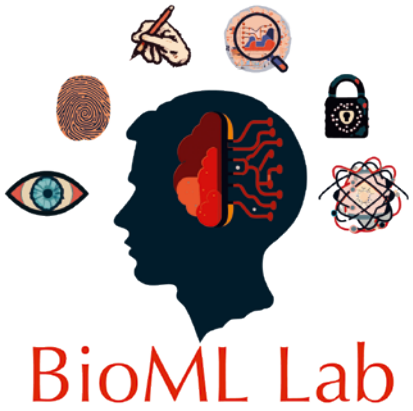
Gefördert durch: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

ABB.: ADOBESTOCK / DENIS PUTILOV

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 und Deep Learning sowie auf kryptografischen Methoden.



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 maschinellen / tiefen Lernens 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.

Biometrie & Kryptographie

Das Hauptproblem bei der biometrischen Erkennung ist, dass wir im Gegensatz zu Passwörtern unseren Fingerabdruck oder unser Gesicht nicht widerrufen und ein Ersatzmerkmal vergeben können. Daher brauchen wir Werkzeuge, um diese sensiblen Daten zu schützen. Die Anwendung gängiger kryptografischer Algorithmen wie Hashes oder RSA ist jedoch nicht die Lösung, nach der wir suchen: Jedes Mal, wenn wir ein biometrisches Sample erfassen, ist Rauschen enthalten, das bei Operationen mit verschlüsselten Daten zu falschen Ergebnissen führen würde. Daher erforscht BioML, wie man homomorphe Verschlüsselungstechniken oder andere Formen irreversibler Transformationen (z. B. Bloom-Filter) auf biometrische Daten anwenden kann, um die Privatsphäre der betroffenen Person durchgängig zu schützen.

Präsentationsangriffserkennung

Wie jede andere Sicherheitstechnologie sind auch biometrische Systeme Angriffen von außen ausgesetzt. Die einfachste Form des Angriffs, die keine technischen Kenntnisse des Angreifers erfordert, besteht darin, dem Erfassungsgerät ein gefälschtes biometrisches Charakteristikum (z. B. eine Gesichtsmaske aus Silikon oder eine dünne Fingerabdruckauflage) vorzulegen, um das System zu täuschen. Dies ist als Präsentationsangriff bekannt und war in den letzten zehn Jahren ein sehr aktives Forschungsgebiet. Da wir nicht vorhersagen können, welche neuen Formen von Präsentationsangriffen in Zukunft auftreten werden, entwickelt BioML Erkennungsmethoden, die sowohl auf traditionellen Zwei-Klassen-Klassifikatoren als auch auf Techniken zur Erkennung von Anomalien basieren.

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

Hon.-Prof. Dr. Udo Helmbrecht

Quanten-kommunikation

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 in München

In einer Welt, in der digitale Sicherheit zunehmend an Bedeutung gewinnt, setzt das Projekt MuQuaNet neue Impulse im Bereich der quantensicheren Kommunikationsinfrastruktur. Mit dem Ziel Quantenschlüsselverteilung (QKD) sowohl für zivile, als auch militärische Anwendungsfälle zu demonstrieren, geht das Projekt wichtige Schritte Richtung Netzintegration im Großraum München.

Vielfältige QKD-Systeme im Test

Das MuQuaNet setzt diverse Quantenschlüsselverteilungssysteme mehrerer Hersteller ein. Die unterschiedlichen Geräte werden in realen Anwendungsfällen getestet, um die Effizienz von QKD in verschiedenen Kontexten besser zu verstehen:

- *LMU Freistrahlsystem:* QKD basierend auf dem BB84-Protokoll, entwickelt in Kooperation mit der LMU. Der Schwerpunkt liegt auf Miniaturisierung und der Untersuchung atmosphärischer Störungen.
- *ID Quantique:* Die Systeme nutzen das Coherent One-Way (COW) Protokoll für Einfachheit oder ein Time-Bin BB84-Protokoll für erhöhte Sicherheit.
- *Quantum Optics Jena:* Systeme basierend auf Verschränkung, die höchste Sicherheit durch quantenmechanischen Zufall und Nicht-Klonbarkeit von Quantenzuständen bieten.
- *QuantLR:* Systeme aus Israel, die das Time-Bin BB84-Protokoll verwenden, ähnlich zu ID Quantique, aber mit spezifischen Optimierungen, besonders bezüglich der Hardwarekosten.

Die Kombination unterschiedlicher Systeme zielt darauf ab, eine robuste Infrastruktur für quantensichere Kommunikation im Großraum München zu schaffen.

MuQuaNet Glasfasernetz.

Schlüsselmanagement als Kernstück

Herausforderungen gibt es bei der Interoperabilität verschiedener QKD-Systeme aufgrund fehlender Standards. Ein Fokus liegt daher auf dem Schlüsselmanagement, um Quantenschlüssel sicher zu verteilen. Ein Aspekt sind die Trusted Relays, die für die Übertragung von Schlüsseln über größere Distanzen nötig sind, aber Vertrauen in die Zwischenknoten erfordern und keine absolute Sicherheit bieten. Daher ist eine Verstärkung durch zusätzliche Mechanismen notwendig.

Lokales KMS mit Rohde & Schwarz

Ein lokales Key-Management-System wurde entwickelt, um QKD in SITLine-Verschlüssler von Rohde & Schwarz zu integrieren. Diese sind für kritische Umgebungen geeignet und erfüllen Anforderungen für die VS-NfD-Zulassung auf OSI-Schicht 2. Zukünftige Entwicklungen werden Hybridisierung mit anderen Schlüsselaustauschverfahren und das Management komplexer Netzinfrastrukturen einschließen.

MKR mit der TU Ilmenau und secunet

Ein alternativer Ansatz wurde für SINA VPNs entwickelt, die die VS-NfD-Zulassungsanforderungen auf OSI-Schicht 3 erfüllen. Diese nutzen Multi-Path-Key-Reinforcement (MKR), eine Methode, die Schlüsselmaterial über unterschiedliche Pfade austauscht und kombiniert, um die Sicherheit zu erhöhen. Dies ist besonders vorteilhaft für die Robustheit der Schlüsselverteilung in komplexen Netzen. Das MuQuaNet trägt maßgeblich zur Entwicklung von quantensicherer Kommunikation für Behörden und kritische Infrastrukturen bei. Durch Kombination verschiedenster Ansätze verbessert es den Schutz unserer Daten, mit wichtigen Auswirkungen für München und Europa.

Hon.-Prof. Dr. Udo Helmbrecht
udo.helmbrecht@unibw.de
Dr. Nils gentschen Felde
felde@unibw.de
+49 89 6004 7375
www.unibw.de/muquanet

Gefördert durch:

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

ABB.: TAUSENDBLAUWERK.DE / M. KRÄMER; FI CODE / MUQUANET / F. FARINA

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.

Projekt AI-GDP

KI-basierte Entwicklung von Leitlinien: Innovative Entscheidungsfindung in der Gesundheitsversorgung

Dieses Projekt spezifiziert und identifiziert die Rolle, die Künstliche Intelligenz bei der Analyse von Informationen, der Entscheidungsfindung und der Entwicklung von Leitlinien im Bereich der öffentlichen Gesundheit spielen kann. KI-Technologien haben in einer Vielzahl von Bereichen Maßstäbe gesetzt. Sie können daher essenziell bei der Erfüllung des Auftrags der WHO in künftigen Prozessen zur Entwicklung normativer Leitlinien sein.

KI in der Analyse von Public Health Intelligence und der Leitfadenentwicklung

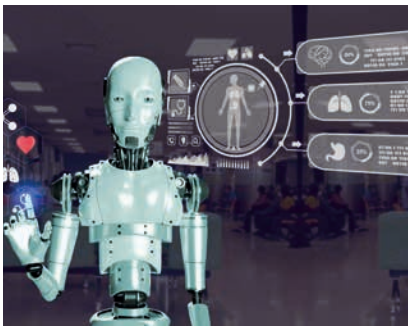
Die Analyse von Erkenntnissen des öffentlichen Gesundheitswesens kann in hohem Maße von KI profitieren, insbesondere durch die Erleichterung der Echtzeit-Überwachung und der Erstellung von Prognosemodellen. Darüber hinaus kann sie die Fähigkeit zur Vorausschau (z. B. bei Epidemien, Pandemien und Krisen) verbessern, Gesundheitstrends überwachen und die Wirksamkeit von Gesundheitsmaßnahmen und Leitlinien bewerten.

Leitlinienentwicklung und Qualitätssicherung von normativen Produkten im Fast-Track

Das Projekt beschreibt, wie KI die Automatisierung der Datenerfassung erleichtern kann, z. B. bei der Bewältigung großer Informationsmengen, bei Echtzeitdaten und bei Daten, die in verschiedenen Sprachen und Formaten (z. B. schriftlich, in Bild- oder Tonformaten) vorliegen. Besonderer Fokus liegt auf der Integration von Daten aus unterschiedlichen Quellen (z. B. elektronische Aufzeichnungen, Leitlinien, soziale Medien usw.) und somit der Erleichterung einer umfassenden Datenerfassung in Echtzeit. Einige innovative Beispiele sind KI-gesteuerte Suchprozesse, KI-gestützte Wearables, KI-gesteuerte Drohnen.

Beeinflussung der Leitlinienentwicklung durch KI-Schlüsseltechnologien

Unter anderem kann KI die Analyse großer Datenmengen schneller und genauer machen. Hierdurch können die neuesten Daten und Trends widergespiegelt, Prozesse standardisiert, und menschliche Fehler reduzieret werden.



Optimierung des Berichtswesen im Bereich der Public Health Intelligence

Das Projekt und die damit verbundenen Workshops haben gezeigt, dass KI dazu beitragen kann, Berichte über die öffentliche Gesundheit auf verschiedene Zielgruppen zuzuschneiden und auf diese Weise die Entscheidungsfindung zu erleichtern. Der Anpassungsprozess kann unter anderem anhand folgender Variablen erfolgen: sprachliche Übersetzung (Beibehaltung der Bedeutung in der Zielsprache), unterschiedliche Fachkenntnisse (Anpassung von Komplexität und Fachbegriffen), Formate (Text, Präsentation, Infografik, audiovisueller Inhalt)

KI in der Entscheidungsfindung im öffentlichen Gesundheitswesen

KI-gestützte Entscheidungsfindungssysteme im öffentlichen Gesundheitswesen können erhebliche Fortschritte bieten, z. B. bei der Entwicklung normativer Leitlinien, der Zuweisung von Ressourcen, der Diagnostik und der Behandlungsplanung, u. a. zur Unterstützung eines künftigen Living Approach. Beispiele für diese Systeme sind: Expertensysteme (Nachahmung der menschlichen Entscheidungsfindung auf Grundlage von Expertenwissen), präskriptive Analytik (Vorhersage von Konsequenzen zur Optimierung des Entscheidungsprozesses) und Konsensalgorithmen.

Prof. Dr. Maximilian Moll

Prof. Dr. Stefan Pickl

stefan.pickl@unibw.de

+49 89 6004 2400

https://go.unibw.de/aigdp

Gefördert durch:
WHO

ABB.: ADOBE STOCK / TIERNEY; ADOBOE STOCK / APITHANA

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

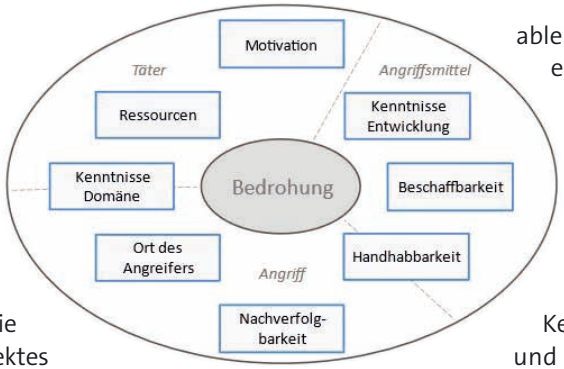
Basierend auf der zunehmenden Anwendung von Digitalisierungsaspekten wie Big Data, IT etc., weist das System Bahn eine erhöhte Vulnerabilität gegenüber Angriffen von Dritten auf. Ein generelles Vorgehen bzgl. einer einheitlichen Angriffssicherheit hat sich bis dato nicht durchgesetzt. REAVRS entwickelt 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 zukunfts-weisendes 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 entwickelden Management Cockpits.

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

Nationales Koordinierungszentrum für Cybersicherheit

FI CODE ist Partner des Nationale Koordinierungszentrums für Cybersicherheit (NKCS, engl. NCC-DE) für Deutschland und arbeitet im Konsortium mit dem BMVg im Bereich militärische Cybersicherheitsforschung eng zusammen. Ziel dieser Initiative durch die Europäische Kommission ist es, nationale Koordinierungszentren und somit Kontaktstellen zu etablieren, die die Forschung und Entwicklung im Bereich Cybersicherheit beobachtet, ein nationales Netzwerk zum Austausch von Expertisen und Wissen zu etablieren, sowie neue Forschungsrichtungen und Aspekte der Europäischen Kommission für ihre Agenda und Rahmenprogramme liefert.

DAS EUROPÄISCHE PARLAMENT und der Europäische Rat haben sich darauf geeinigt, auf der Grundlage der EU-Verordnung 2021/887 das Europäische Kompetenzzentrum für Cybersicherheit (engl. European Cyber Security Centre, ECCC) sowie ein Netzwerk nationaler Koordinierungszentren einzurichten, das sich über die gesamte Europäische Union erstrecken soll. Das ECCC und das Netzwerk sollen Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich der Cybersicherheit bündeln und die Planung der Programme Horizont Europa und Digitales Europa besser koordinieren.

In Deutschland ist das Nationale Koordinierungszentrum (NKCS, engl. NCC-DE) für Cybersicherheit in Industrie, Technologie und Forschung eine gemeinsame Anstrengung

- des Bundesministeriums der Verteidigung (BMVg) und dem angegliedertem Forschungsinstitut Code mit Fokus auf militärische Cybersicherheitsforschung,
- des Bundesministeriums des Innern und für Heimat (BMI) mit Fokus auf alle Cybersicherheitsaspekte,
- des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) mit Fokus auf Betreuung von Industrie, KMUs und Start-ups,
- des Bundesministeriums für Bildung und Forschung (BMBF) mit Fokus auf die Forschung in der zivilen Sicherheit,
- sowie dem DLR-Projektträger in enger Zusammenarbeit mit dem BMBF und BMWK.

Das BSI fungiert als zentraler Ansprechpartner für das ECCC, das NCC-Netzwerk und die nationalen Akteure.

Das NCC-Netzwerk wird den Austausch zwischen den Mitgliedsstaaten intensivieren und es Interessenten aus Verwaltung, Industrie und Forschung in der EU ermöglichen, schneller und einfacher Partner für multilaterale Projekte zu finden und so die digitale Souveränität der EU zu stärken. Innerhalb der einzelnen Mitgliedstaaten fördert und intensiviert das jeweilige NCC den Dialog und Austausch zwischen interessierten nationalen Partnern. Auf diese Weise wird der Informationsfluss zum ECCC konsolidiert, um die nationale Cybersicherheits-Community optimal zu unterstützen und sicherzustellen, dass die nationalen Interessen im EU-Förderprozess effektiv vertreten werden.

Die Kernaufgaben des NCC-DE liegen in der Vernetzung der nationalen Cybersicherheits-Community, die Unterstützung der Cybersicherheits-Community bei der Teilnahme an EU-Förderprogrammen, die Entwicklung von Beiträgen zu EU-Förderprogrammen „Horizon Europe“ und „Digitales Europa“ sowie die kontinuierliche Informationssammlung und der Informationsaustausch auf nationaler und europäischer Ebene auch in den speziellen Gremien. Um den Aufbau des NCC-DE zu beschleunigen und die rasche Umsetzung der Kernaufgaben in der Startphase zu ermöglichen, hat ein Teil des Konsortiums im Rahmen des Programms „Digitales Europa“ Ende 2023 zusätzliche Finanzmittel eingeworben. Auf diversen Veranstaltungen präsentiert sich das NCC-DE regelmäßig, um das nationale Netzwerk aufzubauen und weitere Verbindungen zu etablieren. Gleichzeitig werden diese auch dazu genutzt, um Einblick in die aktuelle Forschungslage sowie einen Überblick über zwingende und dringende Forschungsbedürfnisse zu bekommen, um Partner zu verbinden oder Themen an das ECCC für die zukünftige Agenda weiterzugeben.

NCC-DE Team bei der CODE-Jahrestagung 2023 (v. l. n. r.): Stefan Hillesheim, Dr. Marvin Richter (beide DLR-PT), PD Dr. Corinna Schmitt (FI CODE), Dr. Alexander Khanin (DLR-PT), Heiko Siebel, Christian Sick (beide BSI).

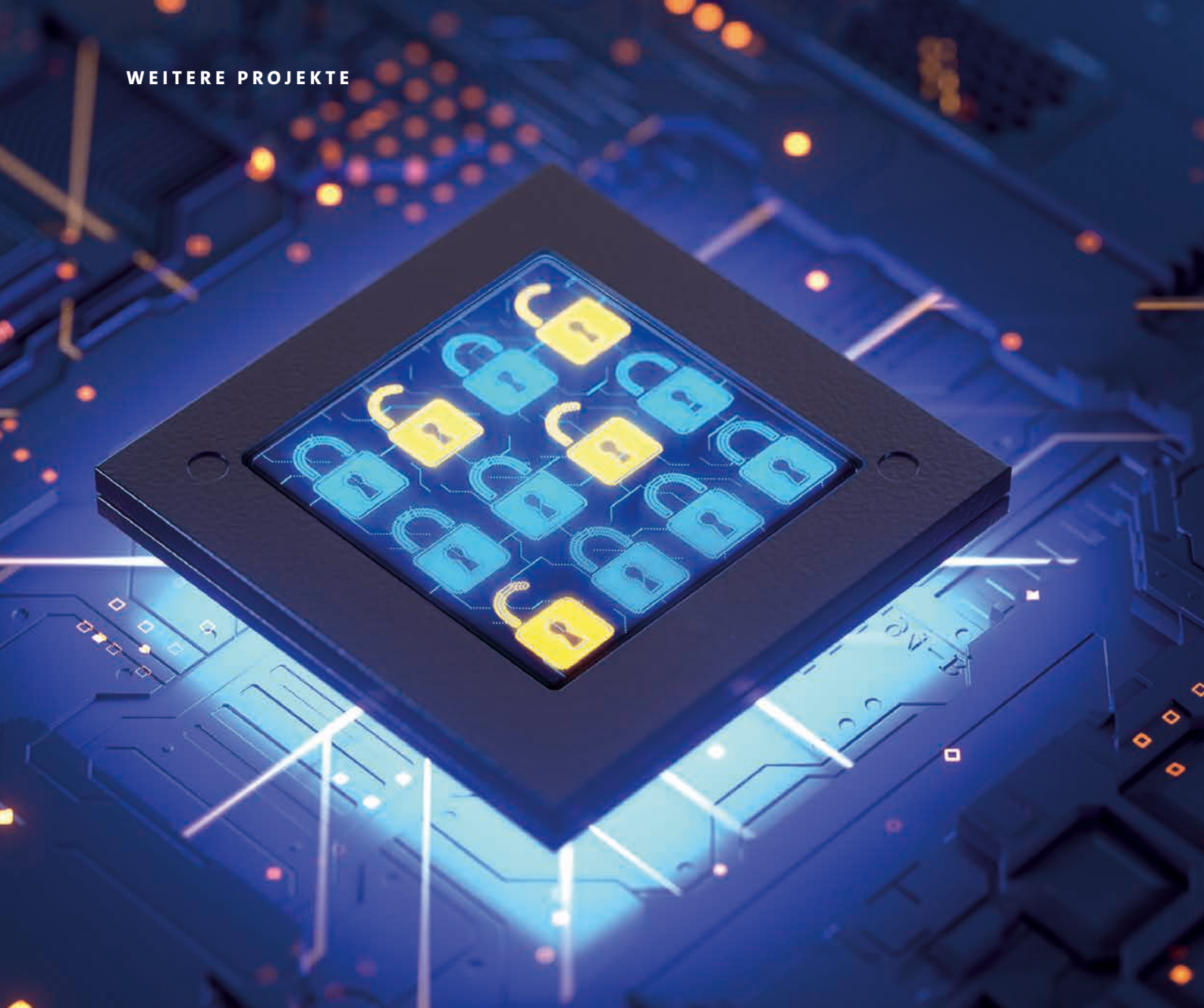
PD Dr. Corinna Schmitt
corinna.schmitt@unibw.de
+49 89 6004 7314
https://nkcs.bund.de

Gefördert durch:
Europäisches Kompetenzzentrum für Cybersicherheit über
Grant Agreement Nr. 101126787

Kofinanziert von der Europäischen Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

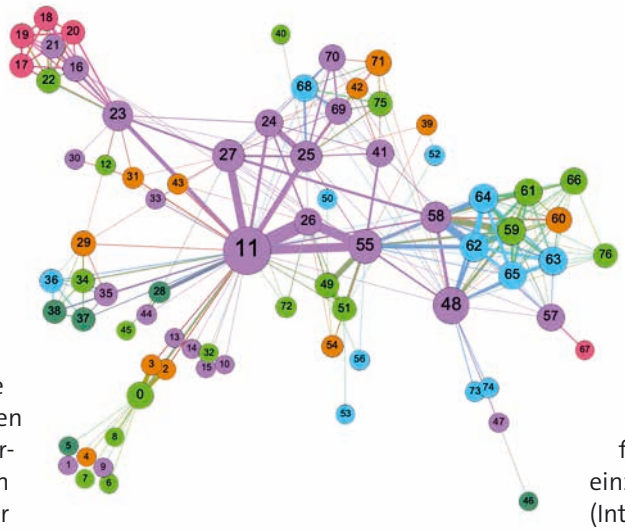
ABB.: ADOBE STOCK / YOUR 123; FI CODE / CORINNA SCHMITT



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 um so 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 / GREENBUTTERFLY

Kooperationen

Deutschland und die Welt

Nationale Partner

Das FI CODE arbeitet in Deutschland mit 96 Partnern in 47 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 96 Institutionen in 47 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 (RWTH) Aachen	Aachen
2	Utimaco Management Services GmbH	Aachen
3	Landkreis Bad Kissingen	Bad Kissingen
4	Universität Bayreuth	Bayreuth
5	Akhetonics GmbH	Berlin
6	Deutsches Institut für Normung (DIN)	Berlin
7	Hochschule für Wirtschaft und Recht Berlin (HWR)	Berlin
8	Verein zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN-Verein)	Berlin
9	Hochschule Bielefeld (HSBI)	Bielefeld
10	IDEMIA Identity & Security Germany AG	Bochum
11	Max-Planck-Institut für Sicherheit und Privatsphäre	Bochum
12	Ruhr-Universität Bochum (RUB)	Bochum
13	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Bonn
14	Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw)	Bonn
15	Deutsches Zentrum für Luft- und Raumfahrt (DLR) Projekträger	Bonn
16	Technische Universität Braunschweig	Braunschweig
17	Constructor University gGmbH	Bremen
18	f.u.n.k.e. AVIONICS GmbH	Buchloe
19	Technische Universität Chemnitz	Chemnitz
20	Fraunhofer-Institut für Graphische Datenverarbeitung (IGD)	Darmstadt
21	GSI Helmholtz-Zentrum für Schwerionenforschung	Darmstadt
22	Hochschule Darmstadt (h_da)	Darmstadt
23	Nationales Zentrum für angewandte Cybersicherheit ATHENE	Darmstadt
24	Technische Universität Darmstadt	Darmstadt
25	RapidMiner GmbH	Dortmund
26	Helmholtz-Zentrum Dresden-Rossendorf (HZDR)	Dresden
27	Technische Universität Dresden (TUD)	Dresden
28	CampusGenius GmbH	Dresden
29	Meshmerize GmbH	Dresden
30	Wandelbots GmbH	Dresden
31	Mimetik UG	Dresden
32	Enari GmbH	Dresden
33	Universität Duisburg-Essen (UDE)	Duisburg/Essen
34	Landeskriminalamt Nordrhein-Westfalen (LKA NRW)	Düsseldorf
35	Rheinmetall AG	Düsseldorf
36	Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)	Erlangen/Nürnberg
37	secunet Security Networks AG	Essen
38	Frankfurt University of Applied Sciences	Frankfurt a. M.
39	nuix	Frankfurt a. M.
40	Droniq GmbH	Frankfurt a. M.
41	KEEQuant GmbH	Fürth
42	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ)	Garching
43	AWARE7 GmbH	Gelsenkirchen
44	Wehrtechnische Dienststelle für Informationstechnologie und Elektronik (WTD 81)	Greding
45	Führungsakademie der Bundeswehr (FüAkBw)	Hamburg
46	Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H)	Hamburg
47	DFN-CERT Services GmbH	Hamburg
48	Technische Universität Hamburg (TUHH)	Hamburg
49	Gottfried Wilhelm Leibniz Universität Hannover (LUH)	Hannover

	Partner	Ort
50	Medizinische Hochschule Hannover (MHH)	Hannover
51	Fraunhofer-Institut für Digitale Medientechnologie (IDMT)	Ilmenau
52	Technische Universität Ilmenau	Ilmenau
53	Quantum Optics Jena GmbH	Jena
54	Christian-Albrechts-Universität zu Kiel (CAU)	Kiel
55	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)	Koblenz
56	SoSafe GmbH	Köln
57	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)	Köln/Oberpfaffenhofen
58	Universität Konstanz	Konstanz
59	Minol-ZENNER-Gruppe	Leinfelden-Echterdingen
60	BWI GmbH	Meckenheim
61	Center for Digital Technology and Management (CDTM)	München
62	ESG Elektroniksystem- und Logistik-GmbH	München
63	FAST-DETECT GmbH	München
64	fortiss GmbH – Landesforschungsinstitut des Freistaats Bayern für software-intensive Systeme	München
65	Google München	München
66	Hanns-Seidel-Stiftung	München
67	Ludwig-Maximilians-Universität München (LMU)	München
68	Polizeipräsidium München	München
69	Rohde & Schwarz GmbH & Co. KG	München
70	Siemens Energy AG	München
71	Technische Universität München (TUM)	München
72	VISTA Geowissenschaftliche Fernerkundung GmbH	München
73	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	München
74	Siemens AG	München
75	Bayerische Motoren Werke Aktiengesellschaft (BMW AG)	München
76	Olive Robotics GmbH	München
77	Cadami GmbH	München
78	Infineon Technologies AG	Neubiberg
79	Carl von Ossietzky Universität Oldenburg	Oldenburg
80	Universität Paderborn (UPB)	Paderborn
81	Universität Passau	Passau
82	CISPA Helmholtz-Zentrum für Informationssicherheit	Saarbrücken
83	INM – Leibniz-Institut für Neue Materialien	Saarbrücken
84	Landeskriminalamt Baden-Württemberg (LKA BW)	Stuttgart
85	Universität Stuttgart	Stuttgart
86	Airbus Protect GmbH	Taufkirchen
87	Hensoldt Cyber GmbH	Taufkirchen
88	SkyFive AG	Taufkirchen
89	Airbus Defence and Space GmbH	Taufkirchen
90	Eberhard Karls Universität Tübingen	Tübingen
91	eesy-innovation GmbH	Unterhaching
92	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE	Wachtberg/Bonn
93	Hessisches Landeskriminalamt (HLKA)	Wiesbaden
94	Hessisches Polizeipräsidium für Technik (HPT)	Wiesbaden
95	Bundeskriminalamt (BKA)	Wiesbaden/Berlin
96	Julius-Maximilians-Universität Würzburg (JMU)	Würzburg

ABB.: TAUSENDBLAUWERK.DE


54 Kiel
45 46 47 48 Hamburg
79 Oldenburg
17 Bremen
5 6 7 8 95 Berlin
49 50 Hannover
16 Braunschweig
9 Bielefeld
10 11 12 Gelsenkirchen
43 Bochum
80 Paderborn
26 27 28 29 30 31 32 Dresden
33 Duisburg
Essen 37
Dortmund 25
34 35 Düsseldorf
53 Jena
19 Chemnitz
Köln 56 57
1 Aachen
2
13 14
60 Meckenheim
Bonn 15
51 Ilmenau
52
93 94 95 Wachtberg
Koblenz 55
92
38 39 40 Frankfurt/Main
Wiesbaden
3 Bad Kissingen
4 Bayreuth
Darmstadt
96 Würzburg
20 21 22 23 24
Erlangen 36
Fürth
Nürnberg 41
82 83 Saarbrücken
Greding 44
84 85 Stuttgart
59 Leinfelden-Echterdingen
90 Tübingen
61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77
81 Passau
42 Garching
München
Neubiberg 78
Unterhaching 91
18 Buchloe
Oberpfaffenhofen
57
Taufkirchen
86 87 88 89
58 Konstanz
Legende
1 Standortnummer der Partner
Standorte der Partner

Internationalität

Auch international pflegt das FI CODE ein großes Netzwerk. Im Jahr 2023 stammten die Mitarbeitenden aus 16 Ländern. In 35 Ländern gab es 130 Kooperationspartner.

Internationale Kooperationspartner

Land	Partner
Ägypten	European Universities in Egypt
	German University in Cairo
Australien	University of Melbourne
Belgien	EIT Digital
	KU Leuven
Dänemark	Aarhus University
Estland	CybExer Technologies
	eu-LISA
	Foundation CR14
Finnland	Jamk University of Applied Sciences
	Tampere University
	University of Oulu
Frankreich	Air and Space Force Academy Research Center (CREA)
	ARIADNEXT
	Cyber-Detect
	EURECOM
	Paris Cité University
	Thales SIX GTS France SAS
	University of Lorraine (UL)
Griechenland	Agroknow IKE
	Athena Research and Innovation Center (ARC)
	Centre for Research and Technology Hellas (CERTH)

Land	Partner
Griechenland	EXUS AI Labs
	Foodscale Hub
	Foundation for Research and Technology – Hellas (FORTH)
	Harokopio University of Athens
	IASIS NGO
	Logstail Mon. IKE
	Ministry of Digital Governance
	National and Kapodistrian University of Athens (NKUA)
	Space Hellas S.A.
	Ubitech
	University of Patras
Irland	Trilateral Research Limited Ireland (TRI-IE)
Israel	Ben-Gurion University of the Negev
Italien	Abaco S.p.A.
	CRF
	CY4GATE S.p.A.
	Leonardo S.p.A.
	Polytechnic University of Turin
	Telecom Italia S.p.A.
	University of Bologna
	University of Insubria
	University of Milan

ABB.: ISTOCK / BLUE PLANET STUDIO

Land	Partner
Italien	University of Roma Tre
Japan	NTT Social Informatics Laboratories
Kanada	University of Toronto
	University of Waterloo
Kroatien	Innovation Center Nikola Tesla (ICENT)
	University of Zagreb
	Utilis Ltd
Litauen	Diversity Development Group
Luxemburg	University of Luxembourg
Malta	University of Malta (UM)
Neuseeland	University of Auckland
Niederlande	Airbus Defence and Space Netherlands B.V.
	Aircision BV
	Arthur's Legal B.V.
	Delft University of Technology
	Dutch Organization for Applied Scientific Research
	Eindhoven University of Technology (TU/e)
	SIDN – Stichting Internet Domeinregistratie Nederland
	SURFnet
	University of Groningen
	University of Twente
Norwegen	Norwegian University of Science and Technology (NTNU)
	Oslo Metropolitan University (Oslomet)
	Telenor ASA
	University of Oslo
Österreich	AIT Austrian Institute of Technology
	Austrian Armed Forces
	Carinthia Emergency Services
	Complexity Science Hub Vienna (CSH)
	Johannes Kepler University Linz (JKU)
	Kelag-Konzern
	Municipality of Neuhaus, Carinthia
	P.SYS Caring Systems
	SBA Research
	TÜV TRUST IT GmbH
	University of Innsbruck
	University of Applied Sciences Campus Vienna
	University of Salzburg
	University of Vienna
	Vienna University of Technology
Polen	Wrocław University of Science and Technology (WUST)
Portugal	EFACEC Electric Mobility SA

Land	Partner
Rumänien	Babeș-Bolyai University
	BitDefender SRL
Schweden	Ericsson AB
	RISE Research Institutes of Sweden AB
Schweiz	EPFL
	ETH Zurich
	RUAG
	University of Lausanne
	University of Zurich (UZH)
Serbien	Foodscale Hub
Slowenien	Jožef Stefan Institute (JSI)
	University of Maribor
Spanien	Association Fòrum Dona Activa 2010
	Atos Spain S.A.
	Autonomous University of Madrid (UAM)
	CaixaBank, S.A.
	i2CAT
	Indra Sistemas S.A.
	NTT Data
	Telefónica I+D SA
	University of Murcia
Südkorea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Tschechien	Flowmon Networks AS
	IMA s.r.o.
	Masaryk University (MU)
Ungarn	Eötvös Loránd University
USA	Auburn University, College of Engineering
	Brave Software
	Brown University
	Social Engineer Inc.
	University of Arizona, College of Engineering
	University of Maryland
	University of North Carolina at Charlotte
	University of Utah
Vereinigtes Königreich	Imperial College of Science, Technology and Medicine
	Lancaster University
	Trilateral Research Limited UK (TRI-IE)
	University of Glasgow
	University of Sheffield
	University of Surrey
Zypern	Centre for Social Innovation Ltd. (CSI)
	Cyprus University of Technology (CUT)
	Eight Bells Ltd.

ABB.: ADOBE STOCK / MH.DESING

Nachwuchs-förderung

Chancen und Angebote

Studienpreis des Forschungsinstituts CODE 2023

An Approach to Creating Adversarial Samples

Das Forschungsinstitut Cyber Defence (CODE) zeichnet gemeinsam mit der Firma Giesecke+Devrient GmbH die Abschlussarbeit von Herrn Hannes Jost Ludwig mit dem CODE-Studienpreis 2023 aus. In seiner Masterarbeit befasst sich der Cyber-Sicherheit-Studentmit Möglichkeiten der Manipulation von Eingabedaten für Künstlicher Intelligenz.

DIE ZUNEHMENDE INTEGRATION von Künstlicher Intelligenz (KI) in alltägliche Anwendungen und deren kontinuierliche Weiterentwicklung prägen das Bild der modernen Informationstechnologie (IT). Diese Entwicklung eröffnet der Gesellschaft einerseits vielfältige Chancen, stellt sie andererseits aber auch vor eine Reihe neuer Herausforderungen, insbesondere im Bereich der IT-Sicherheit. Gerade aufgrund der weiterwachsenden Abhängigkeit von KI müssen diese neuen Sicherheitsbedenken adressiert werden.

In seiner Masterarbeit „An Approach to Creating Adversarial Samples" nimmt sich Herr Ludwig diesen Herausforderungen an, indem er zwei im Sicherheitskontext wichtige Forschungsfelder untersucht: Adversarial Samples und Explainable AI. Bei Adversarial Samples handelt es sich um manipulierte Eingaben, die darauf abzielen, neuronale Netze zu stören und Fehlklassifizierungen hervorzurufen. Adversarial Samples stellen daher ein potenzielles Sicherheitsproblem in vielen KI-Anwendungen dar. Explainable AI strebt die Erklärbarkeit von Modellen an, d. h. Entscheidungsfindungsprozesse KI-basierter Systeme nachvollziehbar und transparent darzustellen.

Die Abschlussarbeit untersucht, wie Explainable AI zur Generierung von Adversarial Samples beitragen kann. Dabei werden sowohl theoretische Ansätze als auch praktische Anwendungen beleuchtet, einschließlich der Integration von Techniken aus dem Bereich der Bildoptimierung. Dabei werden Parallelen zwischen diesem Bereich und der Erzeugung von Adversarial Samples gezogen und liefern neue Erkenntnisse für die effektivere Generierung. Darüber hinaus wird untersucht, inwieweit durch die Generierung von Adversarial Samples neue Angriffsmethoden auf KI-Systeme eingeführt werden können.

Herr Ludwig leistet mit seiner Masterarbeit einen entscheidenden Beitrag zur aktuellen Diskussion um die Sicherheit und Transparenz von KI-Systemen. Die Arbeit ist dabei an der Schnittstelle der beiden Bereiche Smart Data und Cyber Defence angesiedelt und zeichnet sich neben der hohen Aktualität durch einen hohen Schwierigkeitsgrad und eine kritische Reflexion aus. Durch die Entwicklung neuer Methoden zur Generierung manipulativer Eingaben fördert die Arbeit die Forderung nach Robustheit und Zuverlässigkeit neuronaler Netze. Gleichzeitig wird durch die Einbeziehung der Erklärbarkeit ein tieferes Verständnis für die Funktionsweise von KI-Technologien gefördert. Seine Arbeit zeigt und verdeutlicht, dass ungelöste Sicherheitsprobleme existieren und sein Ansatz prinzipiell sehr breit anwendbar ist. Herr Ludwig schafft damit die Grundlage für weitergehende Untersuchungen des Einsatzes von Explainable AI im Forschungsbereich der Adversarial Samples.

Der CODE-Studienpreis wurde im Rahmen der großen Masterfeier am 9. Dezember 2023 auf dem Campus der Universität der Bundeswehr München durch Vizepräsident Prof. Dr. Geralt Siebert im Beisein des Leitenden Direktors des FI CODE Prof. Dr. Wolfgang Hommel sowie der Technischen Direktorin des FI CODE Prof. Dr. Michaela Geierhos und Dr. Michael Tagscherer von Giesecke+Devrient verliehen. ■

Verleihung des CODE-Studienpreises 2023: Prof. Geralt Siebert, Prof. Dr. Wolfgang Hommel, Preisträger Hannes Ludwig, Prof. Dr. Michaela Geierhos, Dr. Michael Tagscherer (v. l. n. r.)

ABB.: ADOBE STOCK / TREECHA; 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

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

ABB.: CLAUS SCHUNK

PROMOTIONEN 2023

Yasmeen Abdrabou

„Leveraging Eye Gaze to Enhance Security Mechanisms“

OBWOHL NUTZER häufig unsichere Passwörter wählen oder Passwörter wiederverwenden, sind Passwörter weiterhin ein weit verbreiteter Authentifizierungsmechanismus. Diese Arbeit befasst sich damit, Sicherheitsmechanismen, insbesondere passwortbasierte Mechanismen, durch die Messung von Blickverhalten der Nutzer zu verbessern. Konkret untersuchen wir das Verhalten von Nutzern beim Erstellen von Passwörtern und die daraus resultierende mentale Belastung mit Hilfe von maschinellem Lernen. Basierend auf unseren Resultaten leiten wir ein Framework zur Verwendung von Blickverhalten in Sicherheitssystemen ab und diskutieren ethische sowie Datenschutzbedenken.

Yasmeen Abdrabou wurde im März 2023 bei Prof. Dr. Florian Alt promoviert. Derzeit ist sie an der Lancaster Universität als Senior Research Associate beschäftigt. ■

Michael Grabatin

„Architecture and Tools for Self-sovereign Identity Management on Distributed Ledgers“

IN DER Dissertation wird ein Konzept für selbstbestimmte (eng. self-sovereign) Identitätsmanagementsysteme beschrieben. Dabei werden die Nutzenden ins Zentrum aller Operationen des Identitätsmanagements gestellt, wodurch die Transparenz im Umgang und die Interoperabilität von Identitätsdaten erhöht wird. Die so geschaffenen Identitäten können nicht nur beim Browsen des Internets, sondern auch für Anwendungen im Internet-of-Things (IoT) und für elektronische Identitäten (e-ID) eingesetzt werden. Die Dissertation beschreibt die dafür notwendigen Komponenten und fasst diese zu einem umfassenden Konzept zusammen. Anhand von prototypischen Implementierungen wird die Eignung des Konzepts nachgewiesen. Die Arbeit zeigt so mögliche Entwicklungen für sicheres und datenschutzfreundliches Identitätsmanagement auf.

Michael Grabatin hat im Dezember 2023 bei Prof. Dr. Wolfgang Hommel promoviert und ist am Institut für Softwaretechnologie als Postdoktorand beschäftigt. ■

Joschka Kersting

„Identifizierung quantifizierbarer Bewertungsinhalte und -kategorien mittels Text Mining“

ZWISCHEN DEN Zeilen zu lesen ist bislang Menschen vorbehalten, dabei entstehen online viele Texte zu zwischenmenschlichen Themen. Dieser Forschungslücke widmet sich die Dissertation mittels Machine Learning-Verfahren. Das Ziel dabei sind Identifikation und Einordnung bewertender Aussagen, um diese mit weiteren Daten in Verbindung setzen zu können. Organisationen können dadurch ihre Services zielgerichtet analysieren.

Joschka Kersting wurde im April 2023 bei Prof. Dr. Michaela Geierhos promoviert. Derzeit ist Herr Kersting im Sonderforschungsbereich (SFB) 901 „On-The-Fly Computing“ an der Universität Paderborn tätig. ■

Nils Mäurer

„Secure Communications in Next Generation Digital Aeronautical Datalinks“

UM DIE Kommunikation in der zivilen Luftfahrt zu modernisieren, werden ab 2022 neue digitale Datenverbindungen wie das L-Band Digital Aeronautical Communications System (LDACS) eingeführt. LDACS ist ein zellulares, bodengestütztes digitales Kommunikationssystem für die Flugführung. In der Dissertation wird eine Cybersicherheitsarchitektur für LDACS vorgestellt. Zu den Neuerungen gehören zwei neue Authentifizierungs- und Schlüsselaustauschprotokolle sowie eine neue Methode zur Sicherung von Kontrolldaten. Diese Sicherheitslösungen ebnen den Weg für eine sichere, digitalisierte und automatisierte Zukunft der zivilen Luftfahrt.

Dr. Nils Mäurer wurde im Mai 2023 bei Prof. Dr. Gabi Dreo Rodosek promoviert. Derzeit ist er bei Airbus Defence and Space als Technical Lead für IRIS² beschäftigt. ■

Lukas Mecke

„User-centered Biometric Interfaces“

BIOMETRISCHE Verfahren nutzen einzigartige Muster in der Physiologie oder im Verhalten des Nutzers zur Authentifizierung. Die Nutzer erhalten jedoch nur wenig Einblick in Modellentscheidungen oder Kontrolle über diesen Authentifizierungsmechanismus. Wir schlagen einen nutzerzentrierten Ansatz vor, um bestehende Schnittstellen mit biometrischen Systemen zu verbessern als auch neue vorzuschlagen. Ziel ist es Nutzern mehr Einblicke zu ermöglichen und ihre Kontrolle über den Erkennungsprozess zu erleichtern und damit die sichere und informierte Nutzung der Biometrie zu unterstützen.

Robert Rödler wurde im Mai 2022 bei Prof. Dr. Wolfgang Hommel promoviert. Er arbeitet inzwischen als Programm-Manager Digitalisierung Land bei der IABG mbH im Geschäftsbereich Verteidigung und Sicherheit. ■

Tai Le Quy

„Fairness-aware Machine Learning in Educational Data Mining“

BEIM Educational Data Mining (EDM) können auf maschinellem Lernen basierende Entscheidungen auf geschützten Attributen beruhen. Wir führen eine verzerrungsbewusste Analyse von Datensätzen mit Bayes`schen Netzen durch, um Gruppenfairness in Modellen für die Leistungsvorhersage von Schülern zu bewerten. Als Nächstes stellen wir das fair-kapazitäre Clustering-Problem und das multi-faire kapazitäre Studenten-Themen-Gruppierungsproblem vor, das Präferenzen von Studenten, Kardinalitäten und Fairness berücksichtigt. Wir zeigen, dass eine verzerrungsbewusste Datenanalyse sowie auf Fairness ausgerichtete Modelle unerlässlich sind, um Fairness im EDM zu gewährleisten.

Tai Le Quy wurde im Oktober 2023 bei Prof. Dr. Eirini Ntoutsi und Prof. Dr. Gunnar Friege promoviert. Derzeit ist er an der International University of Applied Sciences als Dozent beschäftigt. ■

ABB.: ADOBE STCOK; PRIVAT (5)

Capture the Flag 2023

„T 50 OO – Rise of the Machines"

Am 24. und 25. November 2023 fand zum neunten Mal das jährliche „Capture the Flag"-Event statt, das vom FI CODE zusammen mit Team localos und ITIS e.V. organisiert wird. Über 100 Personen in 26 Teams nahmen an dem 18-stündigen Wettbewerb teil und traten in herausfordernden Challenges gegeneinander an.

ENDE NOVEMBER hatte nach einer intensiven organisatorischen Vorbereitung und einer spannenden Qualifikation, an der knapp 60 Teams teilnahmen, das Warten ein Ende: Insgesamt 26 Teams fanden sich am Freitagabend im UniCasino auf dem Campus der Universität der Bundeswehr (UniBw M) ein, um an der neunten Auflage des „Capture the Flag" (CTF) teilzunehmen.

Für viele ist der seit 2015 jährlich ausgetragene Hacking-Wettbewerb bereits als fester Termin etabliert, verbindet er doch auf unterhaltsame Weise Kompetenztraining im Bereich Cybersicherheit mit viel Spaß und Action. Auch in diesem Jahr hatten sich die Organisatoren vom FI CODE, Team localos und ITIS e. V. wieder einiges einfallen lassen. Eine Reihe spannender Aufgaben (sogenannte „Challenges") waren

ALLE ABB.: FI CODE / B. BELLGRAU

in den zurückliegenden Wochen und Monaten ausgearbeitet worden, die nun von den über 100 Teilnehmerinnen und Teilnehmern des CTF alles an Können und Geschicklichkeit abverlangen sollten. Mit dem Motto „T50OO – Rise of the Machines“ stand die Veranstaltung ganz im Zeichen der „Terminator“-Filmreihe. Sämtliche Challenges orientierten sich thematisch an dem Plot des Action-Klassikers. Zugleich gelang es den Organisatoren mit der Zahl 50 im Motto einen Bezug zum 50-jährigen Jubiläum der UniBw M herzustellen, welches 2023 gefeiert wurde.

Pünktlich um 18 Uhr gab der Leitende Direktor des FI CODE, Prof. Dr. Wolfgang Hommel, dann den offiziellen Startschuss. Die über 40 abwechslungsreichen Challenges beinhalteten sowohl Aufgaben im virtuellen als auch im physischen Raum. Entscheidender Faktor war dabei vor allem die Zeit. Je nachdem, wie schnell die Teams die gestellten Aufgaben und Rätsel lösen konnten, wurden Punkte vergeben. Teams, die eine Challenge als erste lösten, erhielten Extrapunkte („First Blood“) und damit einen wertvollen Boost im Rennen um die Spitze. Wie schon im Vorjahr entwickelte sich schnell ein spannender Wettkampf unter den besten Teams, der sich über die ganze Nacht hin durchzog und erst gegen Morgen entschieden wurde.

Am Ende des 18-stündigen Wettbewerbs setzte sich das Team „Pink Fluffy Unicorns“ mit 1.208 erreichten Punkten knapp vor den Teams „SIGTERM;“ (1.155 Punkte) und „Pallas Athena CTF“ (1.044 Punkte) durch.

CODEs Leitender Direktor Prof. Dr. Wolfgang Hommel und CODE-Geschäftsführer Marcus Knüpfer, gratulierten den drei top-platzierten Teams zum großartigen Erfolg und überreichten den glücklichen Siegern die begehrte Flag of Fame, auf der sich alle Teammitglieder zum Abschluss stolz verewigen durften. ■

Was ist ein „Capture the Flag“-Wettbewerb (CTF)?

CTFS BIETEN die Möglichkeit, spielerisch Kompetenzen im Bereich der Cybersicherheit zu entwickeln und tragen damit zur praxisbezogenen Ausbildung von Expertinnen und Experten bei. Das „Capture the Flag“ des Forschungsinstituts CODE ist ein auf Wissenserwerb, Teambuilding und Spaß ausgerichteter Hacking-Wettbewerb, der seit 2015 einmal jährlich auf dem Campus der Universität der Bundeswehr München in Neubiberg stattfindet. Während des Events können bereits Studierende ihr theoretisches Wissen anhand verschiedener praktischer Herausforderungen testen.

CODE-Geschäftsführer Marcus Knüpfer (l.) und der Leitende Direktor des FI CODE, Prof. Dr. Wolfgang Hommel (r.), überreichten zwei Vertretern des Siegerteams „Pink Fluffy Unicorns“ (Mitte) die Flag of Fame.

Auch in diesem Jahr mussten die Teams beim CTF unter anderem wieder eine VR-Challenge meistern.

Mehr Informationen:

www.unibw.de/code/events/ctf

www.unibw.de/code/events/capture-the-flag-2023

ctf@unibw.de

ABB.: ADOBE STOCK / COWARD LION

Addendum

Publikationen
Aktivitäten und
Organisation

Prof. Dr.
Florian Alt

Benutzbare Sicherheit und Privatsphäre

PUBLIKATIONEN

ABDRABOU, Y., ASBECK, M., PFEUFFER, K., ABDELRAHMAN, Y., HASSIB, M., ALT, F.: Empowering Users: Leveraging Interface Cues to Enhance Password Security. In: Proceedings of the 19th IFIP TC 13 International Conference on Human-Computer Interaction (INTERACT '23), Springer, Berlin-Heidelberg, Germany, 2023.

ABDRABOU, Y., DIETZ, F., SHAMS, A., KNIERIM, P., ABDELRAHMAN, Y., PFEUFFER, K., HASSIB, M., ALT, F.: Revealing the Hidden Effects of Phishing Emails: An Analysis of Eye and Mouse Movements in Email Sorting Tasks, 2023.

ABDRABOU, Y., KARYPIDOU, E., ALT, F., HASSIB, M.: Investigating User Behaviour Towards Fake News on Social Media Using Eye Tracking and Mouse Movements. In: Proceedings of the Usable Security Mini Conference 2023 (USEC'23), Internet Society, San Diego, CA, USA, 2023. doi: https://dx.doi.org/10.14722/usec.2023.232041

ABDRABOU, Y., MECKE, L., RADIAH, R., PRANGE, S., NGUYEN, Q. D., VOIGT, V., ALT, F., PFEUFFER, K.: How Unique Do We Move? Understanding the Human Body and Context Factors for User Identification. In: Proceedings of Mensch und Computer 2023 (MuC '23), Association for Computing Machinery, New York, NY, USA, 2023, S. 127–137. doi:10.1145/3603555.3603574

ALT, F., HASSIB, M., DISTLER, V.: Human-centered Behavioral and Physiological Security. In: Proceedings of the 2023 Workshop on New Security Paradigms (NSPW '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3633500.3633504

DELGADO RODRIGUEZ, S., DAO PHUONG, A., BUMILLER, F., MECKE, L., DIETZ, F., ALT, F., HASSIB, M.: Padlock, the Universal Security Symbol? – Exploring Symbols and Metaphors for Privacy and Security. In: Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia (MUM '23), Association for Computing Machinery, New York, NY, USA, 2023.

DELGADO RODRIGUEZ, S., HEIN, O., PRIETO ROMERO, I., MECKE, L., DIETZ, F., PRANGE, S., ALT, F.: Shake-it-All: A Toolkit for Sensing Tangible Interactions on Everyday Objects. In: Workshop Beyond Prototyping Boards: Future paradigms for electronics toolkits (CHI '23 Workshops), 2023.

DELGADO RODRIGUEZ, S., RADIAH, R., MÄKELÄ, V., ALT, F.: Challenges in Virtual Reality Studies: Ethics and Internal and External Validity. In: Proceedings of the Augmented Humans International Conference 2023 (AHs '23), Association for Computing Machinery, New York, NY, USA, 2023, S. 105–111. doi:10.1145/3582700.3582716

DISTLER, V., ABDRABOU, Y., DIETZ, F., ALT, F.: Triggering Empathy out of Malicious Intent: The Role of Empathy in Social Engineering Attacks. In: Proceedings of the 2nd Empathy-centric Design Workshop (EMPATHICH '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3588967.3588969

FLEISCHHAUER, Y., SURALE, H. B., ALT, F., PFEUFFER, K.: Gaze-based Mode-switching to Enhance Interaction with Menus on Tablets. In: Proceedings of the 2023 ACM Symposium on Eye Tracking Research & Applications (ETRA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3588015.3588409

FROEHLICH, M., VEGA, J., PAHL, A., LOTZ, S., ALT, F., SCHMIDT, A., WELPE, I.: Prototyping with Blockchain: A Case Study for Teaching Blockchain Application Development at University. In: Learning in the age of digital and green transition (ICL '22), Springer International Publishing, Cham, 2023, S. 1005–1017. doi:10.1007/978-3-031-26876-2_94

HEIN, O., RAUSCHNABEL, P., HASSIB, M., ALT, F.: Sick in the Car, Sick in VR?: Understanding how Real-World Susceptibility to Dizziness, Nausea and Eye Strain Influences VR Motion Sickness. In: Human-Computer Interaction – INTERACT 2023 (INTERACT '23), Springer Nature, Cham, Switzerland, 2023.

LIEBERS, J., GRUENEFELD, U., BUSCHEK, D., ALT, F., SCHNEEGASS, S.: Introduction to Authentication Using Behavioral Biometrics. In: Extended Abstracts of the 2023CHI Conference on Human Factors in Computing Systems (CHI EA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3544549.3574190

MANSOUR, S., KNIERIM, P., O'HAGAN, J., ALT, F., MATHIS, F.: BANS: Evaluation of Bystander Awareness Notification Systems for Productivity in VR. In: Proceedings of the Usable Security Mini Conference 2023 (USEC'23), Internet Society, San Diego, CA, USA, 2023. doi:10.14722/usec.2023.234566

MECKE, L., PRIETO ROMERO, I., DELGADO RODRIGUEZ, S., ALT, F.: Exploring the Use of Electromagnets to Influence Key Targeting on Physical Keyboards. In: Extended abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3544549.3585703

NAMNAKANI, O., SINRATTANAVONG, P., ABDRABOU, Y., BULLING, A., ALT, F., KHAMIS, M.: Gazecast: Using Mobile Devices to Allow Gaze-based Interaction on Public Displays. In: Proceedings of the 2023 ACM Symposium on Eye Tracking Research & Applications (ETRA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3588015.3589663

PFEUFFER, K., OBERNOLTE, J., DIETZ, F., MÄKELÄ, V., SIDENMARK, L., MANAKHOV, P., PAKANEN, M., ALT, F.: PalmGazer: Unimanual Eye-Hand Menus in Augmented Reality. In: Proceedings of the 2023 ACM Symposium on Spatial User Interaction (SUI '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3607822.3614523

PRANGE, S., ALT, F., Increasing Users' Privacy Awareness in the Internet of Things: Design Space and Sample Scenarios. In: Human Factors in Privacy Research, N. Gerber, A. Stöver, and K. Marky, Eds., Cham: Springer International Publishing, 2023, p. 321–336. doi:10.1007/978-3-031-28643-8_16

RADIAH, R., PRODAN, P., MÄKELÄ, V., KNIERIM, P., ALT, F.: How Are Your Participants Feeling Today? Accounting For and Assessing Emotions in Virtual Reality. In: Proceedings of Mensch und Computer 2023 (MuC '23), Association for Computing Machinery, New York, NY, USA, 2023, p. 37–48. doi:10.1145/3603555.3603577

RADIAH, R., ROTH, D., ALT, F., ABDELRAHMAN, Y.: The Influence of Avatar Personalization on Emotions in VR. Multimodal technologies and interaction, Vol. 7, Iss. 4, 2023. doi:10.3390/mti7040038

SAAD, A., IZADI, K., KHAN, A. A., KNIERIM, P., SCHNEEGASS, S., ALT, F., ABDELRAHMAN, Y.: HotFoot: Foot-based User Identification Using Thermal Imaging. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3544548.3580924

TEUSCHEL, M., PÖHN, D., GRABATIN, M., DIETZ, F., HOMMEL, W., ALT, F.: „Don't Annoy Me With Privacy Decisions!" – Designing Privacy-Preserving User Interfaces for SSI Wallets on Smartphones. IEEE Access, vol. 11, S. 131814-131835, 2023. doi:10.1109/ACCESS.2023.3334908

VOIGT, V., WIETHE, R., SASSMANN, C., WILL, M., DELGADO RODRIGUEZ, S., ALT, F.: Safe Call: A Tangible Smartphone Interface that Supports Safe and Easy Phone Calls and Contacts Management for Older People. In: Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia (MUM '23), Association for Computing Machinery, New York, NY, USA, 2023.

FORSCHUNGSPROJEKTE

Voice of Wisdom

Im Projekt Voice of Wisdom werden Ansätze zur Verhinderung mensch-zentrierter Cyberangriffe erforscht. Durch die Analyse menschlichen Verhaltens und physiologischer Reaktionen werden Anzeichen dafür erkannt, dass Menschen einem Risiko ausgesetzt sind. Außerdem werden neuartige, menschzentrierter Sicherheitsmechanismen entwickelt und die langfristigen Auswirkungen dieser untersucht.

Gefördert durch: dtec.bw
Laufzeit: 01/2021 – 12/2024

PrEvoke – Supporting Users in Informed Privacy Permission Revocation

PrEvoke befasst sich mit den Folgen des Widerrufs von Datenschutz Entscheidungen (z. B. wenn Nutzer Apps den Zugriff auf persönliche Daten entziehen). Die von Nutzern erwarteten Konsequenzen in Bezug auf den Widerruf von Datenschutz-Berechtigungen werden untersucht, und mit der Realität verglichen. Außerdem werden entsprechende Konzepte erstellt, um Missverständnissen und Bedenken entgegenzuwirken.

Gefördert durch: Google München
Laufzeit: 12/2021 – 12/2023

Scalable Biometrics

Dieses Projekt untersucht, wie Pervasive Computing-Umgebungen Verhaltens biometrische Daten zur Identifizierung und Authentifizierung von Benutzern verwenden können. Die zentrale Forschungsfrage ist, wie solche Ansätze für verschiedene Umgebungen skaliert werden können, die mehrere Benutzer mit unterschiedlichem Verhalten, physischen Gegebenheiten sowie Erfassungs- und Interaktionsmöglichkeiten enthalten.

Gefördert durch: DFG
Laufzeit: 04/2020 – 03/2023

ubihave

Computer dienen nicht nur als Alltagsbegleiter sondern erzeugen durch die integrierte Sensorik auch benutzerspezifische Daten, die die Erstellung von Verhaltensmodellen ermöglichen. In diesem Projekt werden Modelle entwickelt, die Nutzerverhalten beschreiben, analysieren und vorhersagen. Vielversprechende Anwendungsbereiche sind: benutzbare Sicherheit, Touch- oder Texteingaben und kontextabhängige, adaptive Systeme.

Gefördert durch: DFG
Laufzeit: 01/2019 – 02/2023

LEHRE

10123 **Software-Ergonomie (Human Factors in Computing Systems) (HT)**

39181 **Benutzbare Sicherheit (FT)**

39182 **Praktikum Design Sicherer und Benutzbarer Systeme (FT)**

39183 **Sichere Mensch-Maschine Schnittstellen (WT)**

55011 **Forschungsmethoden der Benutzbaren Sicherheit (WT)**

MESSEN, TAGUNGEN, SEMINARE

- USEC Summer School zu Usable Security and Privacy
- Dagstuhl Seminar zu Social Engineering
- Winter School zu Human-Centered Security
- CHI 2023 Kurs zu Authentication Using Behavioral Biometrics
- (Be-)Greifbare Interaktionen Workshop (Mensch und Computer 2023)
- VHS-Schulung: Sicherheit im Smart Home (50 Jahre Universität der Bundeswehr)
- Schulung zu Cyber Awareness (NATO JSEC)

PREISE UND AUSZEICHNUNGEN

- ACM Symposium on Spatial User Interaction (SUI `23) – Honorable Mention: Pfeuffer, K., Obernolte, J., Dietz, F., Mäkelä, V., Sidenmark, L., Manakhov, P., Pakanen, M., Alt, F.: PalmGazer: Unimanual Eye-Hand Menus in Augmented Reality.
- 2023 Communication by Gaze Interaction (COGAIN) Symposium – Best Paper Award: Namnakani, O., Sinrattanavong, P., Abdrabou, Y., Bulling, A., Alt, F., Khamis, M.: GazeCast: Using Mobile Devices to Allow Gaze-based Interaction on Public Displays.

WEITERE FUNKTIONEN

- PC Chair / Editor für ACM Interactive Surfaces and Spaces 2023/2024
- TPC Chair für Mensch und Computer 2023
- Mitglied des Program Committee für SOUPS 2023
- Gasteditor für IEEE Pervasive Computing Special Issue on the Pervasive Multiverse
- Department Editor für IEEE Pervasive Computing – Security & Privacy
- Editorial Board für IEEE Pervasive Computing
- Steering Committee Chair der Mobile and Ubiquitous Multimedia (MUM) Konferenzreihe
- Keynote Speaker der Augmented Humans 2023

Prof. Dr. Harald Baier

Digitale Forensik

PUBLIKATIONEN

GÖBEL, T., BAIER, H., BREITINGER, F.: Data for Digital Forensics: Why a Discussion on „How Realistic is Synthetic Data“ is Dispensable. Digital Threats 4, 3, Article 38 (September 2023), 18 pages. https://doi.org/10.1145/3609863

GONCALVES, P., BAIER, H.: Applying Activity-based Models to Integrate Labeled Preset Key Events in Intra-Day Human Mobility Scenarios. In: Proceedings of the 9th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS) 2023, Prague, Czech Republic, April 26–28, 2023, S. 281–288.

KLIER, S., BAIER, H.: Scalable Image Clustering to Screen for Self-produced CSAM. AICSEC 2023 – EAI International Conference on Artificial Intelligence for CyberSecurity.

KLIER, S., BAIER, H.: To Possess or Not to Possess - WhatsApp on Android Revisited with a Focus on Stickers. NordSec 2023 – 28th Nordic Conference on Secure IT Systems.

KLIER, S., VARENKAMP, J., BAIER, H.: Back and Forth – On Automatic Exposure of Origin and Dissemination of Files on Windows. In: Digital Threats: Research and Practice 4.3 (2023): 1–17.

MUNDT, M., BAIER, H.: Abbildung und Simulation cyber-physischer Bedrohungen für kritische Infrastrukturen. In: Proceedings of the 30. DFN-Konferenz „Sicherheit in vernetzten Systemen“, Hamburg, February 2023.

MUNDT, M., BAIER, H.: Enabling Protection Against Data Exfiltration by Implementing ISO 27001:2022 update. In: International Conference on Security & Applications (SECURA 2023), International Journal on Cybernetics & Informatics (IJCI), virtual, August 2023.

MUNDT, M., BAIER, H.: Enhancing Incident Management by an Improved Understanding of Data Exfiltration: Definition, Evaluation, Review. International Conference on Digital Forensics and Cyber Crime. In: Proceedings of the EAI ICDF2C 2023 – 14th EAI International Conference on Digital Forensics & Cyber Crime, New York City (USA), November 30–31, 2023.

MUNDT, M., BAIER, H.: Short contribution to Springer Encyclopedia about Data Exfiltration. Encyclopedia of Cryptography, Security and Privacy. April 2023.

TWENNING, L., BAIER, H., GÖBEL, T.: These ARE the Pictures You Are Looking for – On the Use of Perceptual Hashing in Targeted Content Scanning. In: Proceedings of the 19th Annual IFIP WG 11.9 International Conference on Digital Forensics, hybrid (Arlington USA), January 2023.

UHLIG, F., STRUPPEK, L., HINTERSDORF, D., GÖBEL, T., BAIER, H., KERSTING, K.: Combining AI and AM – Improving Approximate Matching Through Transformer Networks. In: Proceedings of the 23rd Annual DFRWS USA Conference, hybrid (Baltimore USA), July 2023.

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)**

MESSEN, TAGUNGEN, SEMINARE

- Lokale Organisation und Conference Chair der IT-Forensik Konferenz ‚IMF 2023‘ im Mai 2023 im UniCasino der UniBw M, URL: https://imf-conference.org/imf2023/
- Vorbereitung und Moderation des CAST-Workshops Forensik / Internetkriminalität am 14.12.2023, URL: https://cast-forum.de/workshops/infos/328
- Workshop (in Kooperation mit ZITiS) zur Drohnenforensik auf der CODE-Jahrestagung sowie der IMF 2023
- Vortrag Enhancing Incident Management by an Improved Understanding of Data Exfiltration: Definition, Evaluation, Review. 14th International Conference on Digital Forensics and Cybercrime (ICDF2C 2023), 01.12.23, New York, USA
- Vortrag Forensische Vorgehensweise bei Drohnen der Hersteller Parrot Anafi und Yuneec Typhoon. “Veitshöchheimer Runde”, 18.10.23, Veitshöchheim
- Vortrag Forensische Analyse einer Drohne vom Typ Parrot Anafi. Drohnen-Workshop „Ausgewählte Themen der Drohnen-Forensik“ auf der CODE-Jahrestagung 2023, 12.07.23, Neubiberg
- Vortrag Digitale Forensik zwischen dem Gestern und dem Morgen. Plenumsvortrag auf der CODE-Jahrestagung 2023, 11.07.23, Neubiberg
- Vortrag Forensik intelligenter Systeme. Keynote auf dem Symposium „SIC! Security and Innovation in Cyberspace“ der Agentur für Innovation in der Cybersicherheit (Cyberagentur), 20.06.23, Halle (Saale)
- Vortrag Forensic Analysis of a Parrot Anafi UAV. Drohnen-Workshop „Data acquisition and analysis of UAVs (drones)” auf der 12th International Conference on IT Security Incident Management & IT Forensics (IMF 2023), 24.05.23, Neubiberg
- Vortrag Using Perceptual Hashing in Targeted Content Scanning. 19th Annual IFIP Working Group 11.9 International Conference on Digital Forensics, 31.01.23, Arlington, USA (online)

WEITERE FUNKTIONEN

- Gutachter für Journal of Digital Investigation und Computers & Security
- Mitgliedschaft in Programmkomitees: Digital Forensics Research Workshop (DFRWS) EU 2023, Digital Forensics Research Workshop (DFRWS) APAC 2023, IT Security Incident Management & IT Forensics (IMF) 2023, IFIP Working Group 11.9 International Conference on Digital Forensics 2023, CAST-GI Promotionspreis 2023
- Unterstützung des Programmdirektors bei der Leitung des Studiengangs ‘IT Security’ an der Vietnamese-German University in Ho-Chi-Minh City, Vietnam

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

PUBLIKATIONEN

BERLAKOVICH, F., BRUNTHALER, S.: R2C: AOCR-Resilient Diversity with Reactive and Reflective Camouflage. In: Proceedings of the Eighteenth European Conference on Computer Systems, EuroSys 2023, Rome, Italy, May 8–12, 2023. ACM 2023, S. 488–504.

BERLAKOVICH, F., BRUNTHALER, S.: R2C: AOCR-Resilient Diversity with Reactive and Reflective Camouflage. In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

BERNAD, M., BRUNTHALER, S.: HOBBIT – Hash-based Object Integrity. In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

MECHELINCK, R., DORFMEISTER, D., FISCHER, B., VOLCKAERT, S., BRUNTHALER, S.: DEPS: Leveraging Hardware Faults for Binding Software to Hardware. In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

MARKVICA, D., BRUNTHALER, S.: µWASM: Interpreting WebAssembly. In: Aachener Informatik-Berichte (AIB), AIB-2023-03, In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

FORSCHUNGSPROJEKTE

APERITIF – Analysis Pipeline for Effective Vulnerability Identification Through Fuzzing

Im Rahmen des Projekts APERITIF erforscht µCSRL neue, hochskalierende und automatische Schwachstellenanalyse-Verfahren durch Fuzzing auf Datacenter-Ebene. Unterstützt durch ein eigenes Cluster analysiert das Team neue Möglichkeiten zur Parallelisierung und Optimierung von einzelnen Fuzzern.

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021 – 2024

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 am Quellcode erkennen lassen, bevor sie den Entwicklungsprozess unterwandern können.

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021 – 2024

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

- Network and Distributed Systems Symposium 2023, San Diego, CA, USA.
- IFIP Working Group 2.3 Workshop in York Harbor, MN, USA.
- European Conference on Computer Systems (EuroSys) 2023, in Rome, IT.
- European Symposium on Security & Privacy 2023, in Delft, NL.
- Kolloquium in Programmiersprachen und Systeme (KPS) 2023, in Vaals, NL.
- ACM Computer and Communications Symposium (CCS), 2023, in Copenhagen, Denmark.
- Organisator des IFIP Working Group 2.4 Workshop #68.

WEITERE FUNKTIONEN

- Area Chair, Journal of Systems Research (JSys).
- Member IFIP Working Group 2.4, Software Implementation Technology.

Mitglied des Programmkomitees

- Network and Distributed Systems Symposium 2023, San Diego, CA, USA.
- European Symposium on Security & Privacy 2023, in Delft, NL.
- ACM Computer and Communications Symposium (CCS), 2023, in Copenhagen, Denmark.

Prof. Dr. Michaela Geierhos

Data Science

PUBLIKATIONEN

BÄUMER, F. S., BRANDT-POOK, H., MAORO, F., SCHULTENKÄMPER, S, STECKER, B. (2023). Von der Theorie zur Praxis: Erfahrungen bei der akademischen Begleitung von KI-Projekten in KMUs. In: Klein, M.; Krupka, D.; Winter, C.; Wohlgemuth, V. (Hg.). Designing Futures: Zukünfte gestalten. Informatik 2023. Lecture Notes in Informatics (LNI) – Proceedings. Köllen Druck+Verlag Bonn. 2023. S. 1817–1828.

BÄUMER, F. S., CHEN, W.-F., GEIERHOS, M., KERSTING, J., WACHSMUTH, H. (2023). Subproject B1: Dialogue-based Requirement Compensation and Style-adjusted Data-to-Text Generation. In: Haake, C.-J.; Meyer auf der Heide, F.; Platzner, M.; Wachsmuth, H.; Wehrheim, H. (Hg.). On-the-Fly Computing – Individualized IT-services in Dynamic Markets. Verlagsreihenschriften des Heinz Nixdorf Instituts. S. 65–84.

GEIERHOS, M. (2023). German Angst und Datensicherheit: Erwägungen über den passenden Umgang mit Patientendaten in Deutschland. In: Ferber, M.; Seidenath, B. (Hg.). Gesundheitsdaten nutzen! Für eine patientenwohlorientierte Versorgung von morgen. Aktuelle Analysen 94. Hanns-Seidel-Stiftung e.V. München. S. 88–97.

HOMMEL, W., GEIERHOS, M., KNÜPFER, M., BELLGRAU, B., SCHREIBER, U., ZAHN, J. (2023). CODE-Jahrestagung 2023: Zehn Jahre Forschung und Vernetzung im Bereich Cybersicherheit. Zeitschrift für Außen- und Sicherheitspolitik.

KERSTING, J. (2023). Identifizierung quantifizierbarer Bewertungsinhalte und -kategorien mittels Text Mining. Monographie. Universität der Bundeswehr München. 2023. 208 S.

KERSTING, J., GEIERHOS, M. (2023). Towards Comparable Ratings: Quantifying Evaluative Phrases in Physicians Reviews. In: Cuzzocrea, Al; Gusikhin, O.; Hammoudi, S.; Quix, C. (Hg.). Data Management Technologies and Applications: 10th International Conference, DATA 2021, Virtual Event, July 6—8, 2021, and 11th International Conference, DATA 2022, Lisbon, Portugal, July 11—13, 2022, Revised Selected Papers. Communications in Computer and Information Science 1860. Springer 2023. Cham, Schweiz. S. 45–65.

KERSTING, J., MAORO, F., GEIERHOS, M. (2023). Comparable Ratings: Exploring Bias in German Physician Reviews. Data & Knowledge Engineering 148. S. 102–235.

MEISSNER, A., FRÖHLICH, A., GEIERHOS, M. (2023). Keep it Simple: Evaluating Local Search-based Latent Space Editing. SN Computer Science 4, 820.

MERTEN, M.-L., WEVER, M., GEIERHOS, M., TOPHINKE, D., HÜLLERMEIER, E. (2023). Annotation Uncertainty in the Context of Grammatical Change. International Journal of Corpus Linguistics 28(3). S. 430–459.

SCHULTENKÄMPER, S., BÄUMER, F. S., GEIERHOS, M., LEE, Y. S. (2023). From Unstructured Data to Digital Twins. From Tweets to Structured Knowledge. In: Jimenez, J. M. (Hg.). Proceedings of the Thirteenth International Conference on Social Media Technologies, Communication, and Informatics (SOTICS 2023). S. 6–11.

SEEMANN, N., LEE, Y. S., HÖLLIG, J., GEIERHOS, M. (2023). Generalizability of Abusive Langue Detection Models on Homogeneous German Datasets. Datenbank-Spektrum 23(1). S. 15–25.

SEEMANN, N., LEE, Y. S., HÖLLIG, J., GEIERHOS, M. (2023). The Problem of Varying Annotations to Identify Abusive Language in Social Media Content. Natural Language Engineering 29 (6). S. 1561–1585.

ULLRICH, S., SOARES DE SOUZA, A., KÖHLER, J., GEIERHOS, M. (2023). BloomQDE: Leveraging Bloom's Taxonomy for Question Difficulty Estimation. In: Abbas, M. (Hg.). Analysis and Application of Natural Language and Speech Processing. Signals and Communication Technology. Springer 2023. Cham, Schweiz. S. 145–155.

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

KiTIE – Kooperationskompetenz im Technologietransfer: Identifikation und Evaluation von Partnern anhand von Patentinformationen

Das Projekt entwickelt ein Tool zur Identifikation von Kooperationspartnern für außeruniversitäre Forschungseinrichtungen. Das Ziel ist es, eine effektive und effiziente Partnerfindung im Technologietransfer zu ermöglichen sowie eine transparente und eigenverantwortliche Beteiligung aller Akteure zu fördern.

Gefördert durch: Bundesministerium für Bildung und Forschung (BMBF)
Laufzeit: 02/2023 – 01/2026

KI-basierter Sprachsignal-Decoder

Das Ziel dieser Machbarkeitsstudie ist die prototypische Umsetzung eines neuronalen Netzes zur Dekodierung bestehender Vocoder-Daten zur Verbesserung der Empfangsqualität.

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 – 12/2024

SFB 901 „On-the-Fly Computing“ TP: „Parametrisierte Servicespezifikation“

Im Sinne agiler, partizipativer Softwareentwicklung werden Endanwender mehr in den interaktiven Kompositionsprozess von on-the-fly zu erstellenden Software-Services miteinbezogen. Dafür muss transparent klargestellt werden, welche Anforderungen bei der Erstellung berücksichtigt wurden und auf welche verzichtet werden musste.

Gefördert durch: Deutsche Forschungsgemeinschaft (DFG)
Laufzeit: 07/2019 – 06/2023

VIKING – Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen (VIKING)

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
Laufzeit: 01/2022 – 12/2024

LEHRE

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

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

3851 **Information Retrieval (WT)**

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

MESSEN, TAGUNGEN, SEMINARE

- Cyber Awareness Training (NATO JSEC, Ulm)
- Wirtschaftsinformatik Transferforum (HSBI, Bielefeld)
- KI@BW (HSU, Hamburg)

PREISE UND AUSZEICHNUNGEN

- ICIST Best Paper Award
  Sergej Schultenkämper und Frederik S. Bäumer stellen eine Methode vor, mit der potenzielle Datenschutzrisiken in deutschen Patientenforen identifiziert werden können.

WEITERE FUNKTIONEN

- Mitglied im Fakultätsrat INF
- Mitglied in der Studiengangskommission Master Cyber-Sicherheit (seit 12/2023)
- Mitglied im Beirat „Deutsche Biographie“ der Historischen Kommission bei der BAdW
- Gutachterin für die Europäische Kommission
- Gutachterin für VDI/VDE Innovation + Technik
- Gutachterin für Fachzeitschriften, wie u. a. Health Policy

Mitglied des Programmkomitees

- ACL 2023 – Annual Meeting of the Association for Computational Linguistics
- EMNLP 2023 – Conf. on Empirical Methods in Natural Language Processing
- PATTERNS 2023 – Intl. Conf. on Pervasive Patterns and Applications
- SEMANTICS 2023 – Intl. Conf. on Semantic Systems

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

PUBLIKATIONEN

BUSCH, C., DERAVI, F., FRINGS, D., KINDT, E., LESSMANN, R., NOUAK, A., SALOMON, J., ACHCAR, M., ALONSO-FERNANDEZ, F., BACHENHEIMER, D., BETHELL, D., BIGUN, J., BRAWLEY,M., BROCKMANN, G., CABELLO, E., CAMPISI, P., CEPILOVS, A., CLEE, M., COHEN, M., CROLL, C., CZYZEWSKI, A., DORIZZI, B., DRAHANSKY, M., DROZDOWSKI, P., FANKHAUSER, C., FIERREZ, J., GOMEZ-BARRERO, M., HASSE, G., GUEST, R., KOMLEVA, E., MARCEL, S., MARCIALIS, G. L., MERCIER, L., MORDINI, E., MOUILLE, S., NAVRATILOVA, P., ORTEGA-GARCIA, J., PETROVSKA, D., POH, N., RACZ, I., RAGHAVENDRA, R., RATHGEB, C., REMILLET, C., SEIDEL, U., SPREEUWERS, L., STRAND, B., TOIVONEN, S., UHL, A.: Facilitating Free Travel in the Schengen Area. IET Biometrics, 2023.

GONZALEZ-SOLER, L. J., GOMEZ-BARRERO, M., BUSCH, C.: Towards Generalisable Facial Presentation Attack Detection Using Facial Region Ensembles. IEEE Access, 2023.

GONZALEZ-SOLER, L. J., GOMEZ-BARRERO, M., PATINO, J., TODISCO, M., EVANS, N., BUSCH, C.: Fisher Vectors for Biometric Presentation Attack Detection. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, S. 489–519, 2023.

MORALES, A., FIERREZ, J., GALBALLY, J., GOMEZ-BARRERO, M.: Introduction to Iris Presentation Attack Detection in Iris Biometrics and Recent Advances. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, S. 103–121, 2023.

RAJA, K., RAGHAVENDRA, R., VENKATESH, S., GOMEZ-BARRERO, M., RATHGEB, C., BUSCH, C.: Vision Transformers Against CNNs for Fingerprint Presentation Attack Detection: Generalizability and Explainability. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, S. 17-56, 2023.

MESSEN, TAGUNGEN, SEMINARE

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

WEITERE FUNKTIONEN

- General Chair der International Conference of the Biometrics Special Interest Group (BIOSIG, https://biosig.de/)
- 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. Udo Helmbrecht

Quanten-kommunikation

PUBLIKATIONEN

FARINA, F., RÖHRICH, S., RÖDIGER, J., KÖRFGEN, H.: QKD Key Management for Military Applications: A Study in the MuQuaNet Testbed. IST-SET-198-RSY on Quantum Technology for Defence and Security, October 3–4, 2023 – Amsterdam, Netherlands.

SCHATZ, D., ALTHEIDE, F., KÖRFGEN, H., ROSSBERG, M., SCHÄFER, G.: Virtual Private Networks in the Quantum Era: A Security in Depth Approach. SECRYPT 2023 – The 20th International Conference on Security and Cryptography, July 10–12, 2023 – Rome, Italy.

LEHRE

3695 **Quantenkommunikation (FT)**

MESSEN, TAGUNGEN, SEMINARE

- DPG-Frühjahrstagung 2023
- IST-SET-198-RSY on Quantum Technology for Defence and Security in Amsterdam
- QBN Quantum Industry Summit in Stuttgart
- BWI Quantensymposium in Berlin
- ZITiS TechZoom in München
- QR.X-Workshop zur Implementierung von Faserteststrecken für die Quantenkommunikation in Berlin

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

PUBLIKATIONEN

DIETERICH, A., SCHOPP, M., STIEMERT, L., STEININGER, C., PÖHN, D.: Evaluation of Persistence Methods Used by Malware on Microsoft Windows Systems. Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP). Setúbal: SciTePress. 2023. S. 552–559.

DIMARATOS, A., PÖHN, D.: Evaluation Scheme to Analyze Keystroke Dynamics Methods. In: Mori, Paolo; Lenzini, Gabriele; Furnell, Steven (Ed.). Proceedings of the 9th International Conference on Information Systems Security and Privacy – ICISSP. Setúbal: SciTePress. 2023. S. 357–365.

EIPPER, A., PÖHN, D.: How to Design a Blue Team Scenario for Beginners on the Example of Brute-Force Attacks on Authentications. In: Mori, Paolo; Lenzini, Gabriele; Furnell, Steven (Ed.). Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP). Setúbal: SciTePress. 2023. S. 477–484.

FRANK, A., HOMMEL, W., HOPFNER, B.: An Intermediary Protocol Representation to Aid in Avionics Network Development. Proceedings of IEEE/IFIP Network Operations and Management Symposium 2023. Piscataway, NJ. IEEE. 2023. S. 1–5.

GAMISCH, L., PÖHN, D.: A Study of Different Awareness Campaigns in a Company. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery. 2023. S. 68.

HAFNER, L., WUTZ, F., PÖHN, D., HOMMEL, W.: TASEP: A Collaborative Social Engineering Tabletop Role-playing Game to Prevent Successful Social Engineering Attacks. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery. 2023. S. 67.

MAKOWSKI, J.-P., PÖHN, D.: Evaluation of Real-World Risk-based Authentication at Online Services Revisited. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA. Association for Computing Machinery. 2023. S. 73.

PÖHN, D., GRABATIN, M., HOMMEL, W.: Modeling the Threats to Self-sovereign Identities. in: Roßnagel, Heiko; Schunck, Christian H.; Günther, Jochen (Ed.). Open Identity Summit 2023. Bonn. Gesellschaft für Informatik e.V. 2023. S. 85–96.

PÖHN, D., GRUSCHKA, N., ZIEGLER, L., BÜTTNER, A.: A Framework for Analyzing Authentication Risks in Account Networks. Computers & Security. Vol. 135. 2023. S. 103515.

PÖHN, D., HOMMEL, W.: New Directions and Challenges within Identity and Access Management. IEEE Communications Standards Magazine. Piscataway, NJ. IEEE. Vol. 7. 2023. No. 2. S. 84–90.

PÖHN, D., HOMMEL, W.: Towards an Improved Taxonomy of Attacks Related to Digital Identities and Identity Management Systems. Security and Communication Networks. 2023. Special Conference Issue: Interdisciplinary and Sustainable Cybersecurity.

PÖHN, D., MÖRSDORF, N., HOMMEL, W.: Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation. ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery. 2023. S. 91.

PÖHN, D., SEEBER, S., HOMMEL, W.: Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures. Applied Sciences. Vol. 13. 2023. No. 4. S. 2349.

TEUSCHEL, M., PÖHN, D., GRABATIN, M., DIETZ, F., HOMMEL, W., ALT, F.: 'Don't Annoy Me With Privacy Decisions!' — Designing Privacy-preserving User Interfaces for SSI Wallets on Smartphones. IEEE Access. Piscataway, NJ. IEEE. Vol. 11. 2023. S. 131814–131835.

WALKOW, M., PÖHN, D.: Systematically Searching for Identity-Related Information in the Internet with OSINT Tools. In: Mori, Paolo; Lenzini, Gabriele; Furnell, Steven (Ed.). Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP). Setúbal: SciTePress. 2023. S. 402–409.

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.

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

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.

Drittmittelgeber: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021 – 12/2024

ROLORAN – Resilient Operation of LoRa Networks

Als weitreichende, energieeffiziente Funktechnologie bietet LoRaWAN eine vielversprechende Grundlage für beständige Langstreckenkommunikation. Dieses Projekt untersucht die Robustheit und Grenzen von LoRaWAN durch experimentelle und theoretische Analysen, unterstützt durch Softwarehärtung die Protokollsicherheit und zeigt

durch die Entwicklung ausgewählter Prototypen und Aufbau exemplarischer IoT-Infrastrukturen die Anwendbarkeit.

Drittmittelgeber: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021 – 12/2024

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

LEHRE

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)**

WEITERE FUNKTIONEN

- 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.-Ing. Mark Manulis

Forschungsgruppe Privacy and Applied Cryptography Lab

PUBLIKATIONEN

GARDHAM, D., MANULIS, M.: Generalised Asynchronous Remote Key Generation for Pairing-based Cryptosystems. Applied Cryptography and Network Security – 21st International Conference, ACNS 2023, Kyoto, Japan, June 19-22, 2023, Proceedings, Part I, Springer, 2023: S. 394–421.

FRYMANN, N., GARDHAM, D., MANULIS, M.: Asynchronous Remote Key Generation for Post-Quantum Cryptosystems, 8th IEEE European Symposium on Security and Privacy, EuroS&P 2023, Delft, Netherlands, July 3-7, 2023: S. 928–941.

FORSCHUNGSPROJEKTE

EU H2020 Projekt 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, GB

LEHRE

55481 **Modern Cryptography (WT)**

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

55631 **Private Data Processing (FT)**

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

55633 **Seminar 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
- Co-Affiliation und Betreuung von Doktoranden an der University of Surrey, Großbritannien

Mitglied des Programmkomitees

- 21st International Conference on Applied Cryptography and Network Security (ACNS) 2023
- 18th ACM Symposium on Information, Computer, and Communications Security (ACM ASIACCS) 2023
- 28th European Symposium on Research in Computer Security (ESORICS)
- International Conference on Security for Information Technology and Communications (SECITC) 2023 (Chair)

Juniorprof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

PUBLIKATIONEN

DARII, A., MOLL, M., NISTOR, M. S., PICKL, S., NOVAC, O., NOVAC, C. M., GORDAN, I. M., GORDAN, C. E.: Combination and Integration of Neuroevolution and Backpropagation Algorithms for Gaming Environment. 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). 2023.

EHRLICH, J., MOLL, M.; PICKL, S.: GTRF: Generalized Trade Reduction Framework for Double-auction Mechanisms. Operations Research Proceedings 2022. 2023.

MILANI, R., ARNOLD, J., MOLL, M., PICKL, S.: Expanding Reinforcement Learning Modeling Capabilities in Emergency Supply Distribution via Action Masking. Proceedings of the International Conference on Humanitarian Crisis Managment (KRISIS 2023). 2023.

MOLL, M., KARPUS, J., BAHRAMI, B.: Do Artificial Agents Reproduce Human Strategies in the Advisers' Game?. Operations Research Proceedings 2022. 2023.

MILANI, R., MOLL, M., PICKL, S.: Advances in Explainable Reinforcement Learning: An Intelligent Transportation Systems perspective. Explainable AI for Intelligent Transportation Systems. 2023.

MILANI, R., MOLL, M., PICKL, S.: Iterated Boxed Pigs Game: A Reinforcement Learning Approach. Operations Research Proceedings 2022. 2023.

MILANI, R., SAHIN, T., VON DANWITZ, M., MOLL, M., PICKL, S.: Automatic Concrete Bridge Crack Detection from Strain Measurements: A Preliminary Study. CRITIS 2022. Lecture Notes in Computer Science. 2023.

SCHMAUDER, C., KARPUS, J., MOLL, M., BAHRAMI, B., DEROY, O.: Algorithmic Nudging: The Need for an Interdisciplinary Oversight. Topoi 42, S. 799–807. 2023.

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)**

MESSEN, TAGUNGEN, SEMINARE

- Jahreskonferenz der Gesellschaft für Operations Research, OR2023
- Workshop der Arbeitsgruppe „Simulation und Optimierung von komplexen Systemen"
- 19th Cologne-Twente Workshop on Graphs and Combinatorial Optimization
- EU CSDP Innovation Day

WEITERE FUNKTIONEN

- Arbeitsgruppenleiter „Simulation und Optimierung komplexer Systeme", Deutsche Gesellschaft für OR

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLIKATIONEN

FABBRIZZI, S., ZHAO, X., KRASANAKIS, E., PAPADOPOULOS, S., NTOUTSI, E. (2023). Studying Bias in Visual Features Through the Lens of Optimal Transport. Data Mining and Knowledge Discovery, S. 1–32.

GHODSI, S., NTOUTSI, E. (2023). Affinity Clustering Framework for Data Debiasing Using Pairwise Distribution Discrepancy. Proceedings of the 2nd European Workshop on Algorithmic Fairness. Winterthur, Switzerland, June 7–9, 2023. CEUR Workshop Proceedings. 3442.

GKOLEMIS, V., DALAMAGAS, T., NTOUTSI, E., DIOU, C. (2023). Regionally Additive Models Explainable-by-Design Models Minimizing Feature Interactions, XAI-uncertainty Workshop, co-located with ECML PKDD 2023.

GKOLEMIS, V., DALAMAGAS, T., NTOUTSI, E., DIOU, C. (2023). RHALE, Robust and Heterogeneity-aware Accumulated Local Effects, 26th European Conference on Artificial Intelligence (ECAI 2023).

IOSIFIDIS, V., PAPADOPOULOS, S., ROSENHAHN, B., NTOUTSI, E. (2023). AdaCC: Cumulative Cost-sensitive Boosting for Imbalanced Classification. Knowledge and Information Systems, 65(2), S. 789–826.

LE QUY, T., FRIEGE, G, NTOUTSI, E. (2023). A Review of Clustering Models in Educational Data Science Toward Fairness-aware Learning. In: Peña-Ayala, Alejandro (Ed.). Educational Data Science: Essentials, Approaches, and Tendencies. Proactive Education based on Empirical Big Data Evidence. Singapore. Springer Nature Singapore. S. 43–94.

LE QUY, T., FRIEGE, G., NTOUTSI, E. (2023). Multi-fair Capacitated Students-Topics Grouping Problem. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (S. 507–519). Cham: Springer Nature Switzerland.

PANAGIOTOU, E., NTOUTSI, E. (2023). Learning Impartial Policies for Sequential Counterfactual Explanations Using Deep Reinforcement Learning, DynXAI Workshop co-located with ECML PKDD 2023.

PANAGIOTOU, E., QIAN, H., WYNANTS, M., KRIESE, A., MARX, S., NTOUTSI, E. (2023). Explainable AI-based Generation of Offshore Substructure Designs, ISOPE International Ocean and Polar Engineering Conference. The Society of Petroleum Engineers (SPE). S. ISOPE-I-23-045.

QIAN, H., PANAGIOTOU, E., MARX, S., NTOUTSI, E. (2023). Data-Based Conceptual Design of Offshore Jackets Using a Self-Developed Database. ISOPE International Ocean and Polar Engineering Conference. The Society of Petroleum Engineers (SPE). S. ISOPE-I-23-154.

ROY, A., HORSTMANN, J., NTOUTSI, E. (2023). Multi-dimensional Discrimination in Law and Machine Learning-A Comparative Overview. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, S. 89–100.

FORSCHUNGSPROJEKTE

BIAS – Voreingenommenheit und Diskriminierung in Big Data. Philosophische Einschätzungen, rechtliche Dimensionen und technische Lösungen

Wir haben im Zusammenhang mit KI relevante Konzepte und Prinzipien (Bias, Diskriminierung, Fairness) philosophisch analysiert, ihre adäquate Rezeption in dem einschlägigen Rechtsrahmen (Datenschutz-, Verbraucher-, Wettbewerbs-, Antidiskriminierungsrecht) untersucht und konkrete technische Lösungen (Entschärfungsstrategien, Verfahren zur Erkennung von Diskriminierung u. ä.) entwickelt.

Gefördert durch: VolkswagenStiftung
Laufzeit: 12/2018 – 05/2023

Hephaestus – Maschinelles Lernen für adaptive Prozessplanung von 5-Achs-Fräsen

Das Projekt erforscht ein Rahmenwerk für die 5-Achs-Kompensation von Formfehlern in Fräsprozessen, das auf einer prozessparallelen Materialabtragssimulation und hochentwickelten maschinellen Lernstrategien (ML) basiert. Darüber hinaus soll Wissenstransfer zwischen verschiedenen Werkstückgeometrien, Fräswerkzeugen und Werkzeugmaschinen für eine verbesserte Prozessplanung untersucht werden.

Gefördert durch: DFG
Laufzeit: 04/2021 – 11/2024

MAMMoth – Multi-Attribute, Multimodale Mitigation von Vorurteilen in KI Systemen

MAMMoth konzentriert sich auf die Identifizierung und Bekämpfung von Diskriminierung in KI-Systemen in Bezug auf geschützte Attribute, was sowohl tabellarische Daten als auch komplexe Netzwerk- sowie visuelle Daten umfasst. Die entwickelten Lösungen werden in Pilotversuchen in drei relevanten Bereichen getestet: a) Finanz-/Kreditwesen, b) Identitätsmanagmentsysteme und c) akademische Bewertung.

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

LEHRE

23191 **Artificial Intelligence (WT)**

23192 **Seminar Selected topics in Artificial Intelligence and Machine Learning (WT)**

23201 **Responsible Artificial Intelligence (HT)**

23211 **Machine Learning (FT)**

23212 **Praktikum Machine Learning (WT)**

MESSEN, TAGUNGEN, SEMINARE

- Mitorganisator des BIAS-Workshops, der gemeinsam mit ECML PKDD 2023 stattgefunden hat.
- Keynote-Vortrag über Bias in KI-Systemen auf der IEEE ICCNS 2023.
- Organisation des Workshops zu Herausforderungen und Chancen der KI als Teil der CODE-Jahrestagung 2023.
- Abschlussworkshop für das Volkswagen Projekt BIAS in Hannover, April 2023.
- Teilnahme am Dagstuhl-Seminar 23431 „Network Attack Detection and Defense – AI-Powered Threats and Responses!"• Mitveranstalter des CODE-Kolloquiums im HT23 (mit Prof. Dr. Manulis).
- Eingeladener Vortrag über verantwortungsvolle KI im Club der griechischen Akademiker in München.
- Teilnahme am Tag der offenen Tür der UniBw M im Juni 2023
- Mitorganisator des CODE-Kolloquiums im HT23 (mit Prof. Dr. Manulis)
- Ringvorlesung zum Thema „Wie Maschinen lernen und die Ambivalenzen der KI", Besuch der Hochbegabtenklasse des Maria Theresia Gymnasiums, November 2023.

WEITERE FUNKTIONEN

- Externer Beirat für den Masterstudiengang „AI in Society“ an der TU München
- Mitglied im wissenschaftlichen Netzwerk „Digitale Bioethik“, L3S
- Gutachterin für die Europäische Kommission
- Gutachterin für den Schwedischen Forschungsrat
- Gutachterin für den Nationalen Forschungsfonds Luxemburg

Mitglied des Programmkomitees

- DSAA 2023
- ECAI 2023
- ECML PKDD 2023

Prof. Dr. Stefan Pickl

Operations Research – Forschungsgruppe COMTESSA

PUBLIKATIONEN

ALONSO VILLOTA, M., WILLKOMM, E., PICKL, S. (2023). Hybrid Threats to the European Union’s Energy Sector: An Overview. In: Fathi, M., Zio, E., Pardalos, P.M. (Ed.). Handbook of Smart Energy Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-72322-4_37-1

ZHARIKOVA, M., BARBEITO, G., PICKL, S. (2023). Reliability and Risk Analysis in Critical Infrastructure Protection. In: Ram, M.; Xing, L. (Ed.). Advances in Reliability Science. Reliability Modeling with Industry 4.0. Elsevier, 2023, S. 35–43. https://doi.org/10.1016/B978-0-323-99204-6.00003-0

IFFLÄNDER, L., BUDER, T., LORETH, T., ALONSO VILLOTA, M., SCHMITZ, W., NEUBECKER, K.A., PICKL, S. (2023). Physical Attacks on the Railway System. CoRR, June 2023. https://doi.org/10.48550/arXiv.2306.00623

MILANI, R., MOLL, M., DE LEONE, R., PICKL, S. (2023). A Bayesian Network Approach to Explainable Reinforcement Learning with Distal Information. Sensors. 2023; 23(4): 2013. https://doi.org/10.3390/s23042013

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 2023

Intelligence Collection Europe together with Gerhard Conrad and Maximilian Moll „Cyber and Its Implications for Intelligence, Analysis and Decision Making“

MESSEN, TAGUNGEN, SEMINARE

- CRITIS 2023 – 18th International Conference on Critical Information Infrastructures Security
- CTW 2023 – 19th Cologne Twente Workshop on Graphs and Combinatorial Optimization
- HOLM Seminar 2023 – „Quantum-Computing in Aviation, Logistics und Mobility“

PREISE UND AUSZEICHNUNGEN

- NATO Excellence Award 2023 für die Mitarbeit im STO Specialist Team SAS169

WEITERE FUNKTIONEN

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

Prof. Dr. Daniel Slamanig

Kryptologie

PUBLIKATIONEN

CRITES, E., KOHLWEISS, M., PRENEEL, B., SEDAGHAT, M., SLAMANIG, D.: Threshold Structure-preserving Signatures. Advances in Cryptology – ASIACRYPT 2023 – 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4–8, 2023, Springer.

GÖTH, C., RAMACHER, S., SLAMANIG, D., STRIECKS, C., TAIRI, E., ZIKULNIG, A.: Optimizing 0-RTT Key Exchange with Full Forward Security. 2023 ACM Cloud Computing Security Workshop - CCSW 2023, Copenhagen, Denmark, November 26, 2023, ACM.

MIR, O., BAUER, B., GRIFFY, S., LYSYANSKAYA, A., SLAMANIG, D.: Aggregate Signatures with Versatile Randomization and Issuer-hiding Multi-authority Anonymous Credentials. 2023 ACM SIGSAC Conference on Computer and Communications Security – CCS 2023, Copenhagen, Denmark, November 26–30, 2023, ACM.

MIR, O., SLAMANIG, D., BAUER, B., MAYRHOFER, R.: Practical Delegatable Anonymous Credentials From Equivalence Class Signatures. Proc. Priv. Enhancing Technol. 2023.3.

MIR, O., SLAMANIG, D., MAYRHOFER, R.: Threshold Delegatable Anonymous Credentials with Controlled and Fine-grained Delegation. IEEE Transactions on Dependable and Secure Computing, 2023.

RÖSLER, P., SLAMANIG, D., STRIECKS, C.: Unique-path Identity-based Encryption with Applications to Strongly Secure Messaging. Advances in Cryptology – EUROCRYPT 2023 – 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Springer.

SLAMANIG, D., STRIECKS C.: Revisiting Updatable Encryption: Controlled Forward Security, Constructions and a Puncturable Perspective. Theory of Cryptography – 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 – December 2, 2023, Springer.

MESSEN, TAGUNGEN, SEMINARE

- 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2023 (Leitung der Session „Signature Schemes“).

PREISE UND AUSZEICHNUNGEN

- Top Reviewer Award bei der 30th ACM SIGSAC Conference on Computer and Communications Security – CCS 2023.

WEITERE FUNKTIONEN

- Gutachter für die Europäische Kommission
- Academic Editor für IET Information Security

Mitglied des Programmkomitees

- 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2023)
- 30th Annual ACM Conference on Computer and Communications Security (ACM CCS 2023)
- 28th Australasian Conference on Information Security and Privacy (ACISP 2023)
- 26th Information Security Conference (ISC 2023)
- 17th International Conference on Provable and Practical Security (ProvSec 2023)
- The 26th Annual International Conference on Information Security and Cryptology (ICISC 2023)
- 38th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2023)
- 18th International Workshop on Security (IWSEC 2023)
- 10th ACM Asia Public-Key Cryptography Workshop (APKC 2023)
- 23rd Central European Conference on Cryptology (CECC 2023)

Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

FORSCHUNGSPROJEKTE

MiKscHA: Mikrokernel für statische und cloud-basierte Hochsicherheits-Anwendungen

Im Projekt werden State-of-the-Art-Methoden evaluiert für den hochsicheren Betrieb von Mikrokern-basierten Anwendungen. Der Schwerpunkt liegt auf dem sicheren Start des Systems. Die verwendeten Methoden sollen ausreichen, um eine erfolgreiche Zertifizierung des Systems zu ermöglichen.

Gefördert durch: Airbus CyberSecurity
Laufzeit: 01/2021 – 12/2023

SW_GruVe: Erweiterung der Grundlagen für formale Verifikation von Software und deren Anwendung.

Ziel ist es formale Verifikation für die praktische Anwendung in der Softwareentwicklung zugänglich zu machen. Der Schwerpunkt liegt auf hardwarenaher Software in der Programmiersprache C als Teil von Betriebssystemen. Für die Verifikation werden die Programmiersprache Cogent und der Beweisassistent Isabelle eingesetzt.

Gefördert durch: Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie
Laufzeit: 10/2020 – 09/2023

LEHRE

1016 **Einführung in Betriebssysteme**

1016 **Einführung in Rechnernetze**

1026 **Verteilte Systeme**

5505 **Betriebssystemsicherheit**

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

HECK, H., WACKER, A.: Disjoint Lookups in Kademlia for Random IDs. 2023 IEEE International Conference on Autonomic Computing and Self-organizing Systems Companion (ACSOS-C), Toronto, ON, Canada, 2023, S. 47–52, doi: 10.1109/ACSOS-C58168.2023.00035.

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)**

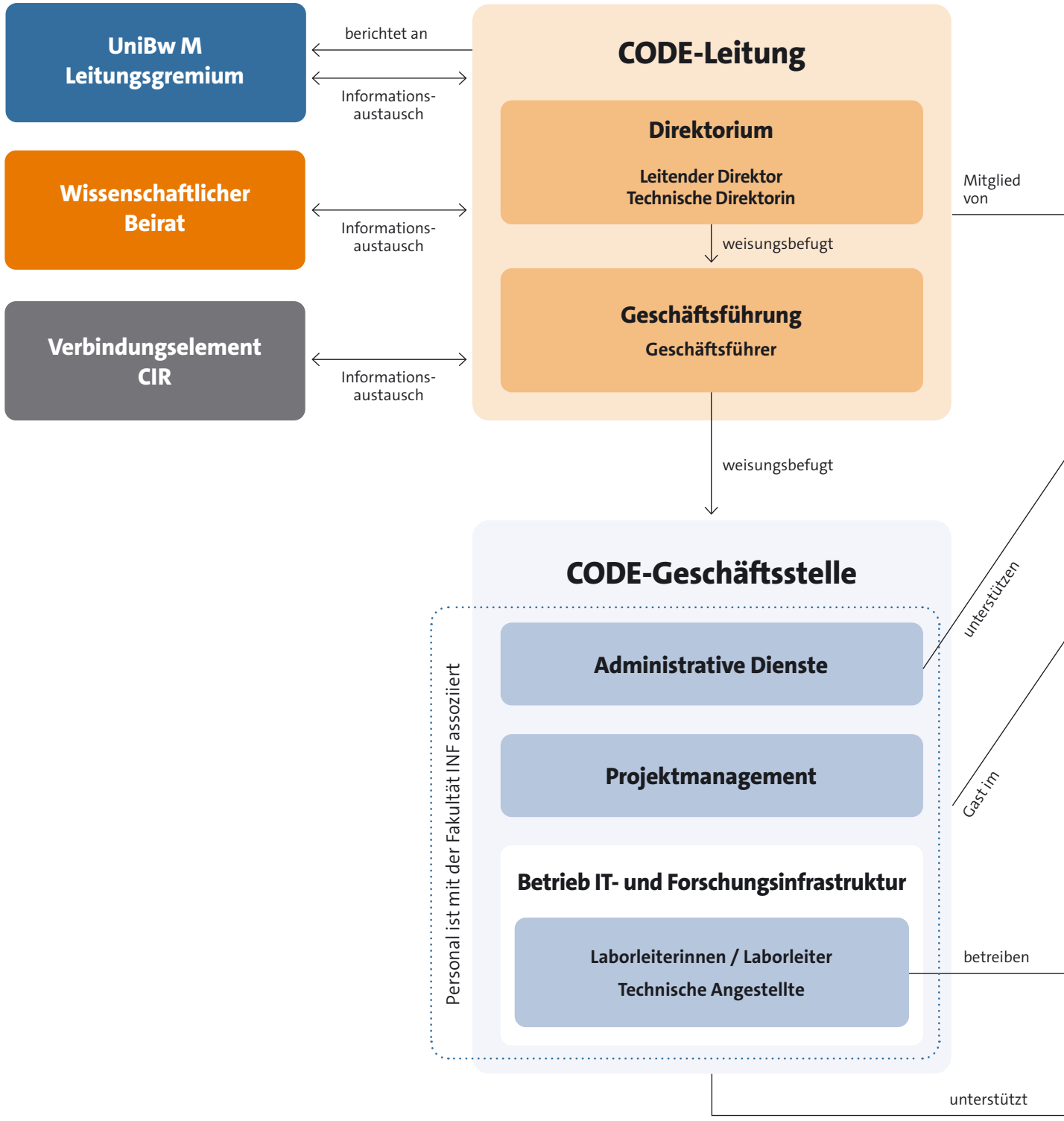
55091 **Penetration Testing (HT)**

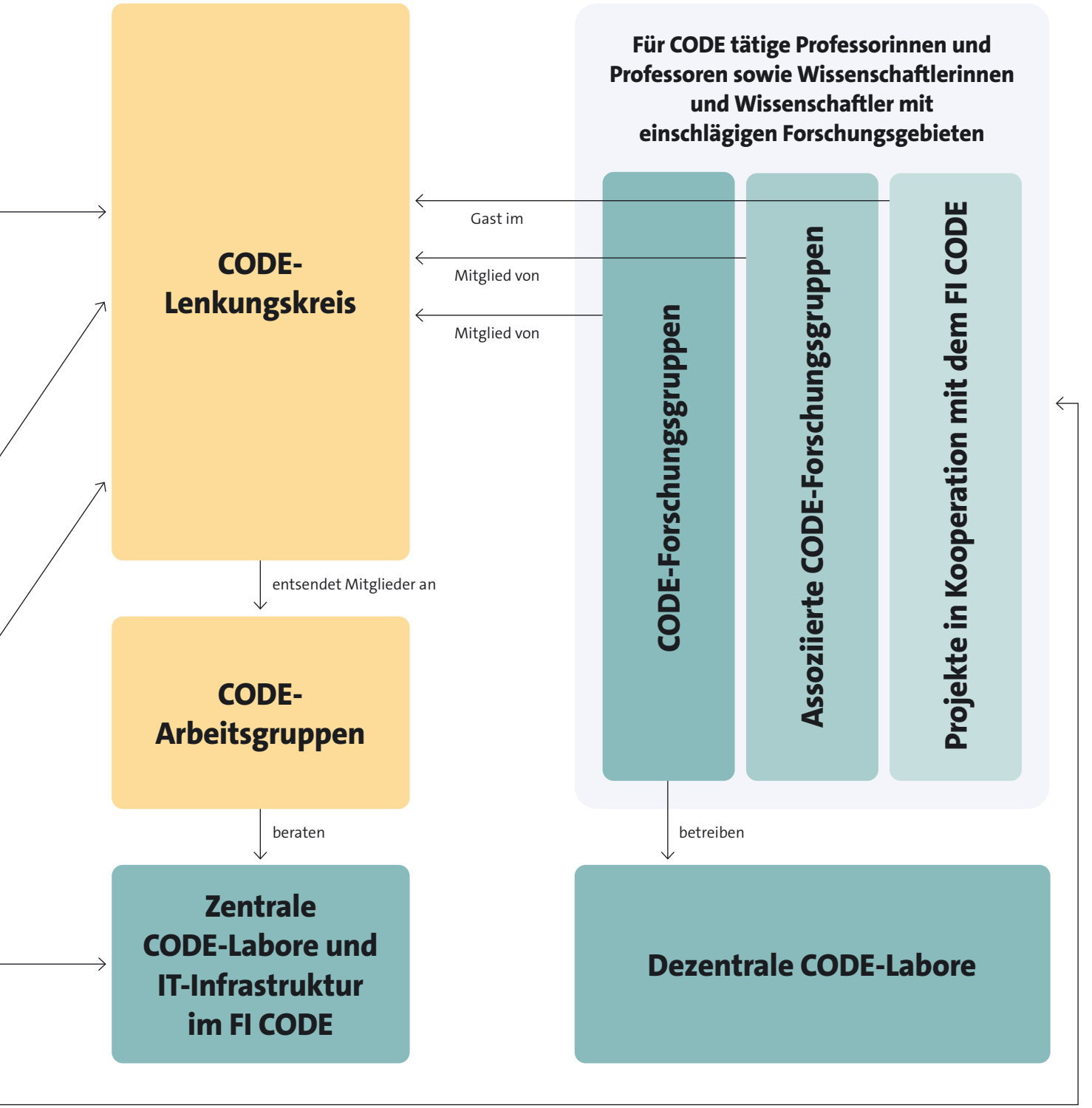
55093 **Praktikum Penetration Testing (WT + FT)**

WEITERE VERANSTALTUNGEN

- 02.03.2023, Vortrag „Von Data-at-Rest zu Domain-at-Risk“
  - Vortrag auf dem 1. IT-Grundschutz-Tag 2023 des BSI. Prof. Dr. Arno Wacker und Christoph Ruhl führten an praxisnahen Beispielen die Stärken und Grenzen der Festplattenverschlüsselung vor.
- 30. und 31.03.2023, CrypTool-Symposium
  - Anlässlich des 25-jährige Bestehens des CrypTool-Projekts fand das CrypTool-Symposium satt. Ein besonderer Programmpunkt für unsere Professur war die Übergabe der Schirmherrschaft durch Prof. Dr. Esslinger an Prof. Dr. Wacker, und somit an die Universität der Bundeswehr München.
- 20. bis 22.06.2023, HistoCrypt-Konferenz im Deutschen Museum
  - Unter der Verantwortung von Prof. Dr. Wacker fand die HistoCrypt-Konferenz dieses Jahr im Deutschen Museum statt.
- 03.07.2023, Vortrag „You‘re Being Watched – Tricks und Tools der Hacker“
  - Prof. Dr. Arno Wacker und Dr. Olga Kieselmann demonstrierten live, wo Gefahren für die eigenen Daten im alltäglichen Umgang mit der digitalen Welt lauern.
- 20.10.2023, Schülerkrypto 2023 beim Youth Science Club
  - Prof. Dr. Arno Wacker gab Mitgliedern des Youth Science Club in der Münchner Sternwarte einen einführenden Vortrag zum Thema „Kryptografie“ und stand im Anschluss für eine Vielzahl von Fragen zur Verfügung.
- 8.11.2023, Vortrag „Web(un)sicherheit“
  - Prof. Dr. Arno Wacker gewährt einen schnellen, jedoch tiefgehenden Einblick in die mannigfaltigen Angriffsmöglichkeiten auf Webanwendungen auf dem IT Security Day 2023 in Kassel.

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 22
81739 München

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

X (ehem. Twitter): @FI_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. 22
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

Prof. Dr. Harald Baier,
Professor für Digitale Forensik

Prof. Dr. Stefan Brunthaler,
Professor für sichere Softwareentwicklung

Prof. Klaus Buchenrieder, Ph.D.,
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,
Professorin für Maschinelles Lernen

Prof. Dr. Udo Helmbrecht,
Honorarprofessor am FI CODE

Prof. Dr. Wolfgang Hommel,
Professor für IT-Sicherheit von Software und Daten

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

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

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 2023)

Aus der Fakultät für Informatik der
Universität der Bundeswehr München

Prof. Klaus Buchenrieder, Ph.D.

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Weitere Mitglieder

Dr. Norbert Gaus,
Executive Vice President der Siemens AG

Prof. Dr. Johann Pongratz,
TU Dortmund

Wolfgang Sachs,
Referatsleiter CIT I.2, Bundesministerium der Verteidigung

Dr. Ralf Wintergerst,
Vorsitzender der Geschäftsführung von Giesecke+Devrient GmbH

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 2024

Titelabbildung: iStock / dem10

ISBN: 978-3-943207-85-9 | ISSN: 2748-8780

Auch erschienen als elektronische Publikation
(ISBN: 978-3-943207-86-6 | ISSN: 2748-8799)
sowie in englischer Sprache
(ISBN: 978-3-943207-87-3 | ISSN: 2748-9485).


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