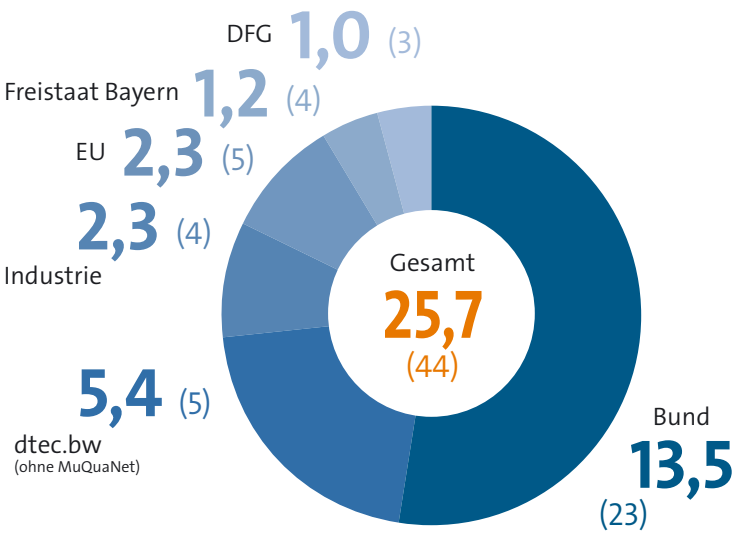

der Bundeswehr
Universität München
CODE
JAHRESBERICHT
2022
CODE FI
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Projektförderung

2022 wurden insgesamt 44 drittmittelfinanzierte Projekte am FI CODE bearbeitet oder eingeworben. dtec.bw-Projekte erhalten Mittel aus dem Etat des Geschäftsbereichs BMVg.

Drittmittel*



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

dtec.bw-Projekt**

MuQuaNet – Das Quanten-Internet im Großraum München

MuQuaNet
The Munich Quantum Network

Beteiligte Professuren

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 stammten im Jahr 2022 aus 17 Ländern.

Kooperationspartner***

Im Jahr 2022 arbeitete das FI CODE mit 80 Partnern in 25 Ländern zusammen.

Legende

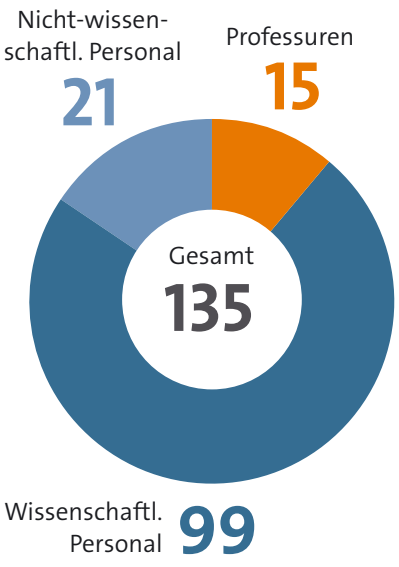
- Standort FI CODE
- 1 — Anzahl von CODE-Mitarbeitenden aus den Herkunftsländern
- 1 — Anzahl internationaler Kooperationspartner im betreffenden Land
- Länder mit Kooperationspartnern und Mitarbeitenden

*** Weitere Informationen zu Kontakten und Kooperationspartnern finden Sie ab S. 82.

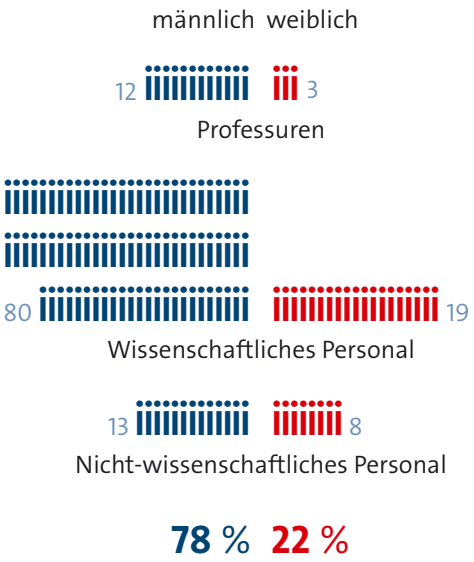
Personalstruktur

Das FI CODE hatte 2022 insgesamt 135 Mitarbeitende. Der Frauenanteil betrug 22 %.

Mitarbeitende



Geschlechteranteil

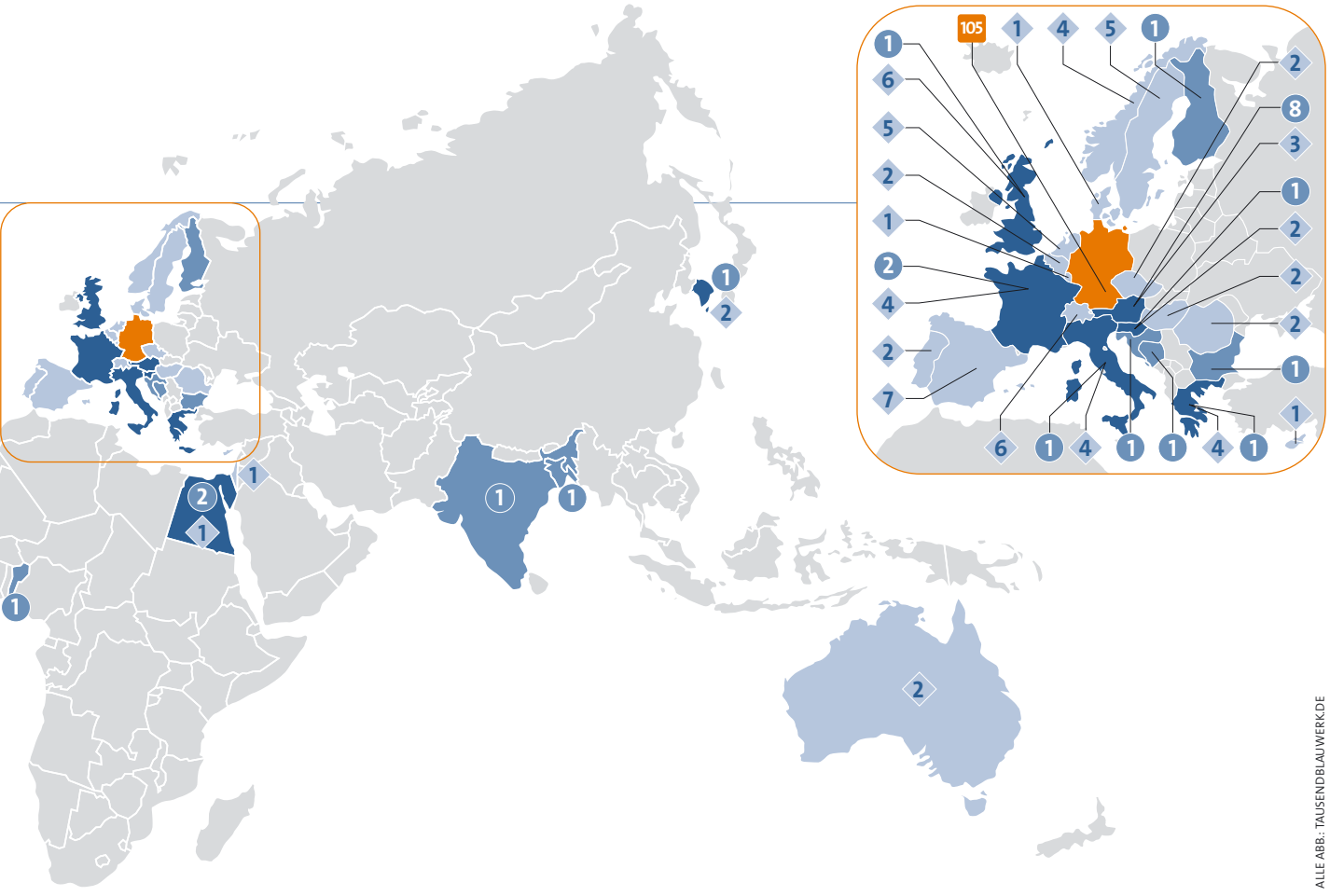


Forschungsarbeit

Übersicht der Promotionen und Publikationen am FI CODE 2022

Promotionen

Publikationen



ALLE ABB.: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
JAHRESBERICHT
2022

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Vorwort der Präsidentin

Angesichts der großen Herausforderungen durch die globalen Krisen, mit denen wir uns auseinandersetzen müssen, wird auch die Verteidigung unserer kritischen Infrastruktur und der IT-Systeme immer wichtiger. Wirtschaft, Politik, Gesellschaft und die Bundeswehr sind auf umfassende, geeignete Schutzmaßnahmen angewiesen, um im Ernstfall einen Zusammenbruch des öffentlichen Lebens zu vermeiden. Wir können stolz darauf sein, dass die Wissenschaft hier einen entscheidenden Beitrag leistet, wie der vorliegende Jahresbericht 2022 unseres Forschungsinstituts CODE für Cyber Defence und Smart Data (FI CODE) verdeutlicht.

Die Universität der Bundeswehr München hat das hybride Bedrohungsszenario viel früher als andere Hochschulen erkannt und mit „Sicherheit und Nachhaltigkeit in Technik und Gesellschaft“ ein maßgeschneidertes Profil entwickelt, um erfolgreich gegenzusteuern.

Mir ist es ein wichtiges Anliegen zu betonen, dass das FI CODE seit seiner Gründung als Forschungszentrum 2013 in diesem Bereich wertvolle Pionierarbeit leistet und innovative Lösungen findet. Zum 10-jährigen Gründungsjubiläum gratuliere ich der Institutsleitung um Wolfgang Hommel und Michaela Geierhos sowie dem gesamten Team ganz herzlich und wünsche weiterhin viel Erfolg! Ad multos annos! Besonders freut mich, dass das CODE-Jubiläum mit dem 50. Geburtstag unserer 1973 gegründeten Universität zusammenfällt, den wir in zahlreichen spannenden Veranstaltungen begehen.

Ein Blick auf die vielversprechenden Projekte und Höhepunkte des FI CODE im vergangenen Jahr zeigt, dass das Institut hervorragend aufgestellt ist. So ging der renommierte Google Faculty Award erstmalig an eine CODE-Professur. Die neue CODE-Professur (Prof. Ntoutsi) ist an zwei Horizont Europe Projekten beteiligt: Die beiden Projekte STELAR und MAMMOth starteten im Herbst 2022. Zudem wurde die Zusammenarbeit mit der Bundeswehr intensiviert: So startete Prof. Alt erstmalig ein Drittmittel-Vorhaben mit dem WIWeB, das zum Ziel hat, militärische XR-Technologien aus verschiedenen Blickwinkeln zu erforschen. Aber auch die zivile Sicherheitsforschung wurde ausgebaut mit einem neuen Verbundprojekt zur Künstlichen Intelligenz. Außerdem beteiligt sich CODE am BMBF-Leuchtturmprojekt 6G-Life (6G-Infrastruktur in Nachfolge zu 5G-Netzen).

Die Bedeutung des FI CODE spiegelt sich in der öffentlichen Wahrnehmung auch in hochrangigen Besuchen aus Politik und Bundeswehr wider. Im Dezember 2022 informierte sich etwa der Generalinspekteur der Bundeswehr persönlich über die Arbeit unseres Instituts. Im Rahmen der Übung „Locked Shields“ waren der stellvertretende Inspekteur Cyber- und Informationsraum (CIR) und ein Bundestagsabgeordneter zu Besuch am FI CODE. Von Belang ist auch der Ausbau der internationalen Kooperationen mit unseren befreundeten Partnerländern, wie Frankreich und die USA. Eine Delegation der École de l’Air et de l’Espace, der akademischen Kaderschmiede der französischen Luftstreitkräfte, besuchte unsere Universität und das FI CODE, um den Austausch in Lehre und Forschung weiter zu vertiefen.

Ich hoffe, dieser kleine Einblick in die vielfältigen und spannenden Aktivitäten des FI CODE hat Ihr Interesse an einer Lektüre des aktuellen Jahresberichts geweckt. Viel Spaß dabei!

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,

Forschung, Aus- und Weiterbildung sowie aktive Vernetzung in den Bereichen Cyber Defence, Smart Data und Quantum Technology sind die drei Schaffensschwerpunkte des FI CODE. 2022 gab es in allen drei Bereichen zahlreiche Aktivitäten, in die der vorliegende Jahresbericht einen spannenden Einblick gibt.

Als zentrale wissenschaftliche Einrichtung der UniBw M und ressorteigenes universitäres Forschungsinstitut leben wir vom Teamwork unserer Forschungsgruppen. Wir freuen uns deshalb besonders über die Verstärkung durch Prof. Dr.-Ing. Mark Manulis im März und Prof. Dr. Eirini Ntoutsi im August 2022, die die Professuren für „Privacy“ bzw. „Open Source Intelligence“ angetreten haben und seither tatkräftig ihre Forschungsgruppen aufbauen. Ein Großteil dieses Berichts, das Kapitel „Forschung“, ist entsprechend der Vorstellung unserer Forschungsgruppen und einer Auswahl aktueller Forschungsprojekte gewidmet.

Neben der forschungsnahen inhaltlichen Gestaltung unserer universitären Studiengänge wie dem Master Cyber-Sicherheit (MCYB) und der Vertiefung Cyber Defence im Master of Intelligence and Security Studies (MISS) kristallisiert sich die Cyber Range des FI CODE als wichtiges Instrument für die Weiterbildung von IT-Security-Spezialisten und Führungskräften der Bundeswehr heraus. So wurde 2022 der deutsche Anteil an der internationalen Cyber Defence Exercise „Locked Shields“ und erstmalig die Übung „Cyber Phoenix“ für Teilnehmer der deutschen und niederländischen Cyber-Reserve am FI CODE durchgeführt. Auch unser jährliches „Capture the Flag“-Event, diesmal unter dem Motto „The Spanning Tree – Catching B8tes“ erzielte mit 80 Teams im Qualifying einen erheblichen Zuwachs. Im Kapitel „Highlights“ erfahren Sie dazu Genaueres.

2022 bot aber auch die Gelegenheit, sich nach mehreren von Videokonferenzen dominierten Jahren wieder persönlich auszutauschen. Insbesondere konnten die CODE-Jahrestagung, 2022 unter dem Motto „Datengetriebene Innovation – Impulse für eine sichere Digitalisierung“, und die zusammen mit dem BMVg CIT ausgerichtete Innovationstagung Cyber/IT wieder in Präsenz auf dem Universitätscampus durchgeführt werden. Eine Zusammenfassung finden Sie in diesem Bericht, Videoaufnahmen vieler Beiträge sind auf unserer Website verlinkt.

Die Vielfalt und Vielzahl unserer Aktivitäten wäre aber ohne umfassende Unterstützung von innen und außen nicht möglich. Den Mitarbeiterinnen und Mitarbeitern in der CODE-Geschäftsstelle und allen Forschungsgruppen gebührt deshalb unser Dank für ihren engagierten und unermüdlichen Einsatz. Für die nicht nur wohlwollende, sondern insbesondere auch tatkräftige Unterstützung danken wir dem Abteilungsleiter CIT, Herrn Generalleutnant Vetter, dem Inspekteur CIR, Herrn Vizeadmiral Dr. Daum, allen unseren direkten Ansprechpartnern im BMVg und KdoCIR sowie der Leitung unserer Universität.

Wir wünschen Ihnen unterhaltsame Lektüre und freuen uns darauf, 2023 das zehnjährige Bestehen von CODE gemeinsam mit Ihnen zu feiern!

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Leitung des Forschungsinstituts CODE

ABB.: UNIBW M; A. WAGENER FOTOGRAFIE

Inhalt

ABB.: ADOBE STOCK / FERNANDO CORTÉS

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 Technologie-Entwicklung in den Themenfeldern Cyber Defence, Smart Data und Quantum Technology. Unsere Arbeit fokussiert sich dabei auf den konkreten und perspektivischen Nutzen für die Gesellschaft und die Bundeswehr. Durch unsere engen Verbindungen mit dem Organisationsbereich CIR (Cyber- und Informationsraum) der Bundeswehr sind wir in einer einzigartigen Position, durch Forschung in einer sicheren Umgebung viele Lösungen für die aktuellen und zukünftigten 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 wir täglich daran, einen wesentlichen Beitrag zum Schutz vor den Gefahren im Cyber- und Informationsraum zu leisten und sind bereit, uns daran messen zu lassen. ■

Highlights

Aus dem Institut

ABB.: ADOBE STOCK / WETTE

Reservisten aus Deutschland und den Niederlanden trainierten gemeinsam bei der Übung „Cyber Phoenix“.

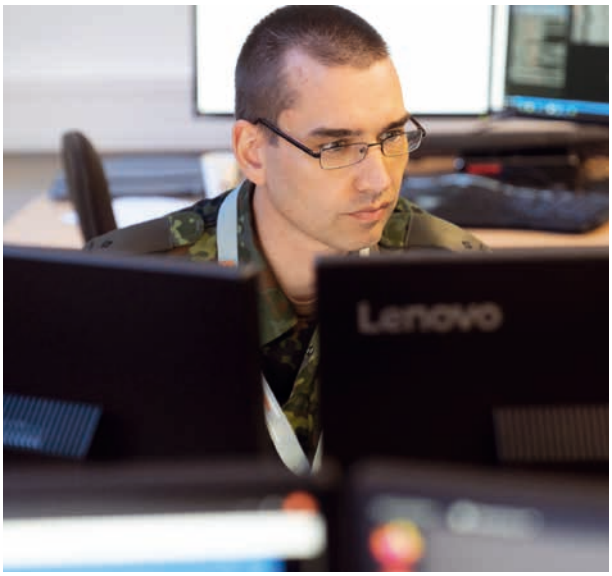
Cyber Phoenix Reserveübung am FI CODE

Die Abwehr von Angriffen trainieren

Vom 29. August bis zum 2. September 2022 fand am Forschungsinstitut CODE die Übung „Cyber Phoenix“ des Kommando Cyber- und Informationsraum (CIR) der Bundeswehr statt. Insgesamt 22 Reservisten aus den Niederlanden und Deutschland trainierten gemeinsam die Abwehr feindlicher Cyberattacken. Generalmajor Setzer und der niederländische Brigadier-General van den Berg überzeugten sich bei einem Besuch von der gelungenen Zusammenarbeit ihrer Teams.

Wissen auffrischen, aufbauen, austauschen

In den Übungsräumen der Cyber Range ICE & T des FI CODE herrschte Hochbetrieb. Fast alle Arbeitsplätze waren belegt und 22 uniformierte Reservisten saßen konzentriert vor jeweils zwei Bildschirmen. Wissen auffrischen und aufbauen, sich austauschen und gemeinsam Erfolg haben, das war das Ziel einer gemeinschaftlichen Cyberübung wie der Cyber Phoenix. In drei Individualübungen und zwei ausgefeilten mehrstündigen Szenarien hatten die Teilnehmenden aus den Niederlanden und Deutschland über fünf Tage ausreichend Gelegenheit, ihre Fähigkeiten auf die Probe zu stellen, um die Streitkräfte der beiden Länder im Ernstfall schnell und zuverlässig unterstützen zu können. Die multinational gemischten Teams bestanden aus jeweils bis zu sechs Mitgliedern, die versuchten, innerhalb einer Mission in einem fiktiven Szenario Netzwerkumgebungen gegen Cyberangriffe zu schützen.



Neben Themen der IT-Forensik waren auch komplexe Cyberabwehr-Szenarien Gegenstand der Übung.

Individuelle Übungsinhalte und direkte Betreuung

Die Inhalte der Übung Cyber Phoenix wurden von den Mitarbeitenden der Cyber Range des FI CODE erstellt. Während der ersten beiden Tage der Cyber Phoenix ging es vor allem um IT-Forensik in den Bereichen Windows, Linux und Network. Am Mittwoch und Donnerstag standen dann komplexe Szenarien mit umfangreichen Storylines im Zentrum: So musste beispielsweise ein fiktives Krankenhaus gegen eine Cyberattacke verteidigt oder Datendiebstahl über ein Mobiltelefon verhindert werden. Das CODE-Trainerteam arbeitete die Aufgaben zum Teil ganz neu für die Übung aus und passte sie auf die Bedürfnisse der Reservisten an: „Unsere Cyber Ran-

Generalmajor Jürgen Setzer und Übungsleiter August F. begrüßten am Distinguished Visitors Day weitere Reservisten zur Begehung der Übung.

BEIDE ABB.: UNIBW M / SIEBOLD

ge ist vollständig virtualisiert und flexibel einsetzbar, wodurch wir unsere Trainings sehr individuell zuschneiden können", so Marcus Knüpfer, kommissarischer Geschäftsführer des FI CODE. Für einen guten Lerneffekt bei allen Beteiligten sorgt zudem die kontinuierliche und direkte Betreuung durch die Trainerinnen und Trainer der Range.

Hochrangige Militärvertreter zu Gast bei CODE

Von der durchdachten Struktur und den aktuellen Inhalten der Übung überzeugten sich am vorletzten Tag auch Generalmajor Setzer, stellvertretender Inspekteur im Kommando Cyber- und Informationsraum, und sein niederländischer Kollege Brigadier-General van den Berg: Während des „Distinguished Visitors Day" nutzten sie die Gelegenheit, sich über die Cyber Phoenix und das FI CODE zu informieren. Bei einer Übungsbegehung kamen die beiden Generale gemeinsam mit weiteren Gästen – Cyberreservisten aus ganz Deutschland sowie militärischen Vertretern aus Peru – ins Gespräch mit den Teilnehmenden und konnten sie zu den trainierten Inhalten befragen.

Feedback-Runde zum Abschluss

Die Übung endete am Freitag mit einer gemeinsamen Abschlussrunde: Was konnten die Reservisten aus der intensiven Trainingswoche mitnehmen? Was lief gut, wo dagegen gibt es noch Verbesserungspotenzial?

Aus den unterschiedlichen Wortmeldungen ergab sich ein positiver Gesamteindruck, in dem insbesondere auch der Beitrag des CODE-Trainerteams gelobt wurde: „Danke für das hervorragende Mentoring und die gut konzipierten Inhalte mit aktuellen Sicherheitslücken! Behaltet Eure Leidenschaft beim Entwickeln", so einer der Teilnehmenden. Das ist auf jeden Fall geplant: Das FI CODE beabsichtigt, seine Fortbildungsangebote für Fach- und Führungskräfte der Bundeswehr und die Cyber-Reserve weiter auszubauen. ■

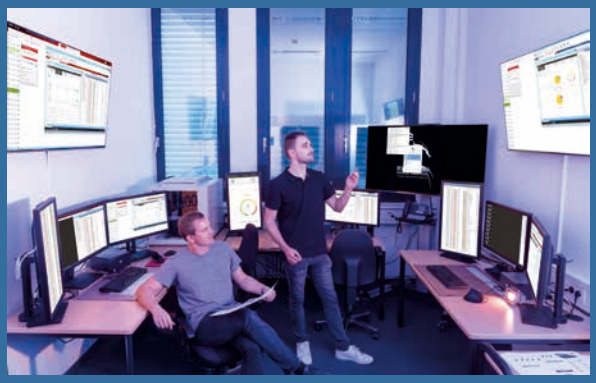
Mehr über Cyber Phoenix

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

Brigadier-General René van den Berg (links, Kommandant niederländisches Defensie Cyber Commando) und Generalmajor Jürgen Setzer (rechts, Stellvertreter Inspekteur Cyber- und Informationsraum).

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 den Trainingseinheiten 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 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

433-Qubit Osprey-Prozessor
mit 3D-Architektur.

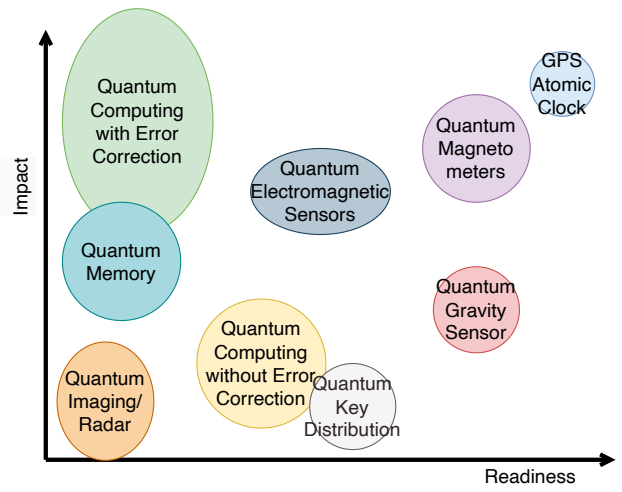
Quantentechnologien

Quanteninformations-verarbeitung mit Quantencomputern

Die experimentelle Kontrolle von Quantensystemen ermöglicht die Verarbeitung von Quanteninformationen, insbesondere durch Ausnutzung der Quanteneigenschaften der Superposition, Interferenz und Verschränkung. Anwendungen der Quantentechnologien werden in den Bereichen Navigation, Sensorik, Datenübertragung und Datenverarbeitung erwartet. Aufgrund der sich daraus ergebenden potenziellen Auswirkungen auf Verteidigung und Sicherheit hat die NATO die Quantentechnologie zu einer ihrer wichtigsten neuen und bahnbrechenden Technologien erklärt.

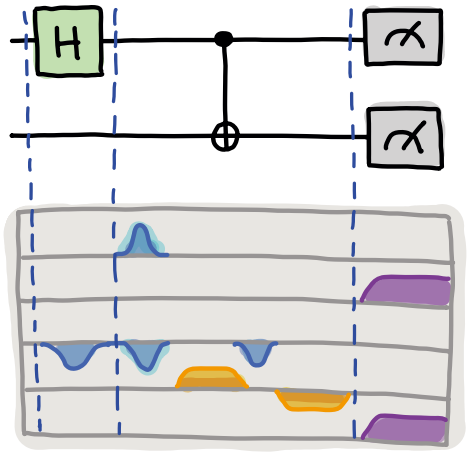
DAS RÜCKGRAT DER Quantentechnologien bildet die Quanteninformationsverarbeitung: Quantendaten aus Quantensensoren können verarbeitet und in Quantenspeichern kurz zwischengesichert werden. Quantencomputer lassen sich über Quantennetze in verteilten Systemen zusammenschließen und mit klassischen Computern verbinden. Die Quantentechnologien sind teilweise noch in einem sehr frühen Stadium und haben verschiedene Einsatzbereitschaften (Readiness) und Impact.

Das FI CODE der Universität der Bundeswehr München hat seit 2018 als IBM Quantum Hub einen exklusiven Zugang zur IBM-Quantencomputer-Infrastruktur. Die derzeitige Verfügbarkeit von kleinen, mit Rauschen behafteten Quantencomputern (bis 433 Qubits) ermöglicht es den Forscherinnen und Forschern an der Universität der Bundeswehr München, Quantenalgorithmen, Heuristiken, Fehlerkorrektur und Fehlerminderungsschemata zu testen, sowie Experimente zur Erforschung und Anwendung der Quanteninformationsverarbeitung auszuführen.



Quantentechnologien.

ABB.: CONNIE ZHOU FOR IBM; FI CODE (2)



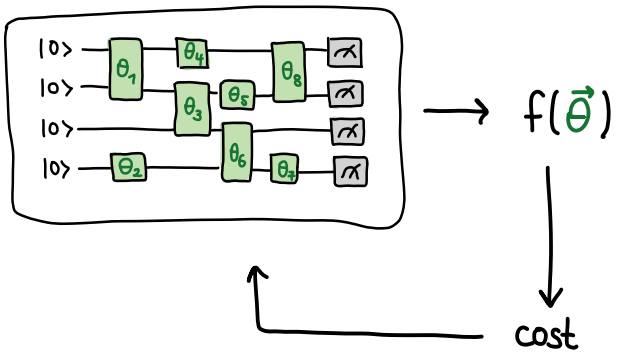
Die Quanteninformationsverarbeitung kann auf Schalkreisebene und Pulsebene auf dem IBM-Quantencomputer untersucht werden.

Die Forschung am FI CODE beschäftigt sich mit Algorithmen-Entwicklung, der Anwendung in den Bereichen Quanten-Optimierung, Quantum Machine Learning, Quanten-Simulation und Quantum Walks und der Implementierung auf den IBM-Quantencomputern mit Hilfe von Schaltkreisoptimierung und Fehlerminderungstechniken, die entwickelt werden müssen. Die Quantencomputer werden mit Qiskit, einem Software-Entwicklungskit, auf der Ebene von Schaltkreisen, Pulsen und Algorithmen programmiert und entsprechende Experimente ausgeführt.

Parallel wird das Angebot in der Lehre weiter ausgebaut und Vorlesungen, Praktika und Workshops zur Quanteninformationsverarbeitung angeboten.

Quantenoptimierung

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



Visualisierung eines Quanten-Variationsalgorithmen-Schaltkreises.

ist. Für viele dieser Probleme können nur Näherungslösungen mit Hilfe von Höchstleistungsrechnern gefunden werden.

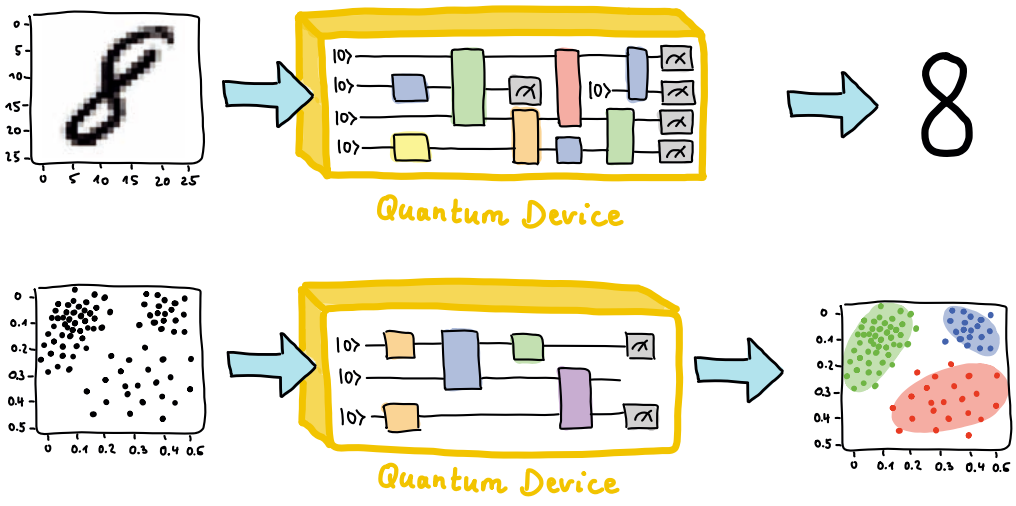
Quanten-Variationsalgorithmen ermöglichen einen lernbasierten Ansatz. Die Parameter des Schaltkreises (Gatter- oder Pulse-Parameter) werden durch Optimierung einer Kostenfunktion gefunden. Die Quanten-Variationsalgorithmen werden kontinuierlich in Theorie und experimenteller Umsetzung verbessert. Es konnte zum Beispiel gezeigt werden, dass Quantencomputer kombinatorische Optimierungsprobleme effizient und mit höherer Genauigkeit approximieren können als klassische Computer. [1]

Quantum Machine Learning

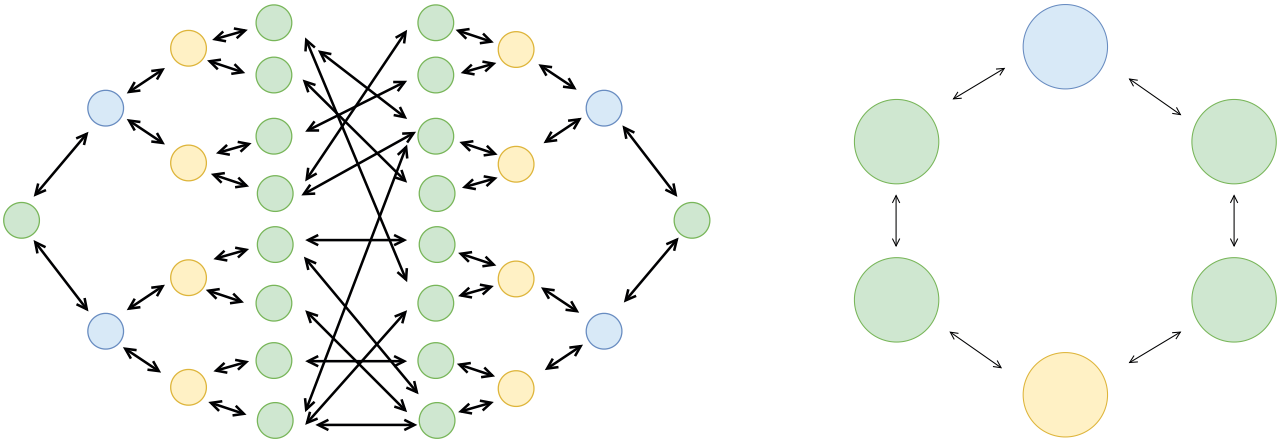
Mit Hilfe von Quanten-Variationsalgorithmen können Anwendungen des Quantum Machine Learnings realisiert werden, sowohl für klassische Daten als auch für Quantendaten, beispielsweise aus Quantensensoren.

Dazu gehören konkret Quantum Clustering, Quantum 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 Quantenalgorithmen verwendet werden können. Die Codierung klassischer Daten in Quantenzustände (Quantenschaltkreise) 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. [2]

Vor kurzem wurde 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. [3]



Visualisierung von Supervised and Unsupervised Quantum Machine Learning.



Quantum Walk auf verschiedenen Geometrien.

Quantum Random Walk

Quantum Walks sind eine leistungsfähige Technik zur Entwicklung von Quantenalgorithmen und zur Simulation komplexer Quantensysteme. 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 mögliche Anwendung für Such- und kombinatorische Optimierungsprobleme, wenn Quantum Walks in verschiedenen Geometrien, durch wiederholte stroboskopische Messungen beeinflusst werden. [4]

Quantensimulation

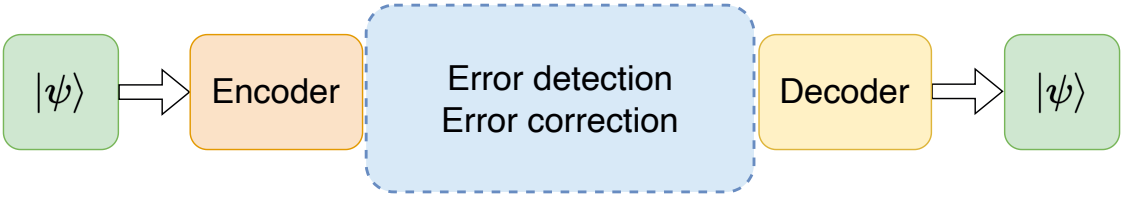
Ein universeller Quantencomputer kann ein Quantensystem nachbilden, indem er dessen natürliche Dynamik simuliert. Die Simulation dieser Systeme mit klassischen Computern ist sehr schwierig, da die benötigten Ressourcen exponentiell mit der Systemgröße anwachsen. Quantencomputer könnten diese Hürde jedoch überwinden und Lösungen in viel kürzerer Zeit liefern. Im Rahmen der Forschung am FI CODE wurden Quantenmaterialien und offene Quantensysteme auf IBM-Quantencomputern simuliert. Dies kann etwa für die Entwicklung von Energiespeichermaterialien wichtig sein. [5]

Quantum Natural Language Processing

Methoden des Quantumcomputing können auch in der Computerlinguistik angewandt werden. Dort helfen sie bei der Bestimmung von Worteinbettungen. Hierbei werden Worte durch einen Vektor in einem reellen Vektorraum repräsentiert, wobei Worte mit ähnlicher Bedeutung auf Vektoren mit geringem Abstand abgebildet werden. Nun entsprechen reine Quantenzustände Strahlen in einem komplexen Hilbertraum, dessen Skalarprodukt auf natürliche Weise zu solch einer Abstandsfunktion führt. Worteinbettungen lassen sich schließlich durch parametrisierte Quantenschaltkreise darstellen, deren Parameter mit Hilfe von Quantum Machine Learning optimiert werden können. Eine Anwendung dieses Ansatzes ermöglicht die Vorhersage eines Wortes in einem bestimmten Kontext. Diese Techniken sind ebenso adaptierbar für NISQ Geräte. [6]

Hardware-Implementierung

Zur Erforschung der Quanteninformationsverarbeitung werden verschiedene Experimente auf einem supraleitenden Quantencomputer durchgeführt, wie zum Beispiel Entanglement Measurement, Tomography,

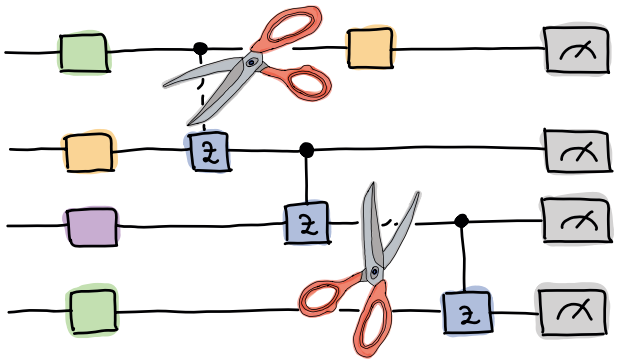


Quantum Error Correction.

ALLE ABB.: FI CODE

Quantum Optimal Control, Kalibration oder Pulse Level Programming, „Learning from Experiments“ oder Quantum Algorithmic Measurement. Außerdem können Fehlerminderungstechniken getestet werden, um die beim Ausführen von Quantencomputer-Algorithmen auftretenden Hardwarefehler zu reduzieren. Die Quantenfehlerminderung steht in Verbindung mit der Quantenfehlerkorrektur und der optimalen Quantensteuerung – zwei Forschungsbereiche, die ebenfalls darauf abzielen, die Auswirkungen von Fehlern bei der Quanteninformationsverarbeitung in Quantencomputern zu verringern.

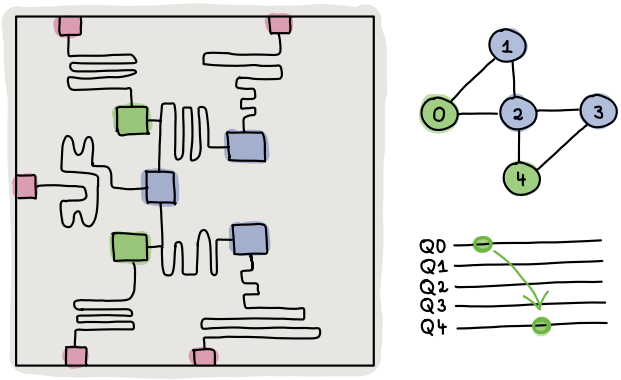
Das Quantenschaltkreismodell ist eine Abstraktion, welche die zugrunde liegende physikalische Implementierung von Gattern und Messungen auf einem Quantencomputer verbirgt. Die präzise Steuerung von echter Quanten-Hardware erfordert die Fähigkeit, Anweisungen auf der Ebene von Pulsen und Auslesungen auszuführen. „Qiskit Pulse“ kann verwendet werden, um fortgeschrittene Kontrollschemata, wie beispielsweise optimale Kontrolltheorie und Fehlerminderung, die im Schaltkreismodell nicht verfügbar sind, zu erforschen,



Quantenschaltkreise werden durch „Wire Cutting“ und „Gate Virtualization“ in kleinere Einheiten zerlegt.

indem man einen Quantencomputer direkt auf der Pulsebene programmiert. Noch ist die Tiefe von Quantenschaltkreisen, die zuverlässig auf aktuellen Quantencomputern ausgeführt werden können, durch ihre verrauschten (also durch Wechselwirkung mit der Umgebung gestörten) Operationen und die geringe Anzahl von Qubits begrenzt. So bleibt die Skalierung ein aktuell 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.

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 als verfügbar benötigt, und es können Laufzeit und Genauigkeit optimiert werden, bis es möglich ist, eine Quantenfehlerkorrektur anzuwenden.



Quantenteleportationsexperiment.

Quantencomputer in der Lehre

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

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

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

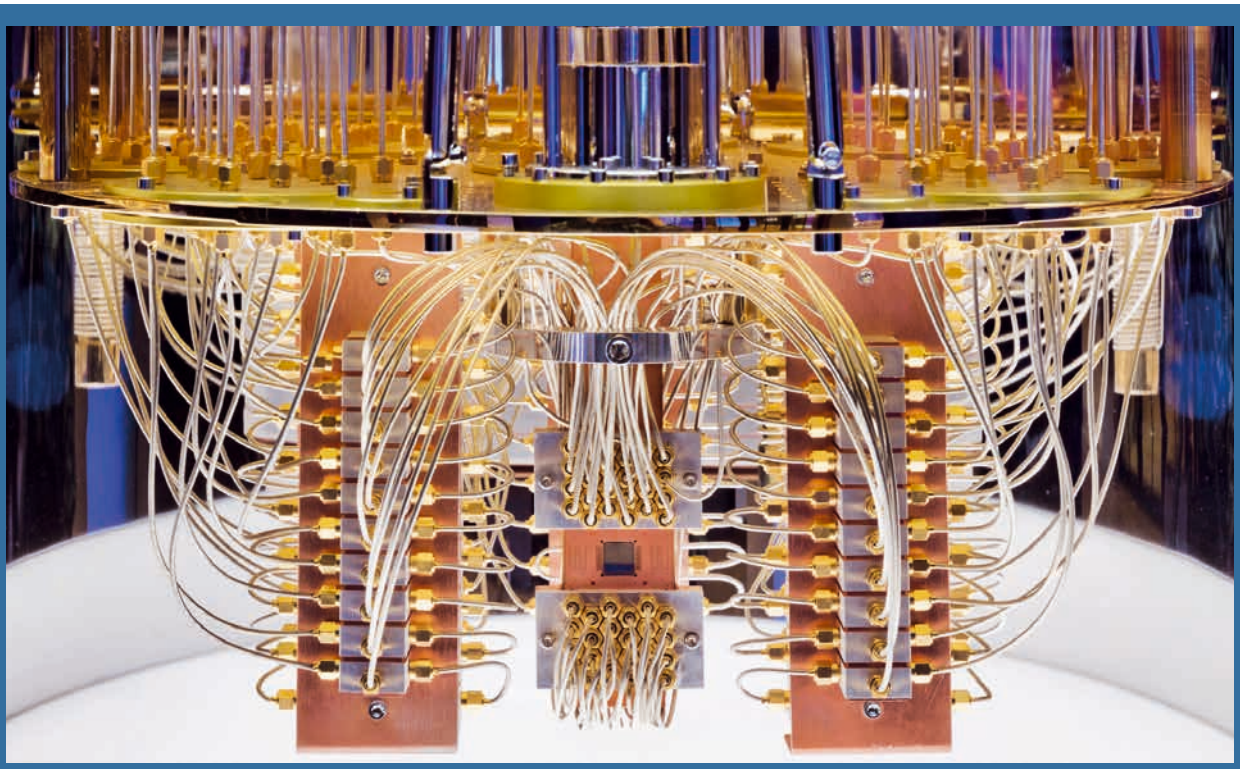
3) CEREZO, M., VERDON, G., HUANG, HY. et al.: Challenges and opportunities in quantum machine learning. Nat Comput Sci 2, pp. 567–576, 2022. https://doi.org/10.1038/s43588-022-00311-3.

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

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

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

ABB.: FI CODE (2); IBM CORPORATION



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 Quanten-Hardware 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

Bericht zur CODE-Jahrestagung 2022

Digitalisierung? Aber sicher!

Sicherheit für eine Welt, die sich immer mehr ins Digitale wandelt: Unter dem Motto „Datengetriebene Innovation – Impulse für eine sichere Digitalisierung“ nahm die Jahrestagung des Forschungsinstituts Cyber Defence und Smart Data (FI CODE) der Universität der Bundeswehr München am 12. und 13. Juli die Herausforderungen der Zukunft in den Blick.

DASS DIGITALISIERUNG nicht mehr nur ein Buzzword ist, zeigt sich an der Entwicklung der vergangenen Jahre: Spätestens seit Pandemiezeiten gehören digitale Lösungen zum (Arbeits-)Alltag von Milliarden Menschen weltweit. Videokonferenzen, virtuelle Kurse mit vernetzten Geräten und sprachbasierte Assistenzsysteme sind innerhalb kurzer Zeit Normalität geworden. Doch wie sicher sind diese Angebote, die einen zunehmend großen Einfluss auf unser Leben und Arbeiten haben? Und was sollte mit Blick auf die rasanten zukünftigen Entwicklungen bedacht werden?

Im Spannungsfeld zwischen Möglichkeiten und Risiken

Die CODE-Jahrestagung 2022 vom 12. bis zum 13. Juli auf dem Campus der Universität der Bundeswehr München widmete sich den großen Fragen der Digitalisierung und richtete den Fokus dabei insbesondere auf die Themen Cybersicherheit, Künstliche Intelligenz und Innovation.

Der erste Veranstaltungstag begann am Morgen mit der Begrüßung durch die Präsidentin der Universität der Bundeswehr München, Prof. Dr. Merith Niehuss. Es folgte ein eine Videobotschaft von Bundesverteidigungsministerin Christine Lambrecht. In ihrem Grußwort hob die Ministerin u. a. die Relevanz von Forschung im Bereich der Cybersicherheit hervor. Die sicherheitspolitische Zeitenwende infolge des Ukraine-Krieges stelle die Gesellschaft vor neue Herausforderungen und verstärke den Druck auf den digitalen Fortschritt. Insbesondere Fähigkeiten im Bereich Cyber Defence nähmen in diesem Zusammenhang eine wichtige Schlüsselrolle ein. Lambrecht betonte: „Cyber Defence reicht weit über die Bundeswehr hinaus bis tief in unsere Gesellschaft. Umso wichtiger ist es, dass sich das Forschungsinstitut CODE seit Jahren mit den drängenden Fragen des digitalen Wandels und nun auch der Zeitenwende befasst."

Nach einer Darstellung der aktuellen Entwicklungen am Forschungsinstitut CODE durch den Leitenden Direktor Prof. Dr. Wolfgang Hommel setzten am ersten Veranstaltungstag eine Reihe hochrangiger Vertreter aus verschiedenen Bundesministerien und Fachberei-

Über „Regulierung von KI und Cybersicherheit – Digitaler Aufschwung oder verpasste Chance?" diskutierten (v. l. n. r.): Lina Rusch (Moderation), GenLt Michael Vetter, Wilfried Karl, Benjamin Brake, Prof. Patrick Glauner und Dr. Arndt von Twickel.

BEIDE ABB.: FI CODE / A. WAGENER FOTOGRAFIE

chen Impulse – darunter Generalleutnant Michael Vetter (BMVg), Benjamin Brake (BMDV) und Wilfried Karl (ZITiS). Zwei kontrovers besetzte Paneldiskussionen ermöglichten lebhafte Debatten im Spannungsfeld zwischen Potenzial und Risiken der Digitalisierung: Am Vormittag des 12. Juli ging es im ersten Panel unter der Moderation von Lina Rusch (Redaktionsleiterin Tagesspiegel Background Digitalisierung und KI) um das Thema „Regulierung von KI und Cybersicherheit – Digitaler Aufschwung oder verpasste Chance?“. Die zweite Panel-Diskussion am Nachmittag unter dem Titel „Datenschutz vs. Datenschatz“ warf die Frage auf, wem große Datenmengen bei welchen Fragestellungen nützen können und dürfen. Durch das Panel führte Marc Akkermann (Infodas GmbH).

Transfer von Forschungsergebnissen in die Praxis

Ergänzend stellten die CODE-Professoren Dr. Florian Alt und Dr. Johannes Kinder ihre aktuelle Arbeit vor und schufen so die Voraussetzung für den Transfer von aktuellen Forschungsergebnissen in die Praxis. In seinem Vortrag zu „Benutzbare Sicherheit für Intelligente Umgebungen“ wies Prof. Alt auf die Problematik hin, dass in vielen Fällen menschliches Verhalten die Ursache für den durch Cyberkriminalität verursachten Schaden ist. In seinem vorgestellten Ansatz werden Sensoren genutzt, um menschliches Verhalten und physiologische Zustände in Echtzeit zu erfassen und darauf basierend bessere Sicherheitsmechanismen zu entwickeln. Anschließend ging Prof. Kinder in seiner Präsentation auf das Thema „Sicherheit für moderne Softwaresysteme“ ein. Obwohl insgesamt das Sicherheitsbewusstsein bei den Software- und Systemherstellern in den letzten Jahren erheblich gestiegen sei, biete die kontinuierlich steigende Komplexität moderner Softwaresysteme immer wieder neuartige Schwachstellen für Angreifer, so der Professor für Härtung von IT-Systemen. Seine Forschungsgruppe am FI CODE untersucht daher sowohl Software als auch Malware auf allen Ebenen – von JavaScript bis hin zu Maschinencode und Effekten der CPU-Architektur – und setzt dabei neben Techniken der formalen Programmanalyse u. a. auch Maschinelles Lernen ein.

Der erste Veranstaltungstag endete mit einem Social Event im UniCasino. Bei bestem Sommerwetter und kühlen Getränken nutzen die Teilnehmerinnen und Teilnehmer der Jahrestagung die Gelegenheit zum weiteren Austausch und Networking.

Neben dem Austausch zwischen Wissenschaft, Wirtschaft, Politik, Behörden und Bundeswehr steht auch der Wissenstransfer im Vordergrund der CODE-Jahrestagung.

Generalleutnant Michael Vetter (links, Abteilungsleiter CIT sowie CIO im BMVg) und Generalmajor Jürgen Setzer (rechts, Stellv. Inspekteur im Kommando Cyber- und Informationsraum sowie CISO der Bundeswehr) während der Tagung.

ABB.: FI CODE / A. WAGENER FOTOGRAFIE (2)

„Deep Dive“ in Zukunftsthemen

Der zweite Veranstaltungstag am 13. Juli begann mit der Begrüßung durch die Technische Direktorin des FI CODE, Prof. Dr. Michaela Geierhos, und einer Keynote des Forschungsdirektors der Agentur für Innovation in der Cybersicherheit (Cyberagentur), Prof. Dr. Christian Hummert. In seinem Vortrag wies Prof. Hummert auf die Notwendigkeit von konsequenter Trendbeobachtung hin: „Wenn eine Thematik beim Marktforschungs-Anbieter Gartner steht, ist es für uns zu spät.“ Auch der weitere Vormittag war der tiefergehenden Beschäftigung mit wichtigen Zukunftsthemen gewidmet: In insgesamt sechs abwechslungsreichen Workshops ging es etwa um Quantentechnologien, die Rolle Europas in der Cybersicherheitsforschung oder die Digitalisierung im Gesundheitswesen.

Workshop: Entwicklung der Quantentechnologien

Im Workshop „Quantentechnologien“ wurde der aktuelle Stand der Technik verschiedener Quantentechnologien thematisiert. Die Entwicklung der Quantentechnologie, wie z. B. von Quantensensoren, der Quanten-Bildgebung, von Quantenspeichern oder Quantencomputern, schreite in hohem Tempo voran und werde sowohl von nationalen Initiativen und von der Industrie massiv gefördert. Während der Pandemie wurden die nationalen Finanzierungsbemühungen, z. B. für den Bau von Quantencomputern, sogar noch weiter verstärkt. Auch die Anwendungen wurden sowohl aus Sicht der Industrie als auch der Wissenschaft ausführlich diskutiert. Hierzu zählen bspw. die Erdbeobachtung, medizinische Diagnostik, Kommunikationstechnik, Materialentwicklung, Quantenoptimierung und das Maschinelle Lernen.

Workshop: Chancen der Cybersicherheitsforschung

Der Workshop „Chancen der Cybersicherheitsforschung im Rahmen der EU- Förderprogramme ‚Horizont Europa‘ und ‚Digitales Europa‘“ stellte inhaltlich das Nationale Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS) mit seinen Plänen zur Etablierung einer nationalen Cybersicherheits-Community sowie den EU-Fördermöglichkeiten im Bereich Cybersicherheit und den dazu erforderlichen Antragsprozessen vor. Vor allem im Hinblick auf die vorgestellten EU-Fördermöglichkeiten wurden die gegenwärtigen Trends in der Cybersicherheitsforschung von den Teilnehmerinnen und Teilnehmern diskutiert. Dabei standen u. a. Fragen zu aktuellen Herausforderungen und zukünftigen Risiken im Vordergrund.

Workshop: Digitalisierung im Gesundheitswesen

Bei der Sicherstellung der Einsatzfähigkeit militärischer, aber auch ziviler Kräfte, stellt die Stressprävention einen erheblichen Faktor dar. Ziel des Smart Health Lab ist es, mit Hilfe eines interdisziplinären Projekts (Informatik, Psychologie, Sportwissenschaften) und unter Nutzung von Extended Reality-Technologien Stressprävention und Leistungssteigerung im Kontext der Einsatzvorbereitung und Prävention umzusetzen.

Dazu wird neben Grundlagenforschung auch anwendungsorientierte Forschung durchgeführt und alle relevanten Einflussfaktoren der Infrastruktur, sowie physiologische und psychologische Parameter sowohl einzeln als auch im Sinne eines Systems interagierender Bedingungen erforscht.

Zu diesem Zweck werden Techniken der Data Science und Artificial Intelligence eingesetzt, um die mittels verschiedener Sensorik erfassten physiologischen Daten zu verarbeiten. Erkenntnisse aus dem Projekt liefern wichtige Hinweise und Umsetzungsempfehlungen für ein digitalisiertes, individualisiertes Stresstraining zur Einsatzvorbereitung von Soldatinnen und Soldaten. Der Workshop führte anhand praktischer Beispiele in die Thematik ein und stellte aktuelle Herausforderungen, Untersuchungsfragen und Lösungsansätze vor.

Innovationskonferenz

Im Anschluss an die Workshops fand am Nachmittag die von der Bundeswehr ausgerichtete Innovationskonferenz Cyber- und Informationstechnologie statt. Mit Hilfe der Innovationskonferenz Cyber- und Informationstechnik will die Bundeswehr einen ganzheitlichen Weg für den Innovationsdialog Cyber/IT sowie für die bedarfsgerechte Identifikation und Einführung von IT-Innovationen im Geschäftsfeld des Bundesministeriums der Verteidigung einschlagen.

Aus den zahlreichen Einreichungen zu den relevanten Themenfeldern Cybersicherheit, Kommunikation, Geoinformation und Informationsverarbeitung hatte eine Jury vorab sechs innovative Ideen ausgewählt, welche jeweils im Rahmen eines siebenminütigen Kurzvortrages dem Fachpublikum präsentiert wurden. Die Preise, um die sich Teilnehmende aus Hochschulen, Start-Ups, Unternehmen und Verbänden bewarben, hatten eine Gesamthöhe von € 39.000.

Über den ersten Platz der Innovationskonferenz 2022 freuten sich Oberleutnant Marc A. Wietfeld (3. v. r.) und sein Team (ARX Landsysteme & Hensoldt Venture/Sensors GmbH).

Viele Gäste nutzten das Social Event im UniCasino am Abend des ersten Veranstaltungstages für weiteren Austausch und Vernetzung.

Nach den sechs einfallsreichen Pitch-Vorträgen gab es für die Tagungsgäste die Gelegenheit zur Diskussion mit den Vortragenden. Anschließend prämierte Generalleutnant Michael Vetter die Gewinner: Der erste Platz ging an Oberleutnant Marc A. Wietfeld und sein Team (ARX Landsysteme & Hensoldt Venture/Sensors GmbH), die mit „Bird's Nest" ein KI-gestütztes System zur Feuerunterstützung der Bundeswehr auf dem Gefechtsfeld entwickelten.

Auch die Plätze zwei (João Schneider, Uni Würzburg, und Lennard Rose, Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt) und drei (Kai Rehnelt, SECLOUS GmbH) zielten auf konkrete Anwendungsmöglichkeiten in der Bundeswehr ab: So wurden ein Machine-Learning-Modell zur Klassifizierung von Wasserfahrzeugen anhand von akustischen Signalen sowie eine hochsichere Infrastruktur zur effizienten Kollaboration von Bündnispartnern mit Preisen ausgezeichnet.

Ziel der CODE-Jahrestagung: Austausch und Wissenstransfer

Die Jahrestagung des FI CODE soll die interdisziplinäre Vernetzung und den Austausch zwischen Wissenschaft, Wirtschaft, Politik, Behörden und Bundeswehr fördern – ein Anspruch, dem Programm und Gäste in diesem Jahr erneut gerecht wurden: Speaker und Diskussionsteilnehmer aus Industrie, Behörden und Verbänden ermöglichten unterschiedliche Blickwinkel auf Fragestellungen rund um die Digitalisierung. Auch der am FI CODE neu etablierte Bereich Quantentechnologien sowie die Zusammenarbeit mit IBM fanden ihren Platz im Programm. Die begleitende Fachmesse bot zusätzliche Möglichkeiten für Austausch, Information und Vernetzung. ■

Mehr Informationen zur CODE-Jahrestagung

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

ABB.: FI CODE / A. WAGENER FOTOGRAFIE; FI CODE / D. PÖHN

Bericht von der CRITIS 2022

Kritische Infrastrukturen und Energiesicherheit im Fokus

Die International Conference on Critical Information Infrastructures Security (CRITIS) fand 2022 an der Universität der Bundeswehr München (UniBw M) statt. Die dreitägige Veranstaltung wurde in enger Kooperation mit dem Forschungsinstitut CODE (Cyber Defence und Smart Data) von der Forschungsgruppe COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) unter der Leitung von Prof. Dr. Stefan Pickl (Professur für Operations Research) durchgeführt.

MITTE SEPTEMBER begrüßten Prof. Stefan Pickl und der Vorsitzende des Lenkungsausschusses von CRITIS, Prof. Bernhard Hämmerli (Hochschule Luzern), mehr als 100 Teilnehmende aus Wissenschaft, Industrie, Politik, Behörden und insbesondere Betreibende von Kritischen Infrastrukturen. Die Konferenz setzte sich mit den drei zentralen wissenschaftlichen Domänen Information, Infrastrukturen und Sicherheit speziell im Kontext von Operations Research (OR)-basierten Analysen und komplexen datenbasierten Optimierungsverfahren auseinander. Für die gemeinsame exzellente Kooperation in diesem aktuellen Tehmenfeld dankte Prof. Bernhard Hämmerli insbesondere dem Honorary Chair, Prof. Dr. Udo Helmbrecht, sowie dem FI CODE.

Generalmajor a. D. Dr. Dr. Dieter Budde, Prof. Bernhard Hämmerli, Dr. Päivi Mattila, Christian Després, Prof. Stefan Pickl (v. l. n. r.).

ABB.: PIXABAY / H.HUMMEL; UNIBW M

Christian Després (l.) und Stefan Pickl stellen das SANCTUM Projekt und das internationale Konsortium vor: SANCTUM repräsentiert ein zukünftiges Krisenzentrum, das auch Reach-back-Services integriert.

Im Rahmen der Konferenz wurden die zentralen Themenbereiche unter dem Aspekt der Kritikalität von verschiedenen Seiten sowohl wissenschaftlich als auch praxisnah beleuchtet. Geleitet wurde die Konferenz vom Kompetenzzentrum COMTESSA, das von der Professur für Operations Research an der UniBw M entwickelt wurde und sich mit der Analyse und Simulation komplexer Systeme sowie der Entwicklung von Optimierungsverfahren zur IT-basierten Entscheidungsunterstützung beschäftigt.

Hybride Bedrohungen – Internationale Kooperation im EU-HYBNET

Moderiert von Generalmajor a. D. Dr. Dr. Dieter Budde (COMTESSA), wurde die Veranstaltung mit zwei eindrucksvollen Keynotes eröffnet. Dr. Päivi Mattila, Koordinatorin des Projekts EU-HYBNET, ging in ihrem Vortrag zum Thema hybride Bedrohungen im Bereich kritischer Infrastrukturen auch auf die aktuelle politische Lage ein. Diese werde gegenwärtig stark durch Russlands Angriffskrieg gegen die Ukraine und die daraus resultierende Energiekrise in Europa geprägt. Sie betonte die Bedeutung von Energieszenarien, strategischer Autonomie, OR-basierten Verfahren zum Schutz von Pipelines und speziellen Datenanalysen (indikatorbasierte Ad-hoc-Analysen). Ein Teil dieser Szenarien werde auch in enger Zusammenarbeit mit dem Forschungsinstitut CODE entwickelt.

SANCTUM – Intelligentes Krisenmanagement

In seiner Keynote erläuterte Christian Després vom französischen Ministerium für Ausrüstung, Verkehr, Ökologie und Wohnungsbau die komplexe Problematik von IT-basierter Entscheidungsunterstützung. Christian Després koordiniert das internationale Projekt SANCTUM, welches speziell die Wirksamkeit von Krisenmanagement auf Regierungsebene verbessern soll. Er zeigte auf, wie die zukunftsweisende Methodik von SANCTUM insbesondere die strategische Entscheidungsfindung optimieren kann.

Plenarvorträge

In den Plenarvorträgen präsentierten Vertreter aus den USA, Australien und Asien u. a. aktuelle Szenarien und zukunftsweisende Echtzeit-Analyseplattformen. Gerade Letztere sind angesichts der aktuellen Krise von großer Bedeutung sind, u. a. im Bereich maritimer Sicherheit. Monica Cardarilli vom Joint Research Center (JRC) der EU stellte einen „Water Security Plan" für den Schutz von Trinkwassersystemen vor. Katharina Ross (Fraunhofer Institut EMI) präsentierte in ihrem Plenarvortrag das EU-Projekt Safety4Rail.

Der Münchner Wirtschaftsreferent und Wiesn-Chef Clemens Baumgärtner (l.) begrüßte die Gäste beim Empfang im Rathaus.

Die Plenarvorträge von Bernhard Tellenbach (Cyberdefence Campus EPFL) und Maximilian Moll behandelten die Themen „Komplexe Cyberabwehr" und „Prescriptive

Virtual-Reality-Demonstration während der Bits & Bretzel-Session.

Analytics“ zum besseren Schutz von kritischen Infrastrukturen. Horia Nicolai Teodorescu gab einen Überblicksvortrag über sogenannte „Power-Side Channel Attacks“.

Eingebettet in die Konferenz fand zudem ein NATO-Workshop zu Energiesicherheit und ein hybrides Treffen der EU-Expertengruppe „Hybrid Threats“ statt.

Festlicher Höhepunkt in der BMW Welt

Gesellschaftlicher Höhepunkt der Veranstaltung war das Conference Dinner in der BMW Welt München, gegenüber dem Olympiagelände. Generalmajor a. D. Dr. Dr. Dieter Budde, der als junger Offizier während des Olympia-Attentats 1972 für besondere Schutzmaßnahmen an diesem Ort verantwortlich war, reflektierte in seiner Tischrede die Bedeutung und den Umgang mit kritischen Infrastrukturen: „Nach fünf Tagen Leichtigkeit hat sich die Welt damals schlagartig geändert …“

Auch Clemens Baumgärtner, Referent der Stadt München für Wirtschaft und Arbeit, nahm in seiner Rede beim Empfang der Konferenzteilnehmenden im Münchner Rathaus Bezug auf das Olympia-Attentat vor 50 Jahren: „Das Attentat hat damals dazu geführt, Sicherheitskonzepte komplett neu zu überdenken, vielleicht zählt deshalb München heute zu einer der sichersten Städte der Welt.“ Konferenzen wie die CRITIS tragen für ihn dazu bei, „diese Konzepte immer wieder zu verbessern.“

Bits & Bretzel – Young Scientist Awards – Echtzeitanalysen

Am letzten der drei Konferenztage fand die „Bits & Bretzel“-Session statt – ein technisches Forum, in dessen Rahmen zudem auch drei Young Scientist Awards vergeben wurden. Prof. Pickl dankte zum Abschluss allen Teilnehmenden sowie den Sponsoren und nicht zuletzt auch der Universität der Bundeswehr München. ■

Mehr Informationen zu CRITIS

https://critis2022.comtessa.org/welcome

stefan.pickl@unibw.de

ALLE ABB.: UNIBW M

ABB.: ADOBE STOCK / YOUR123

Forschung

Porträts und Projekte

Die Forschung am FI CODE

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

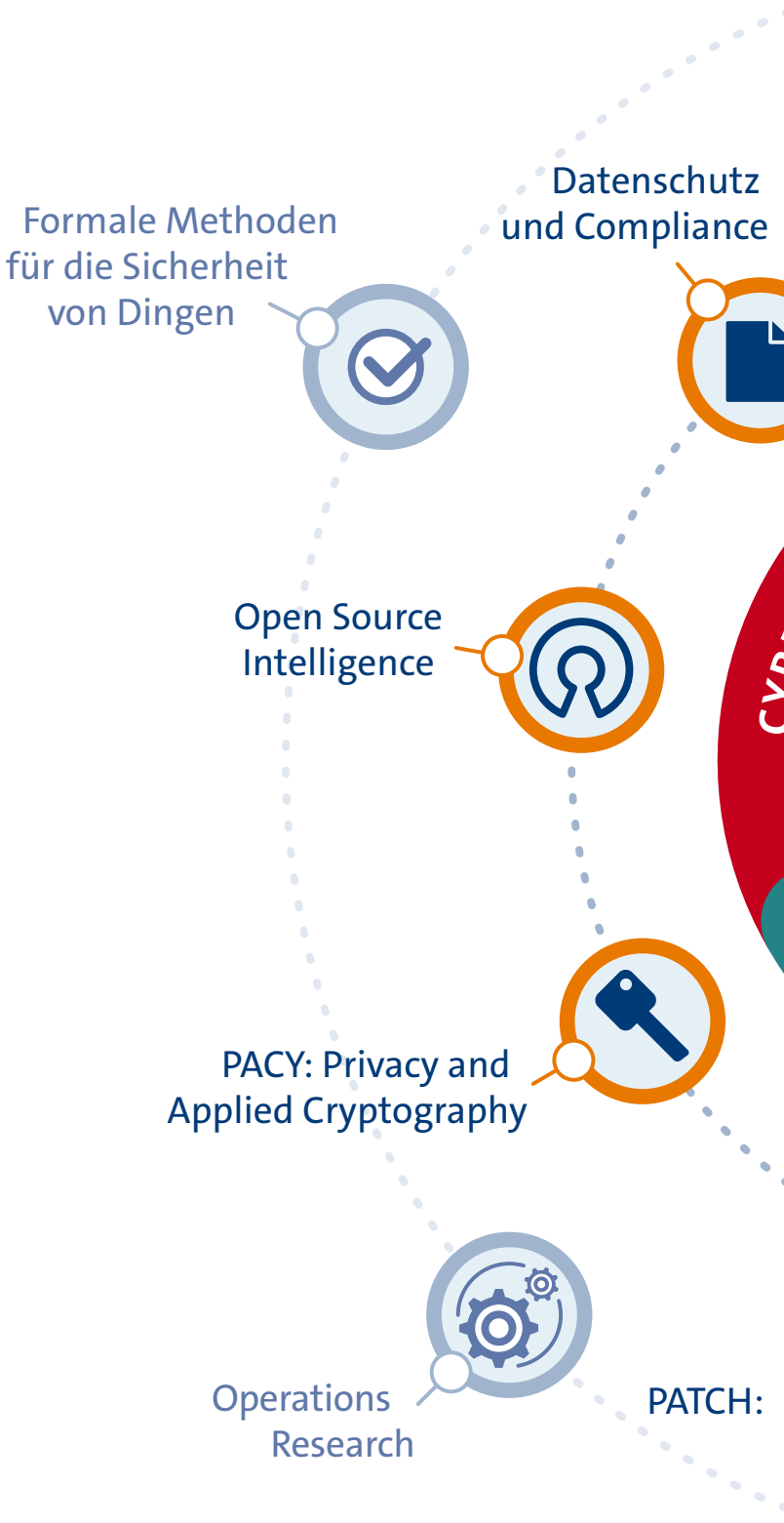
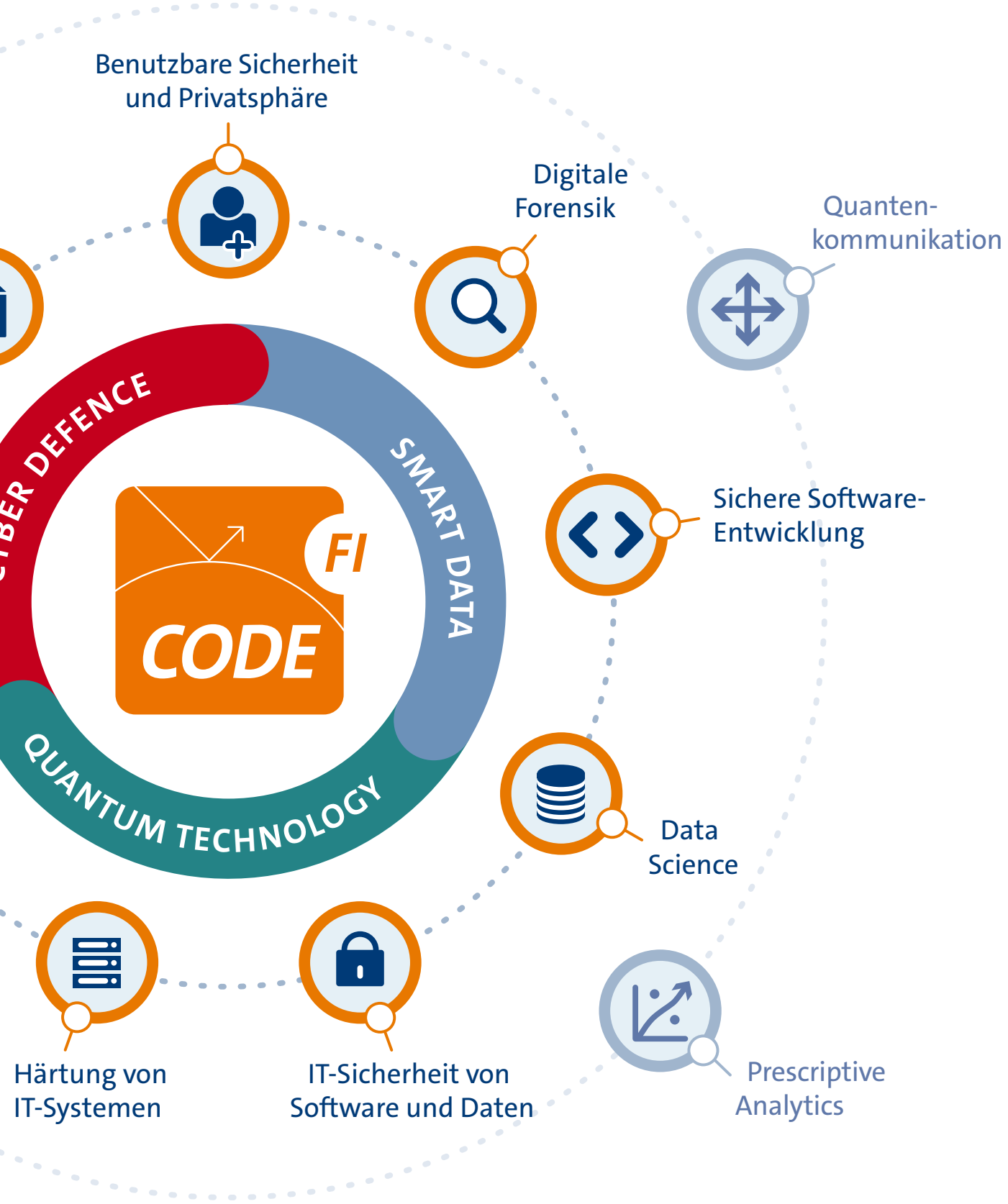


ABB.: TAUSENDBLAUWERK.DE


Benutzbare Sicherheit
und Privatsphäre
Digitale
Forensik
Quanten-
kommunikation
CYBER DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
FI
CODE
Sichere Software-
Entwicklung
Data
Science
Prescriptive
Analytics
Härtung von
IT-Systemen
IT-Sicherheit von
Software und Daten

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.

DER LEHRSTUHL 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 Datenschutzbedürfnisse bereits im Designprozess zu berücksichtigen mit dem Ziel, Sicherheits- und Datenschutzmechanismen 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 Datenschutzmechanismen basierend auf menschlichem Verhalten und menschlicher Physiologie (insbesondere der Blick), 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 Heimumgebungen, Social Engineering, Verhaltensbiometrie 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 260 in DBLP gelistete wissenschaftliche Beiträge veröffentlicht und mehr als 15 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 2022

Das Forschungsgruppe Usable Security and Privacy ist 2022 weitergewachsen und umfasst neben Prof. Dr. Florian Alt aktuell 16 Mitarbeiter und sechs wissenschaftliche Hilfskräfte. Unter den wissenschaftlichen Mitarbeitern der Forschungsgruppe befinden sich neun Promovierende und sechs Postdoktoranden, die 2022 an über 35 Publikationen mitgewirkt haben. Drei Doktoranden haben ihre Promotion sechs 2022 erfolgreich abgeschlossen.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

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

Die Forschungsgruppe für Benutzbare Sicherheit und Privatsphäre befasst sich mit Themen der Mensch-Computer-Interaktion, der IT-Sicherheit und des Datenschutzes. Neben Prof. Dr. Florian Alt umfasst sie aktuell 16 Mitarbeiter und sechs wissenschaftliche Hilfskräfte.

ABB.: ISTOCK / PHOTOTECHNO; FLORIAN ALT

Projekt Blickbasierte Sicherheitsmechanismen

Identifizierung der Wiederverwendung von Passwörtern anhand von Blick- und Tippverhalten

Benutzer müssen sich viele komplexe Passwörter merken. Daher entwickeln sie Strategien, die oft die Sicherheit beeinträchtigen. Besonders problematisch ist das Wiederverwenden von Passwörtern, da ein Angreifer so direkt Zugang zu allen entsprechenden Konten erhält. Wir erforschen, wie die Wiederverwendung von Passwörtern anhand von Blick und Tippverhalten erkannt werden kann, um Benutzer zur Verwendung sicherer Passwörter zu motivieren.

Verwendung physiologischer Daten zur Erkennung von Passwortwiederverwendung

Die Wiederverwendung von Passwörtern ist ein bekanntes Phänomen. Besonders problematisch hierbei ist, dass Benutzer selbst dann ihr Passwort nicht ändern, wenn dieses nachweislich geknackt wurde (Studien zeigen, dass innerhalb von drei Monaten nach Bekanntwerden eines Datenlecks nur 13 % der Nutzer ihr Passwort ändern). Ziel ist es also, bereits bei der Erstellung eines Passwortes zu verhindern, dass der Benutzer ein Passwort wiederverwendet. In diesem Projekt zeigen wir, dass es mittels einer Analyse von Blickdaten sowie Tippdaten von der Tastatur möglich ist, die Wiederverwendung eines Passwortes bereits bei der Registrierung vorherzusagen. Hierbei werden Methoden des maschinellen Lernens verwendet, welche es ermöglichen zu erkennen, ob ein Nutzer ein neues Passwort erstellt oder ein altes verwendet – ohne das eigentliche Passwort zu kennen.

Anhand von Verhaltensdaten kann ermittelt werden, ob ein Benutzer ein neues Passwort erstellt oder ein altes wiederverwendet. Während der Passworterstellung werden hierfür insbesondere das Blick- und Tippverhalten analysiert.

Blicke sind aussagekräftiger als Tippen

Unsere Ergebnisse zeigen, dass Tippverhalten Hinweise auf die Wiederverwendung von Passwörtern liefern. Insbesondere tippen Benutzer bei der Wiederverwendung deutlich schneller. Die Erkennungsgenauigkeit kann durch Blickdaten weiter erhöht werden. Grund ist, dass sich die kognitive Last, welche mit dem Ausdenken eines neuen Passwortes verbunden ist, im Blickverhalten (insbesondere der Pupillenweitung) widerspiegelt. Interessant ist zudem, dass Blickdaten eine Vorhersage vor der eigentlichen Eingabe eines Passwortes ermöglichen, da der kognitive Prozess bereits mit dem Aufruf der Registrierungsseite beginnt.

Datensensitivität beeinflusst die Genauigkeit der Vorhersage

Unsere Studienteilnehmer haben häufiger Passwörter für eine Website mit weniger sensiblen Daten (Benutzeraccount für eine Zeitung) wiederverwendet als für sensible Daten (E-Mail). Je sensibler also die zu schützenden Daten sind, desto mehr Mühe geben sich die Nutzer mit ihren Passwörtern und desto seltener werden sie wiederverwendet. Dies beeinflusst auch die Vorhersagegenauigkeit: bei sensitiven Daten ist eine genauere Vorhersage der Wiederverwendung von Passwörtern möglich.

Erstellen einzigartiger Passwörter

Unser System kann als Grundlage für Interventionen dienen, die Benutzer aufklären oder ihnen helfen, ein besseres, einzigartiges Passwort zu erstellen. Durch die Nutzung des Blickverhaltens kann die Wiederverwendung von Passwörtern sofort und in vielen Fällen sogar vor der Eingabe des Passworts erkannt werden. Auf diese Weise kann die Wahrscheinlichkeit erhöht werden, dass Nutzer die Empfehlungen zur Nichtwiederverwendung von Passwörtern befolgen – im Vergleich zu Ansätzen, die auf die Wiederverwendung von Passwörtern im Nachhinein hinweisen.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

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

Gefördert durch:

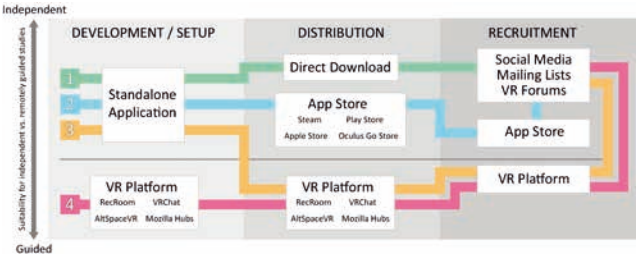
dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

Projekt Remote VR-Studien

Ein Framework für die Durchführung von entfernten Virtual-Reality-Studien

Virtual Reality (VR) Headsets werden immer häufiger in der Forschung genutzt, um etablierte Methoden zu ergänzen oder gar zu ersetzen, insbesondere für Anwendungsfälle, welche eine potenzielle Gefahr für Probanden darstellen (z. B. Benutzeroberflächen von Fahrzeugen, militärische Anwendungsfälle). Die zunehmende Beliebtheit von VR-Geräten unter Verbrauchern bietet Forschern nun zudem die Möglichkeit, die VR-Forschung aus Laboren zu den Benutzern nach Hause zu verlagern und somit heterogene Zielgruppen zu erreichen.



Framework für die Durchführung von Remote Studien in Virtueller Realität.

VR-Forschung zu Hause

Dieses Projekt untersucht die Rahmenbedingungen, Herausforderungen und Chancen von Forschungsvorhaben, welche außerhalb von Laborumgebungen mit Besitzern von VR-Headsets durchgeführt werden. Ergebnis des Projekts ist ein Framework, welches unterschiedliche Wege aufzeichnet, wie entsprechende Studien technisch realisiert werden können, wie Studienanwendungen an Probenden verteilt werden können und über welche Kanäle diese für die Teilnahme rekrutiert werden können.

Gegenwärtige VR-Nutzer

Basierend auf einer Online-Umfrage haben wir zunächst die Zielgruppe untersucht um deren Kenntnisse, Motivationen und VR-Umgebungen besser zu verstehen. VR-Nutzer sind häufig männliche Gamer, die neben dem Spielen VR als soziale Plattformen und für das Treffen mit Freunden und Familie verwenden. Die deutliche Mehrheit der Teilnehmer zeigt Interesse und Bereitschaft, an Remote VR-Studien teilzunehmen. Die VR-Umgebungen sind jedoch eher heterogen hinsichtlich verwendeter Technologien und räumlichem Setup.

Unabhängige und Remote angeleitete Studien

Studien können asynchron durchgeführt werden und eine große Anzahl von Teilnehmern erreichen. Herausforderungen sind jedoch mögliche Ablenkungen (z. B. durch andere Personen im Haushalt) sowie dass es in der Regel keinen Versuchsleiter gibt, der die korrekte Durchführung der Studie überwachen und bei Fragen und Problemen Hilfestellung leisten kann. Daher ist das es ratsam, Möglichkeiten hierfür zu schaffen, was jedoch aufgrund unterschiedlicher Zeitzonen und Arbeitszeiten, ggf. eine hohe Flexibilität erfordert.

Framework für Remote VR-Studien

Für die Entwicklung und Verteilung von Remote VR-Studien bestehen verschiedene Möglichkeiten – von Stand-Alone VR-Anwendungen zum Download über App-Stores bis hin zur Verwendung einer VR-Plattform (z. B. Steam). Alle Möglichkeiten haben verschiedene Vor- und Nachteile und unterscheiden sich darin, wie Nutzerdaten erhoben werden können, wie Remote-Unterstützung realisiert werden kann und über welche Kanäle die Rekrutierung möglich ist.

Unser Framework besteht aus vier primären Ansätzen für Remote VR-Studien:

1 Entwicklung einer eigenständigen VR-Anwendung, die direkt an die Teilnehmenden verteilt wird.
2 Entwicklung einer VR-Anwendung, die über bestehende Anbieterplattformen (App-Stores) vertrieben wird.
3 Erstellung einer VR-Anwendung, welche eine API einer VR-Plattform (z. B. Rec Room, VRChat) nutzt, und dort auch hochgeladen wird.
4 Einrichtung der Studienumgebung direkt auf einer sozialen VR-Plattform und Nutzung der von den Plattformen bereitgestellten Tools.

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

ABB.: CHRISTIAN GESSNER / FI CODE; VILLE MÄKELÄ / FI CODE

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. MICROGEN

Kinderpornografie: „Nur“ Besitz oder mehr?

Vor dieser Frage stehen Ermittler tagtäglich – technische Unterstützung ist dringend notwendig.

Die Zahl der Fälle von Kinderpornografie nimmt dramatisch zu. Unsere Forschung im Bereich der Digitalen Forensik soll eine effiziente Identifizierung von selbst hergestellter Kinderpornografie unter im Internet beschafften Material ermöglichen. In einem ersten Schritt gruppieren wir Mediendateien automatisiert anhand ihrer Metadaten mit Hilfe von Data-Science-Algorithmen, um sie anschließend priorisiert bearbeiten zu können.

Visualisierung des Projektziels, Meilensteine und Anforderungen.

IM ZUSAMMENHANG mit dem Besitz von Kinderpornografie von „nur“ zu sprechen, ist provokativ, da es sich um eine Straftat handelt, die unmittelbar eine starke Reaktion der Abscheu hervorruft. Leider ist die Feststellung von Kinderpornografie für IT-Forensiker nichts Besonderes mehr, sondern der Normalfall. IT-Forensiker sind damit konfrontiert, dass sich nicht nur die Anzahl der Fälle innerhalb der letzten fünf Jahre mehr als versechsfacht hat, sondern auch die generelle Datenmenge der Fälle nimmt zu.

Die meisten dieser Fälle gehen auf automatisierte Meldungen aus den USA zurück. Plattformbetreiber, wie bspw. Facebook sind durch US-Gesetze dazu verpflichtet Daten, die bei ihnen hochgeladen werden, auf bekanntes kinderpornografisches Material zu überprüfen. Im Jahr 2021 erhielt das BKA 79.701 solcher Meldungen, dies entspricht knapp einer Meldung pro 1.000 Einwohner. Erfahrungen zeigen, dass unter diesen Verdächtigen ein mindestens einstelliger Prozentsatz von Personen ist, der selbst Kinder missbraucht hat und dies in Form von Bild- und Filmdateien dokumentiert hat. Um weiteren Kindesmissbrauch zu verhindern, muss eine Identifikation dieser Dateien höchste Priorität haben.

Ermittler betrachten dafür gerne spezifische Metadaten der kinderpornografischen Dateien und suchen nach Verbindungen zu den vom Verdächtigen benutzten Kameras oder Smartphones. Allerdings funktioniert dieses Vorgehen nicht, wenn der Verdächtigte die entsprechenden Metadaten gelöscht hat. Bei großen Datenmengen ist das Vorgehen außerdem ineffizient. Da Ermittler es mittlerweile häufig mit mehr als 100.000 Dateien mit kinderpornografischen Inhalten in nur einem einzigen Fall zu tun haben, ist eine manuelle Identifikation dieser Dateien Glückssache.

Durch unsere Forschung im Bereich der Digitalen Forensik wollen wir selbst hergestellte kinderpornografische Dateien effizient und effektiv in großen Datenmengen identifizieren. Im ersten Schritt gruppieren wir Dateien automatisiert anhand ihrer Metadaten. Hierbei verwenden wir, im Gegensatz zum üblichen Vorgehen der Ermittler, alle verfügbaren Metadaten, was unseren Ansatz resilienter gegen das Löschen bestimmter Metadaten macht. Dieses Jahr haben wir, eine erste Datenanalyse mit Hilfe neuester Data-Science-Algorithmen von ca. 4.000 öffentlich zugänglichen Bildern erstellt und bei einer Konferenz veröffentlicht. Die Ergebnisse waren vielversprechend und wir sind nun dabei unseren Ansatz zu skalieren. Unsere weiteren Schritte bestehen darin, die Gruppen zu priorisieren und Abbruchkriterien zu definieren, bei deren erreichen ein Ermittler sicher sein kann, dass es höchst unwahrscheinlich ist, noch Beweise für Kindesmissbrauch zu finden.

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

ABB.: FI CODE / S. KLIER, H. BAIER (2)

Synthetische Erzeugung von Datensätzen

Zum Testen von IT-forensischer Auswertesoftware für die Aus- bzw. Weiterbildung in der digitalen Forensik sowie zum Training maschineller Lernverfahren werden realitätsnahe, individuelle und dynamisch konfigurierbare Datensätze sowohl von persistenten Datenträgern, volatilen Hauptspeicherinhalten als auch vom zugehörigen Netzwerkverkehr benötigt. Datensätze von weiteren IT-Systemen wie Smartphones oder Drohnen sind ebenfalls von steigender Bedeutung. Solche Datensätze müssen jeweils die forensisch relevanten Spuren enthalten, sodass Forensiker und deren Werkzeuge für den späteren realen Praxiseinsatz vorbereitet sind. Die Bereitstellung solcher Datensätze ist sehr zeitaufwendig.

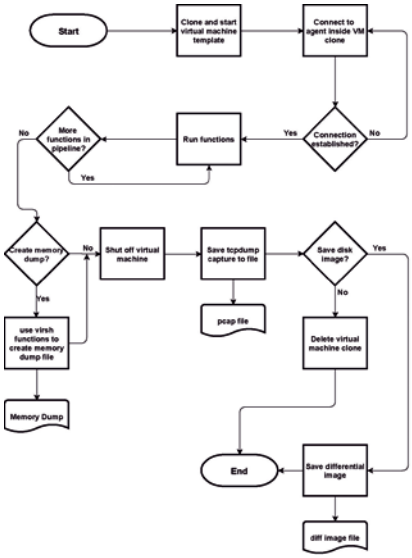
Anforderungen

An qualitativ hochwertige Datensätze werden zahlreiche Anforderungen gestellt, wie beispielsweise die Kohärenz der Datensätze – die jeweiligen digitalen Spuren müssen also im Kontext des gleichen Szenarios gemeinsam erzeugt werden, sodass komplexere forensische Analysen auf Basis mehrerer Datenquellen überhaupt erst ermöglicht werden.

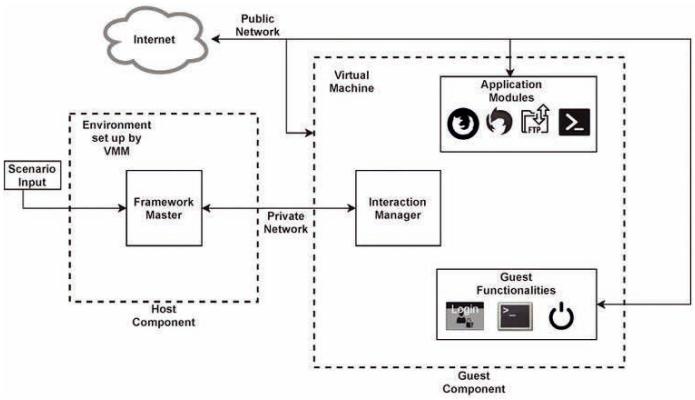
Zudem müssen die Datensätze weitere Anforderungen wie Anpassbarkeit, Verfügbarkeit, Nachvollziehbarkeit und Nachprüfbarkeit erfüllen. Ein weiterer wesentlicher Punkt für die Evaluation der Datensätze ist, dass bekannt sein muss, was die IT-forensische Software später überhaupt finden soll – das heißt, dass der Datensatz „gelabelt", also die Ground Truth bekannt ist.

ForTrace

Mit ForTrace verfolgen die Forschenden einen ganzheitlichen Ansatz bei der Datensynthese, das heißt, die Synthese von persistenten Spuren, flüchtigen Spuren und Netzwerkspuren. ForTrace ist in der Lage, verschiedene bereits vorhandene, realistische und komplexe, IT-forensisch relevante Szenarien nachzustellen oder durch das modulare Framework-Design die Datensynthese nach eigenen Wünschen dynamisch zu konfigurieren und zu erweitern. Das Framework ForTrace kann neben dem klassischen persistenten Datenträger zugleich auch volatile Arbeitsspeicherinhalte und Spuren im Netzwerk von ein und demselben in Betrachtung stehenden IT-forensischen Szenario erzeugen. Dadurch wird eine nachfolgende Multi-Source-Analyse überhaupt erst ermöglicht.



ForTrace kann mehrere virtuelle Maschinen mit unterschiedlicher Software ausrollen. Diese werden im Anschluss per separatem Netzwerkinterface mit einer Vielzahl verschiedener Steuerkommandos dazu veranlasst, Benutzerinteraktionen nachzuahmen.



Das Datensynthese-Framework ForTrace ist in der Lage, typisches Nutzerverhalten an Endsystemen nachzuahmen, um somit möglichst realistische Datensätze für die IT-forensische Auswertung automatisiert zu erzeugen.

Thomas Göbel, M.Sc.

thomas.goebel@unibw.de

+49 89 6004 7347

www.unibw.de/digfor/forschung/fortrace

Github-Link „ForTrace":
https://github.com/dasec/ForTrace

Prof. Dr. Stefan Brunthaler

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.

Die µCSRL Forschungsgruppe kann aus dem vergangenen, sehr erfolgreichen Kalenderjahr 2022 Erfreuliches berichten. Zum einen konnten wir unsere Verteidigungstechnik im Bereich AOCR Angriffe (EN: *Address Oblivious Code Reuse*) weiter ausbauen und zusätzlich konstatieren, dass auch ein weiterer moderner Angriff, nämlich PIROP, durch unsere Verteidigungstechnik substantiell erschwert wird. Dazu haben wir auch aus der akademischen Welt äußerst positives Feedback erhalten und gehen davon aus, dass unsere Arbeit im ersten Quartal 2023 auf einer hoch-kompetitiven internationalen Konferenz veröffentlicht wird. Dieses Ergebnis ist in vielerlei Hinsicht erfreulich: Unsere Arbeit widerlegt eine Kernaussage einer vorherigen Arbeit anderer Wissenschaftler, welche behauptet hatte, fundamentale Grenzen im Bereich Software Diversity aufgezeigt zu haben. Dadurch sind wir derzeit die weltweit einzige Forschungsgruppe, die gegen praktisch alle Code-Reuse Angriffe eine Verteidigung besitzt.

Zum anderen konnten wir unseren Fuzzing Cluster ebenfalls vollständig in Betrieb nehmen und haben damit auch schon erste Bugs gefunden (in unserem Fall einen Bug in „curl“). Dadurch haben wir die Weichen erfolgreich gestellt und erwarten in Zukunft auch in diesem Bereich hervorragende wissenschaftliche Resultate erarbeiten zu können.

Darüber hinaus ist es Prof. Dr. Brunthaler gelungen, einen kompetitiven internationalen Forschungsantrag im Rahmen des COMET Modul Programms der österreichischen Forschungsförderungsgesellschaft (FFG) zu gewinnen. Dabei werden gemeinsam mit Prof. Dr. Mathias Payer (EPFL), Prof. Dr. Stijn Volckaert (KU Leuven) und Prof. Dr. Rene Mayrhofer (Universität Linz) in Zusammenarbeit mit Dr. Thomas Ziebermayr vom Software Competence Center Hagenberg (SCCH) neuartige Techniken zum Kopierschutz und zur Wahrung des geistigen Eigentums erforscht. Das Projekt *Dependable Production Systems* (DEPS) hat eine lange Laufzeit bis Ende 2026 und ermöglicht es uns daher, uns eingehend mit dem Problem zu beschäftigen.

Prof. Dr. Brunthaler und sein Team haben bisher 37 Arbeiten im Systems Bereich publiziert, davon laut dem australischen CORE Ranking knapp die Hälfte in den Top Kategorien A und A*. Der Aufwand einer jeden Arbeit liegt dabei im Schnitt zwischen 15.000 und 20.000 Zeilen C/C++ Code.

Im Jahr 2022 wurde Prof. Dr. Brunthaler eingeladen, als Mitglied der Programmkomitees folgender internationaler Top Konferenzen zu dienen: *Symposium on Network and Distributed Systems Security* (NDSS 2023 in San Diego), *ACM Conference on Computer and Communications Security* (ACM CCS 2023 in Kopenhagen) und das *IEEE European Symposium on Security and Privacy* (EuroS&P 2023 in Delft). Im Frühjahr 2023 wird Herr Prof. Dr. Brunthaler auch den Vorsitz des Bereichs „System Security“ im *Journal of Systems Research* (JSys) von Prof. Dr. Payer übernehmen.

µCSRL Projekte werden gefördert vom Bundesministerium der Verteidigung, der Österreichischen Forschungsförderungsgesellschaft, dem Land Oberösterreich und der Airbus Defence & Space GmbH.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

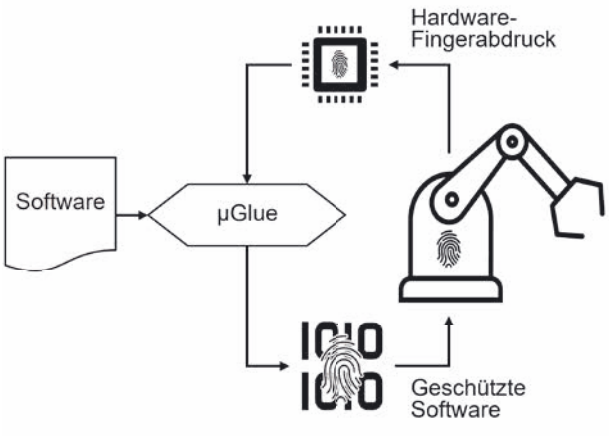
www.unibw.de/ucsrl

ABB.: ISTOCK / DE M10

Projekt µGlue

Effiziente und skalierbare Software-Hardware-Bindung unter Verwendung von Rowhammer

Der Diebstahl geistigen Eigentums verursacht jährlich einen beträchtlichen wirtschaftlichen Schaden. Während die Bauweise der Fertigungsmaschinen selbst gut gegen Diebstahl geschützt werden kann, fehlt ein ähnlich effektiver Schutz für die zugehörige Software. Mit µGlue entwickeln wir einen neuartigen Kopierschutz auf Basis von Software Diversity und Rowhammer, der sicherstellt, dass sich die geschützte Software nur auf der originalen Hardware korrekt verhält.



Um industrielles Reverse Engineering zu verhindern, generiert µGlue Programme so, dass sie zur Laufzeit einen sog. Hardware Fingerprint erwarten um korrekt ausgeführt zu werden. Ist dieser zur Laufzeit nicht vorhanden, führt das Programm anderen Code aus und führt daher die Angreifer in die Irre.

Software Diversity

Die Idee von Software Diversity ist, die innere Struktur von Programmen zu verändern, ohne jedoch ihre Funktionalität zu beeinflussen. Software Diversity macht Programme nicht nur resilienter gegenüber Schadsoftware, sondern erschwert auch das Reverse-Engineering. Insbesondere können Erkenntnisse aus der Analyse einer Programmkopie nicht mehr ohne weiteres auf eine andere Programmkopie übertragen werden, wodurch die Kosten für das Reverse-Engineering erheblich steigen.

Rowhammer

Bei Rowhammer handelt es sich um eine Technik, die Fehler ausnutzt, die in den meisten im Handel verfügbaren Arbeitsspeichermodulen auftreten. Dabei wird in einem bestimmten Muster wiederholt auf den Arbeitsspeicher zugegriffen um einen sogenannten „Bit-Flip“ zu erzeugen. Bei einem Bit-Flip ändert sich der Wert einer Speicherzelle von null zu eins oder eins zu null, obwohl auf die Speicherzelle selbst nicht zugegriffen wurde. Dieses Phänomen ist auf die kompakte Bauweise von modernen Speicherbausteinen zurückzuführen. Durch gezieltes Vermessen der Bausteine und Koordinieren der Zugriffe können Bit-Flips gezielt herbeigeführt werden.

µGlue

Im Projekt µGlue kombinieren wir die Techniken der Software Diversity mit Rowhammer um Software untrennbar mit der zugrunde liegenden Hardware zu verknüpfen. Während Rowhammer meist in Angriffen gegen Computersysteme zum Einsatz kommt, nutzen wir Rowhammer gezielt als Grundlage eines neuartigen Kopierschutzes. µGlue nutzt das für jede Speicherkonfiguration höchst individuelle Muster von Bit-Flips um den korrekten Betrieb der Software zu garantieren. Wird die Software allerdings auf einem Nachbau der Hardware ausgeführt, zeigt sie nicht mehr das gewünschte Verhalten. Dadurch können die Kosten für Reverse-Engineering derart gesteigert werden, dass der Diebstahl intellektuellen Eigentums nicht länger wirtschaftlich ist.

Bedeutung und gesellschaftliche Relevanz

µGlue hilft bei der Eindämmung von Diebstahl geistigen Eigentums und garantiert so, dass sich z. B. teure Investition in die Verbesserung von Fertigungsprozessen oder die Entwicklung von neuen Fertigungsanlagen auch weiterhin lohnen.

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

Gefördert durch:
Österreichische Forschungsförderungsgesellschaft (FFG)

ABB.: FI CODE / S. BRUNTHALER

Projekt µOI

C++ Objekt Integrität

Trotz seiner Anfälligkeit für Sicherheitslücken kommt C++ nach wie vor in einer Vielzahl von Anwendungsfeldern zum Einsatz. Unter der Vielzahl von Angriffen auf C++ Programme, kommt den sog. „Code-Reuse“ Angriffen eine besondere Bedeutung zu. Dabei missbraucht ein Angreifer bereits vorhandenen Programmcode. Ein aktueller und schwer zu erkennender Vertreter dieser Familie ist „Counterfeit Object-Oriented Programming“ (COOP). Mit µOI entwickeln wir eine Verteidigung, die sowohl statische als auch dynamische Konzepte vereint, um COOP zu verhindern.

Code-Reuse Attacks

Lange Zeit war es Angreifern möglich bei einem Angriff beispielsweise über einen Pufferüberlauf eigenen Schadcode in das angegriffene Programm einzubringen. Solch ein Vorgehen konnte durch neue Verteidungstechniken wie z. B. „Data Execution Prevention“ verhindert werden. Um solche Verteidigungen zu umgehen, haben auch Angreifer ihre Methoden weiterentwickelt. In sogenannten „Code-Reuse“-Angriffen schleusen Angreifer keinen eigenen Schadcode mehr in das Programm ein. Stattdessen werden vorhandene Programmfragmente neu zusammengeschaltet um den Angriff auszuführen.

Counterfeit Object-oriented Programming

Gegen herkömmliche „Code-Reuse“-Angriffe existieren bereits eine Reihe von effektiven Verteidigungen, wie z. B. Control-Flow Integrity oder Software Diversity.

Ein Angriffstyp namens „Counterfeit Object-Oriented Programming“ (COOP) jedoch, missbraucht gezielt die interne Struktur von C++ Programmen und bleibt von bestehenden Verteidigungen weitgehend unberührt. Bei COOP bringt ein Angreifer gefälschte C++ Objekte in den Speicher ein, um vorhandenen Programmcode missbräuchlich auszunutzen.

COOP Mitigation

Die im Zuge des Projekts µOI implementierte Verteidigung schützt die Integrität von C++ Objekten im Speicher. Ein eigens modifizierter Compiler passt dabei kompilierte C++ Programme so an, dass zur Laufzeit Prüfsummen von C++ Objekten erstellt und überprüft werden. Diese Prüfsummen verhindern, dass Angreifer unbemerkt gefälschte Objekte in den Speicher einbringen können. Dadurch werden COOP Angriffe erfolgreich verhindert.

Bedeutung und gesellschaftliche Relevanz

Unsere Verteidigung trägt dazu bei, C++ Applikationen, die auf einer Vielzahl von Geräten verwendet werden, sicherer zu machen und die Angriffsmöglichkeiten im Bereich von fortgeschrittenen CRAs einzuschränken.

Ähnlich wie bei Lösegeldbriefen, werden bei „Code-Reuse“-Angriffen vorhandene Programmcode-Fragmente so kombiniert, dass sie eine andere Funktionalität aufweisen.

ABB.: PICTURE ALLIANCE / DPA

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 vereinigt Kompetenzen aus den Bereichen Informatik, Computerlinguistik und Wirtschaftswissenschaften, um aktuellen und zukunftsorientierten Forschungsfragen auf den Gebieten des Semantic Information Processing sowie des Knowledge & Data Engineering auf den Grund zu gehen.

Angewandte Forschung

Data Science ist eine angewandte, interdisziplinäre Wissenschaft. Ihr Ziel ist es, Wissen aus Daten zu generieren, um beispielsweise Entscheidungsfindungsprozesse zu unterstützen. Es kommen Methoden und Wissen aus verschiedenen Bereichen wie Mathematik, Statistik, Stochastik, 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 von großen Datenmengen (Big Data). Dabei konzentriert sie sich auf wissensbasierte und computerlinguistische Ansätze. Dazu zählt insbesondere die Entwicklung von Algorithmen zur (semantischen) Textanalyse und das Ermöglichen von Mensch-Maschine-Kommunikation durch die Interaktion mit Informationssystemen (z. B. Freitextsuche, Frage-Antwort-Systeme). Praktische Anwendungen sind unter anderem Suchmaschinen, Social-Media-Mining-Systeme, Stimmungsanalysen und wissensbasierte Frage-Antwort-Systeme.

Praxisorientierte Lehre

Die Data-Science-Veranstaltungen basieren auf einem Lehrkonzept, welches die Theorie mit der Praxis verbindet. Die Studierenden profitieren dabei von Anfang an von der Möglichkeit, das in den Vorlesungen gesammelte theoretische Wissen in abwechslungsreichen Übungen und vielfältigen, praxisnahen Projekten direkt zur Anwendung zu bringen. Damit leistet die Professur für Data Science einen Beitrag zu der exzellenten akademischen Ausbildung der Studierenden an der Universität der Bundeswehr München.

Theorie-Praxis-Transfer

Um Theorie und Praxis auch in Forschungsfragen miteinander zu verknüpfen, pflegt das Data-Science-Team zahlreiche Kooperationen mit Partnern aus Militär, Wirtschaft und dem öffentlichen Sektor. In einer sich immer schneller wandelnden Welt sind zukunftsfähige und innovative Softwarelösungen der Schlüssel zum langfristigen Erfolg. Auch wenn die Zukunft oft ungewiss scheint, lassen sich die Mitglieder der Forschungsgruppe von Alan Kays Leitsatz aus dem Jahr 1970 inspirieren: „The best way to predict the future is to invent it."

Data Science Use Cases

Die Anwendungsgebiete erstrecken sich derzeit vom Aufdecken von Desinformationskampagnen und Hate Speech in Social Media über die Identifikation von sogenannten Deepfakes bis hin zur lagebildbasierten Krisenfrüherkennung. Ziel der aktuellen Forschung ist es, Beeinflussungskampagnen frühestmöglich zu erkennen, vor ihnen zu warnen sowie ihre Entwicklung und Verbreitung zu verfolgen, um dann letztendlich geeignete Gegenmaßnahmen einleiten zu können. Hierfür steht die Identifikation und Modellierung von kurzfristigen Desinformationskampagnen in Sozialen Medien wie Twitter, Facebook etc. im Fokus.

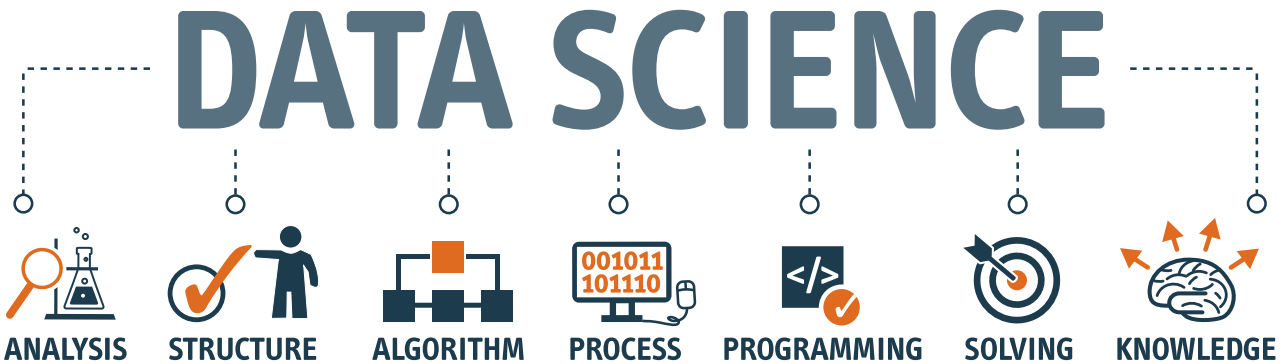
Die jüngsten technologischen Fortschritte und Entwicklungen im Bereich der Künstlichen Intelligenz (KI) haben auch sogenannte Deepfakes hervorgerufen. Hierunter wird eine mittels KI erzeugte audiovisuelle Modifikation eines Videos verstanden, in welcher das Gesicht und/oder die Aussagen der im Video dargestellten Person verändert wurden. Diese Manipulationen will die Forschungsgruppe aufdecken.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

www.unibw.de/datascience



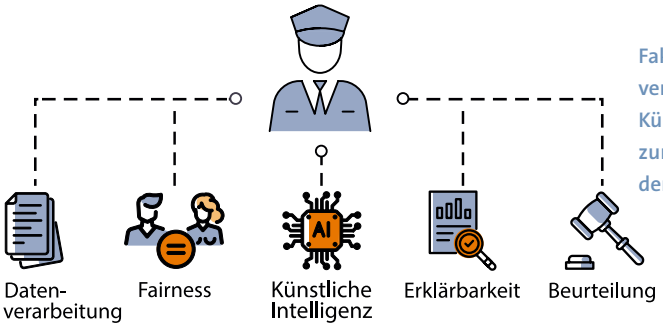
Aufgabenspektrum der Professur für Data Science.

ABB.: SHUTTERSTOCK / RYZHI, TRUEFFELPIX

Projekt VIKING

Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen

Künstliche Intelligenz wird häufig als Black-Box verstanden, bei der nicht ersichtlich ist, wie Entscheidungen zu Stande kommen, wie vertrauenswürdig eine Entscheidung ist, ob gewisse Eigenschaften von Personen zu Benachteiligungen führen und wie bzw. womit das Wissen erlernt wurde. In VIKING sollen diese Problemstellungen daher unter Beachtung von technischen, rechtlichen und ethischen Faktoren gelöst werden.



Faktoren einer vertrauenswürdigen Künstliche Intelligenz zur Unterstützung in der Polizeiarbeit.

Polizeiliche Anwendungsfälle

Den zahlreichen Möglichkeiten im Internet, sich zu vernetzen, stehen vielfältige Potentiale zum Missbrauch der Möglichkeiten für kriminelle Zwecke entgegen. Deshalb sind polizeiliche Behörden erforderlich, die sowohl Überwachung von gewissen Quellen als auch die gezielte Untersuchung von angezeigten Fällen übernehmen. Darüber hinaus untersuchen Strafverfolgungsbehörden große Datenbestände aus Texten, Bildern, Videos und strukturierten Daten aus unterschiedlichen Quellen, die z. B. bei sozialen Medien, Unternehmen oder privaten Endgeräten anfallen. Diese Vielfalt stellt Ermittelnde vor die Herausforderung, Massendaten auf spezifische Fragestellungen hin zu untersuchen und konkrete Nachweise für ein mögliches Fehlverhalten herauszustellen – eine Aufgabe, die ohne maschinelle Unterstützung nicht mehr umfassend lösbar ist. Deshalb werden im Projekt VIKING Lösungen zur Textauswertung sowie die Sprecher-, Bild- und Objekterkennung beim Einsatz von Künstlicher Intelligenz erforscht.

Textauswertung durch Künstliche Intelligenz

Im Rahmen von VIKING beschäftigt sich das FI CODE mit Verfahren zur Filterung von und Informationsextraktion aus polizeilich relevanten Texten. Aus der Kombination der Verfahren können Texte zu vordefinierten Deliktgruppen zugeordnet werden, konkrete Informationen, wie z. B. Personen, Orte, Zeitpunkte und Objekte, herausgestellt und strukturierte Datenmodelle generiert werden. Somit können große Datenmengen gefiltert und mit weiteren Ermittlungsergebnissen sowie Datenbanken abgeglichen werden. Darüber hinaus sind Lagebilder möglich, die Ballungsräume spezifischer Delikte, Zeiträume oder Orte abbilden können. Der Anspruch an die verwendeten Modelle besteht in einer fairen Behandlung von z. B. ethnischen oder demographischen Eigenschaften. Darüber hinaus ist eine Nachvollziehbarkeit der Modelle und Modellergebnisse notwendig. Abschließend werden die Projektergebnisse in einen Demonstrator integriert.

Unterstützung statt Autonomie

Die in dem Projekt erarbeiteten Lösungen sollen keineswegs menschliche Entscheidungen ersetzen und auch nicht als Automatisierung des Justizsystems verstanden werden. Vielmehr unterstützen die Algorithmen dabei, die relevanten Daten in umfangreichen und heterogenen Quellen ausfindig zu machen. Hierfür werden Vorschläge zu erkanntem Fehlverhalten oder zu gesuchten Textinhalten, wie z. B. Personen, Orts- und Zeitangaben, sowie relevanten Objekten von der Software bereitgestellt. Die Strafverfolgungsbehörden müssen diese dann auf Basis der zugehörigen Erläuterungen prüfen und manuell in den weiteren Ermittlungsprozess einbringen, wobei keinerlei Entscheidungen durch die KI selbst getroffen werden, sondern sie lediglich unterstützende Funktion hat.

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

Gefördert durch: Bundesministerium für Bildung und Forschung (BMBF)

ABB.: FI CODE / F. MAORO

Sonderforschungsbereich 901 – OTF-Computing

Parametrisierte Servicespezifikation für maßgeschneiderte Apps

On-The-Fly (OTF) Computing erforscht die Möglichkeiten, den Menschen individuellere, auf ihre Bedürfnisse zugeschnittene Softwaredienste (Apps) zur Verfügung zu stellen. In diesem Teilprojekt werden verschiedene Arten von Anforderungsspezifikationen behandelt, die eine erfolgreiche Suche, Zusammenstellung und Analyse von Services ermöglichen.

Natürlichsprachliche Spezifikationen

Ziel ist es, Endanwenderinnen und -anwender in die Lage zu versetzen, sich an deren Spezifikationsprozess zu beteiligen, indem Anforderungen in natürlicher Sprache ohne Einschränkungen der Ausdrucksfähigkeit formuliert werden können. Ähnlich wie bei der Benutzung einer Suchmaschine sollen sie in der Lage sein, ihre Anforderungen in natürlicher Sprache und ohne spezielles technisches Hintergrundwissen zu formulieren. Aus diesem Grund ist die Verarbeitung und Interpretation natürlichsprachlicher Anfragen eine wesentliche Voraussetzung für die OTF-Vision. Da formale Spezifikationen nicht sehr intuitiv sind, ist natürliche Sprache in der Regel das einzige Format, das in Frage kommt. Entwicklerinnen und Entwickler müssen daher frei formulierte, natürlichsprachliche Anforderungsbeschreibungen akzeptieren. Dabei haben sie mit typischen Schwierigkeiten frei formulierter Texte zu kämpfen. Dazu gehören z. B. mangelnde Struktur und Korrektheit, Grammatik- und Rechtschreibfehler sowie Mehrdeutigkeit in Syntax und Semantik. Darüber hinaus fehlen Informationen, die für die Entwicklung wichtig sind, welche die Nutzerinnen und Nutzer aber nicht im Kopf haben. Nachfragen sind daher vorprogrammiert.

Anwenderzentrierte Dialogplanung und -gestaltung

Im Sinne agiler, partizipativer Softwareentwicklung werden Nutzerinnen und Nutzer künftig mehr in den interaktiven Kompositionsprozess von on-the-fly zu erstellenden Apps miteinbezogen. Dieser Dialog wird von einem Chatbot geführt, der einerseits der gezielten Nachfrage und andererseits der Auflösung von Unklarheiten dient. Hierfür erforscht das Teilprojekt iterative Klärungsprozesse zur Präzisierung und Vervollständigung bestehender Anforderungsbeschreibungen in natürlicher Sprache. Durch gezielte Rückfragen, passende Beispiele oder Vorschläge werden die Endanwenderinnen und -anwender bereits während des Spezifikationsprozesses individuell unterstützt.

Transparenz von Servicekonfigurationen

Darüber hinaus muss für das Endprodukt, die sogenannte Servicekonfiguration einer App, klargestellt werden, welche anfänglichen Anforderungen berücksichtigt wurden und auf welche verzichtet werden musste. Auf diese Weise wird nicht erst durch Ausprobieren herausgefunden, ob die initialen Erwartungen an die neu konfigurierte App erfüllt wurden, sondern frühzeitig ein Verständnis für die Umsetzbarkeit von Anforderungen bei den Nutzerinnen und Nutzern geschaffen. Hierfür wird ein Vorher-Nachher-Abgleich durchgeführt, um aufzuklären, inwiefern ursprünglich gemachte Anforderungen Berücksichtigung im resultierenden Service finden. Beispielsweise können dann mittels ChatGPT passende Antworten generiert werden.

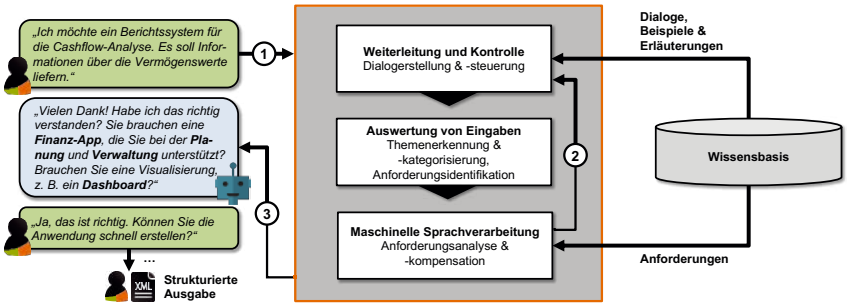


ABB.: FI CODE / M. GEIERHOS

Anforderungslücken mit einem Chatbot beheben.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

https://go.unibw.de/sfb901

Gefördert durch: DFG

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.

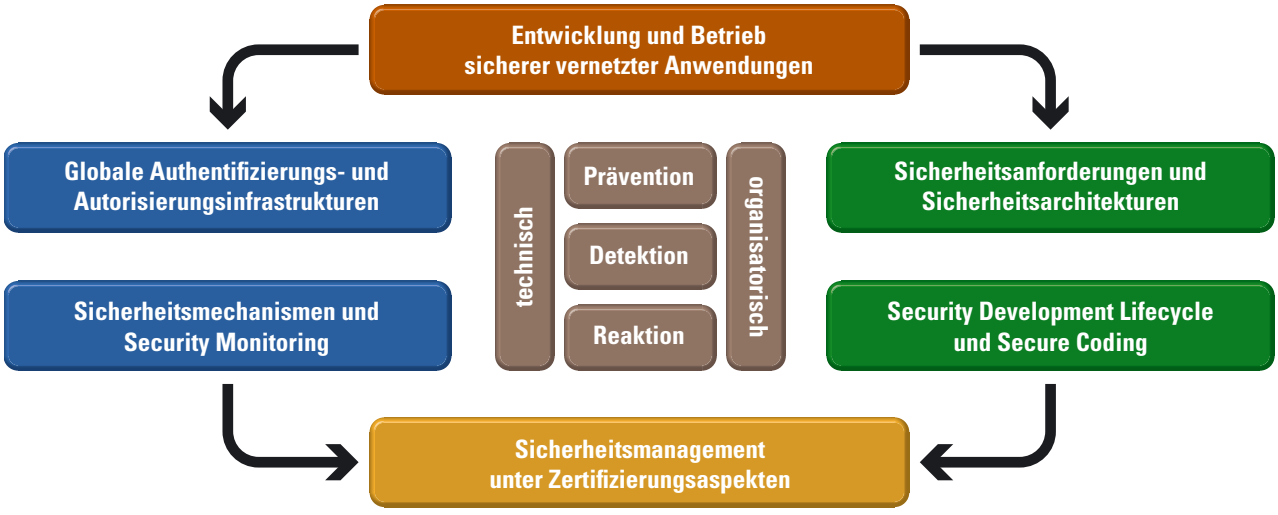
In laufenden Forschungsvorhaben und Projekten wurde 2022 beispielsweise an der Umsetzung des Self-Sovereign-Identity-Paradigmas für den Einsatz in organisationsübergreifenden Authentifizierungs- und Autorisierungsinfrastrukturen als datenschutzfreundliche technologische Weiterentwicklung des in der Praxis bewährten Federated Identity Management gearbeitet. Laufende Arbeiten an Security-Monitoring-Komponenten und richtliniengesteuerte Managementplattformen für föderierte softwarebasierte Netze finden beispielsweise beim Auf- und Ausbau der 5G-Telekommunikationsinfrastruktur und bei der dedizierten standortübergreifenden Vernetzung industrieller Steuerungssysteme Anwendung. Sie legen den Grundstein für die Absicherung künftiger 6G-Technologien und finden ihre Anwendung beispielsweise bei der Absicherung der Remote-Management-Infrastrukturen zukünftigter Energieversorgungsnetze. Im Bereich Internet of Things liegt der Forschungsschwerpunkt auf der softwareseitigen Absicherung von LoRa- bzw. LoRaWAN-basierten Infrastrukturen, die besonders störungsresilient sind und sowohl für industrielle als auch behördliche und militärische Anwendungen attraktive Eigenschaften aufweisen.

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: W. HOMMEL

Projekt DISPUT

Digitale Identitäten mit Self-Sovereign Identity Management: Prozesse und Technologien

IT-Sicherheit, Datenschutz und Nutzbarkeit sind insbesondere bei staatlichen digitalen/elektronischen Identitäten (eID) essentielle Aspekte. Das Projekt DISPUT begleitet zu diesen Themen das Bayerische Staatsministerium für Digitales (StMD) beim Aufbau und Betrieb der nationalen Identitätsföderation FINK und erforscht im selben Kontext selbstbestimmte Identitäten (SSI) als Zukunftstechnologie.

Mögliche zukünftige Nutzung von OZG-Verwaltungsleistungen über Self-Sovereign Identities.

DIGITALE IDENTITÄTEN begleiten uns alle privat, beruflich und zunehmend beim eGovernment, bei dem Verwaltungsdienstleistungen wie die Beantragung von Kindergeld online genutzt werden können. Klassisch muss man bei jedem Online-Dienstleanbieter einen eigenen Account einrichten. Um die Daten konsistent zu halten und die Verwendung von Diensten zu erleichtern, wurde föderiertes Identitätsmanagement (FIM) eingeführt. Alle Benutzenden haben dabei eine individuelle Heimatorganisation, die für die Verwaltung der Personendaten zuständig ist. Mit diesen Daten können Dienste innerhalb einer sogenannten Föderation genutzt werden.

SSI für den Datenschutz

Da bei FIM die Heimatorganisationen Daten (wann welcher Dienst genutzt wurde) sammeln und unerwünscht Profile erstellen könnten, entstand das Prinzip der selbstbestimmten Identitäten. Hier verwaltet jede Person ihre Identitätsdaten in einer Art digitalem Geldbeutel (Wallet) per Smartphone oder am PC. Die so gespeicherten digitalen Ausweise können flexibel verwendet werden. Auch wenn SSI häufig mit Blockchains in Verbindung gebracht wird, kann es u. a. mit einer Public Key Infrastructure (PKI) umgesetzt werden.

Identity Management

Im Kontext des Projekts DISPUT beschäftigt sich das Team der Professur „IT-Sicherheit von Software und Daten" mit der Frage, wie bestehende Systeme im eGovernment-Bereich betrieben werden sollen und welche Möglichkeiten es gibt, diese Systeme zukünftig mit SSI zu gestalten. Das StMD ist im Auftrag des IT-Planungsrats in der bund- und länderübergreifenden Zusammenarbeit federführend für die Umsetzung der deutschlandweiten Identitätsföderation FINK (Föderiertes Identitätsmanagement interoperabler Nutzerkonten) verantwortlich. FINK ermöglicht Bürgerinnen und Bürgern einen bundesweiten Zugang zu Online-Verwaltungsdienstleistungen im Rahmen des Online-Zugangsgesetzes (OZG) mit nur einem Nutzerkonto.

Umfassender Ansatz für FINK

Grundlage für FINK ist die Nutzung des FIM-Protokolls Security Assertion Markup Language (SAML), welches im Hochschulumfeld erprobt ist. Durch den technologischen Wandel werden vermehrt modernere Protokolle eingesetzt, die für die Anwendung in FINK u. a. in Form von Demonstratoren untersucht wurden. Zudem wurde bei den betrieblichen Prozessen im Sinne eines professionalisierten IT-Service Managements unterstützt. Zur Betrachtung der Nutzerperspektive auf SSI und möglicher Awareness-Designs wurde eine Nutzerstudie durchgeführt. Darüber hinaus nehmen die Aktivitäten rund um SSI international zu, wie u. a. an der Neufassung der eIDAS-Verordnung zu sehen ist. Hier liegt im Projekt der Fokus auf Kooperationen mit anderen Projekten, u. a. IDunion und der SSI and AARC BPA Expert Group, und auf der Integration in bestehende IT-Infrastrukturen.

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

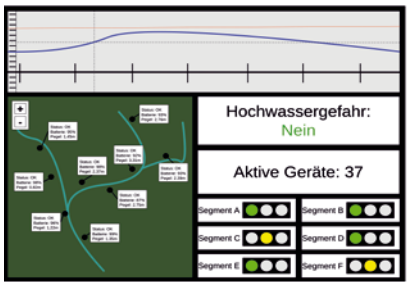
Gefördert durch:
Bayerisches Staatsministerium für Digitales (StMD)

ABB.: FI CODE / M. GRABATIN

Projekt ROLORAN

Resilienter Betrieb von LoRa-Netzen

Die Zielsetzung des Projekts ROLORAN ist die Untersuchung und Verbesserung der Robustheit des IoT-Protokolls LoRaWAN (Long Range Wide Area Network), welches auf der Modulationstechnik LoRa aufbaut. Neben Messreihen, Softwareanalysen und Härtungsmaßnahmen sind die praktischen Schwerpunkte die Prototypisierung im Rahmen von Meshes, Störsendern und Ortungsmechanismen sowie die Erprobung in verschiedenen Anwendungsszenarien.



Schematische Darstellung des Einsatzes LoRaWAN-basierter Wasserpegelsensoren.

SEIT EINIGEN JAHREN etabliert sich LoRaWAN im IoT-Bereich als besonders robustes Low-Power-WAN-Protokoll. Technische Grundlage hierfür ist die störresistente LoRa-Modulationstechnik zur Signalübertragung, welche sich der Chirp Spread Spectrum-Technologie bedient. Auf logischer Ebene ergänzen zusätzliche AES128-basierte Verfahren zur Integritätssicherung und Nutzdatenverschlüsselung die Robustheit des Protokolls. Dennoch können LoRa(WAN)-Geräte dank ausgeprägter Energieeffizienz im Batteriebetrieb eine Lebensdauer von über 10 Jahren erzielen und zudem je nach Bebauung Reichweiten von mehreren Kilometern problemlos überbrücken. Übertragene Datenmengen von 256 Byte pro Paket eignen sich vor allem für kompakte Datenrepräsentationen und Sensorwerte. Günstige Endgeräte versenden diese Datenpakete an (meist) stationäre Gateways, welche die empfangenen Informationen an eine nachgelagerte Serverinfrastruktur zur Auswertung weiterleiten.

Funkstandard für die Zukunft?

Da LoRaWAN inzwischen breite Verwendung in IoT-Anwendungen findet, untersucht das Projekt den aktuellen Zustand der existierenden LoRaWAN-Landschaft aus der IT-Sicherheitsperspektive. Dafür werden im Projekt statische und dynamische Analysewerkzeuge genutzt, um Referenzimplementierungen auf Schwächen zu prüfen und bei kritischen Fehlern gehärtete Open-Source-Software zur Verfügung zu stellen. Verschiedene Messreihen im Labor sowie im Außenbereich ergänzen hierbei eine Einschätzung durch die Bestimmung der physikalischen Grenzen und Verhaltensweisen einer LoRaWAN-Übertragung. Die Untersuchungen berücksichtigen zudem (un-)absichtliche Einflüsse durch Störsignale/-sender und stufen abschließend die Eignung für Senderortung ein. Insgesamt stellt eine gesamtheitliche Einschätzung der Fähigkeiten das Ziel der Analyse dar.

Anwendungspotenzial in Krisenszenarien

Neben der Analyse von LoRa(WAN) spielt die praktische Anwendung eine tragende Rolle im Projekt. Hierbei evaluiert das Projekt ausgewählte Szenarien. Auf LoRaWAN-Ebene betrifft dies vor allem großflächig angelegte Sensornetzwerke. Als eines der zu evaluierenden Szenarien dient eine Kooperation zwischen dem Projekt und dem Landkreis Bad Kissingen mit dem Ziel des Aufbaus und Betriebs einer Infrastruktur für die Realisierung einer Sturzflutfrühwarnung. Bei direkter Verwendung von LoRa ohne die LoRaWAN-Architektur sind Szenarien mit Punkt-zu-Punkt-Übertragungen interessant. Hierfür erprobt das Projekt eigene Prototypen mit Repeater-Funktionalität und deren Erweiterung auf selbstorganisierende Meshes, welche beispielsweise in Blackout-Szenarien nutzbare Alternativen zu den ausgefallenen Kommunikationskanälen darstellen.

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

Gefördert durch:

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

ABB.: FI CODE / M. SILACI

Prof. Dr. Johannes Kinder

PATCH: Programmanalyse, -transformation, -verstehen und -härtung

Die Forschungsgruppe PATCH beschäftigt sich seit ihrer Gründung 2019 durch Prof. Dr. Johannes Kinder mit der Absicherung von Software. Das Team entwickelt Systeme zur Programmanalyse, um Software automatisch verstehen und härten zu können. Besonderer Wert wird dabei auf den Transfer von theoretisch fundierten Konzepten in die Praxis gelegt.

DIE FORSCHUNG DER Gruppe PATCH beschäftigt sich mit automatischen Methoden zur Absicherung von IT-Systemen und Software. Das Ziel der Arbeit ist dabei der Entwurf von Werkzeugen für Entwickler und Organisationen, um fehlerhaften oder schädlichen Code zu finden und zu neutralisieren. Der Ansatz basiert dabei auf wissenschaftlich fundierten Methoden, insbesondere Abstraktion, Logik und maschinellem Lernen.

PATCH steht auf Englisch für „Program Analysis, Transformation, Comprehension, and Hardening", und entsprechend forscht das Team unter der Leitung von Prof. Dr. Kinder an der Analyse, der Transformation, dem Verstehen, und der Härtung von Software. Von Interesse ist dabei all die Software, die uns im Alltag umgibt, von Betriebssystemen und Gerätetreibern über Mobile Apps bis zu Anwendungen für Geräte im Internet of Things.

Programmanalyse und Fehlererkennung

Automatische Methoden, zum Beispiel statische Analyse oder Fuzzing, können heutzutage viele klassische Softwarefehler wie Überläufe in C-Programmen finden. Nach wie vor sind aber Softwarebugs eine Hauptursache für IT-Sicherheitsprobleme. In ihrer Forschung beschäftigt sich die Gruppe mit den Problemen, die in der Praxis durch komplexe Laufzeitumgebungen, Systeme und Hardware entstehen. So betrachtet das Team etwa JavaScript-Ökosysteme wie Node.js, neuartige Plattformen wie WebAssembly, aber auch Schwachstellen, die von spekulativer Ausführung in modernen Prozessoren verursacht werden.

Programmverstehen und Reverse Engineering

Um Software vor dem Einsatz auf ihre Eignung und Sicherheit zu überprüfen, entwickeln die Forscher automatische Verfahren, um Programmkomponenten zu kategorisieren und zu verstehen. Dies kann es einem Unternehmen ermöglichen, Hintertüren oder Malware in Software mit Hilfe automatisierter Tools oder durch manuelle Sicherheitsprüfungen zu entdecken. Das Team entwickelt hierfür sowohl klassische Ansätze mit formalen Methoden als auch Modelle mit neuronalen Netzen und statistischem maschinellen Lernen. Jede Vorgehensweise hat ihre eigenen Stärken: Statische Analyse kann sämtliches mögliches Programmverhalten abdecken, ist aber oft zu ungenau. Dynamische Analysen (oder Tests) sind konkurrenzlos im zuverlässigen Aufdecken von abweichendem Programmverhalten, sind jedoch auf das zur Laufzeit observierbare Verhalten beschränkt. Deep Learning schließlich ist in der Lage, menschliche Beschreibungen von Programmverhalten zu erfassen, wie sie in Funktionsnamen und Quellcodekommentaren enthalten sind, erfordert jedoch große Mengen an kommentierten Daten. Die Fähigkeiten und Grenzen jeder Methode zu verstehen ist eine Grundvoraussetzung, um die richtigen praxisrelevanten Lösungen zu finden.

Programmtransformation und -härtung

Neben der Erkennung von Schwachstellen ist es wichtig, die möglichen Auswirkungen eines Angriffs zu begrenzen. In komplexen Systemen können Fehler praktisch nie ausgeschlossen werden. Durch Einfügen von zusätzlichen Kontrollen im Programmcode kann aber verhindert werden, dass ein Angreifer Kontrolle über kritische Komponenten des Systems erlangt. Bei diesen Programmtransformationen gilt es, das Verhalten so wenig wie möglich zu beeinflussen oder zu verlangsamen.

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+49 89 6004 7335

www.unibw.de/patch

2022 startete der bayerische Forschungsverbund ForDaySec mit einem Kickoff-Event in Passau unter Beteiligung von Staatsminister Markus Blume. Von links nach rechts: Robert Obermaier, Felix Freiling, Harald Kosch, Sabine Toussaint, Thomas Riehm, Henrich Pöhls, Markus Blume, Johannes Kinder, Dominik Herrmann, Joachim Posegga, Stefan Katzenbeisser, Achim Dilling.

ABB.: ISTOCK / MONSITJ; UNIVERSITÄT PASSAU

Projekt ForDaySec

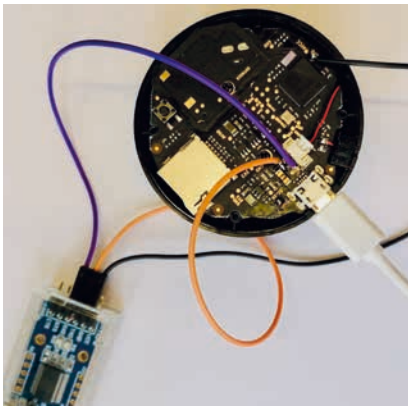
Sicherheit in der Alltagsdigitalisierung

Der bayerische Forschungsverbund ForDaySec verfolgt einen ganzheitlichen Ansatz, um die Sicherheitsprobleme der Digitalisierung im privaten und beruflichen Alltag anzugehen. Am FI CODE sollen insbesondere Verfahren zur Behebung von Schwachstellen in smarten Alltagsgeräten entwickelt werden, vom Netzwerkdrucker im Büro bis hin zum Staubsaugerroboter zu Hause.

DIE ZUNEHMENDE Vernetzung von alltäglichen Geräten ist eine zentrale Herausforderung für die IT-Sicherheit. Dies gilt für Staubsaugroboter oder digitale Heizungssteuerungen in Privathaushalten ebenso wie für Drucker, WLAN Router und Industriesteuerungen in mittelständischen Unternehmen, kommunalen Wasserversorgern oder Krankenhäusern. Es kommen Komponenten mit mangelhaften Sicherheitsfunktionen zum Einsatz, bisher eigenständige Systeme werden ohne Vorkehrungen vernetzt, und zum aktiven Management von Cybersicherheit fehlen an vielen Stellen Wissen und Personal.

Interdisziplinäre Forschung

Bestehende digitale Infrastrukturen können oft nicht grundlegend neu entworfen oder verändert werden – es müssen Sicherheitslösungen für bestehende Systeme und Komponenten gefunden werden. Sicherheits- und Datenschutztechniken sollen dabei einfach und ohne tiefes Fachwissen administrier- und implementierbar sein. Hier aber sind die Herausforderungen nicht nur technischer Art, sondern treffen auch auf organisationale, prozessuale und personelle Hürden. ForDaySec nimmt diese Probleme mit einer interdisziplinären Forschung in Angriff, die zusammen mit den Partnern Universität Passau, Technische Universität München, FAU Erlangen-Nürnberg und Universität Bamberg die Herausforderungen der Alltagspraxis und der Alltagspraktiken systematisch von Beginn an integriert.



Platine einer smarten Überwachungskamera. Schwachstellen in der Firmware von Smart-Home-Geräten können ein Einfallstor für Angreifer sein.

Firmware-Härtung

IoT-Geräte führen Software aus, die häufig auf Open-Source-Produkten in Verbindung mit Eigenentwicklungen der Hersteller besteht. Die IT-Sicherheit wird von Herstellern allerdings häufig wenig beachtet. Gerade bei Produkten aus dem Niedrigpreissegment werden selten bis nie Sicherheitsupdates zur Verfügung gestellt, ein Kundensupport findet nicht oder nicht langfristig statt. So bleiben bekannte Sicherheitslücken in den verwendeten Open-Source-Projekten dauerhaft offen und Angreifer können sie noch Jahre später erfolgreich ausnutzen.

Unser Ziel als Teil von ForDaySec ist es, Schwachstellen auf den Geräten selbst zu schließen und sie so zu härten. Bekannte Schwachstellen in Open-Source-Projekten sollen erhoben werden und mit Hilfe von Mustern direkt in der Gerätesoftware erkannt und anschließend beseitigt werden, auch dann, wenn ein Hersteller hierfür keinerlei Hilfestellung zur Verfügung stellt.

Der Fokus liegt auf den softwareseitigen Aspekten eines solchen Ansatzes zum Härten von Firmware. Passgenau sollen für die Schwachstellen semantische Patches erstellt und angewendet werden. Dabei muss die Integrität und Funktionalität der Firmware gewahrt bleiben. Abschließend soll die Funktionalität der gepatchten Firmware getestet werden, so dass sie erfolgreich aufgespielt und eingesetzt werden kann.

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

Gefördert durch:
Bayerisches Staatsministerium für Wissenschaft und Kunst (StMWK)

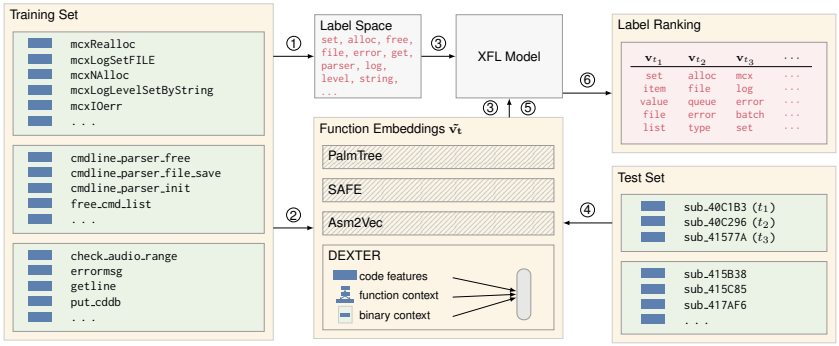
ABB.: FI CODE

Projekt XFL

Synthetisieren von Funktionsnamen mit Multi-Label-Lernen

Bezeichner von Funktionen sind im Reverse Engineering äußerst hilfreich, sind aber in sicherheitsrelevanten Anwendungen üblicherweise nicht verfügbar. XFL lernt den Zusammenhang zwischen Namen und Code anhand von tausenden Open-Source-Paketen und kann so plausible Namen für Funktionen in Binärdateien vorschlagen.

SOFTWARE Reverse Engineering hat zum Ziel, die Architektur und Implementierung eines bestehendes Softwaresystems zu verstehen. Im Kontext der Cybersicherheit wird es normalerweise ohne Zugriff auf Quellcode direkt auf Binärdateien durchgeführt. Diese enthalten normalerweise keine Funktions- oder Variablennamen mehr, welche aber überaus wertvolle Informationen wären. Daher enthalten gängige Reversing-Tools Unterstützung, um zumindest sehr häufig verwendete Standardkomponenten mit Namen zu kennzeichnen.



XFL lernt die Zuordnung von Bestandteilen eines Funktionsnamens zum Binärcode der jeweiligen Funktion. So können Namen für bislang unbekannte Funktionen erzeugt werden.

Funktionsnamen als Labels

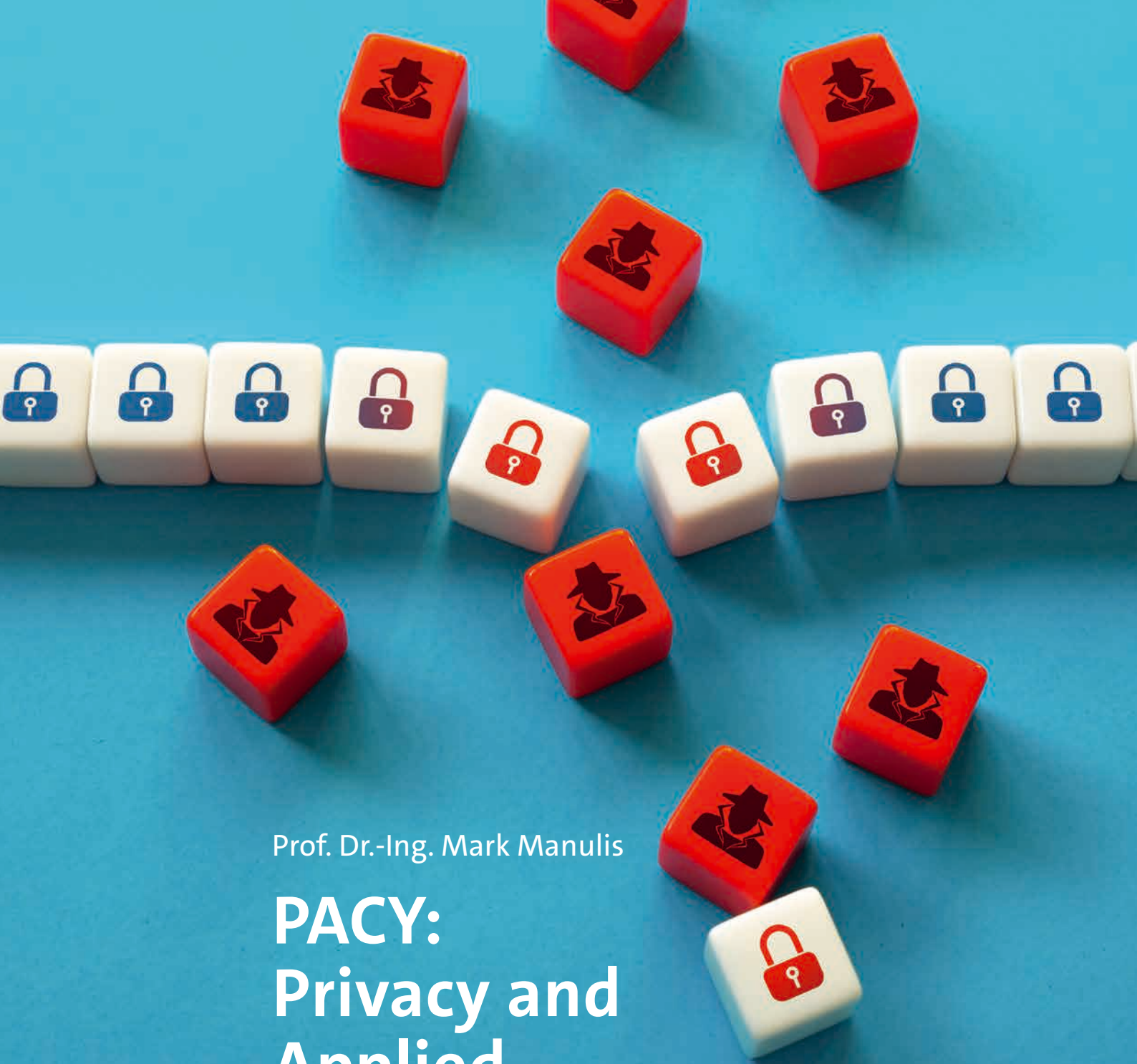
Maschinelles Lernen verspricht eine neue Generation noch leistungsfähigerer Werkzeuge zur Funktionsidentifikation. Vorhandene Ansätze stehen jedoch vor zwei grundlegenden Problemen: Erstens, sie können nur Funktionsnamen erzeugen, die bereits im Trainingsdatensatz enthalten waren. Jeder dieser Funktionsnamen stellt dann eine eigene Ausgabeklasse dar, wobei die Anzahl möglicher Funktionsnamen im Wesentlichen unbegrenzt ist. Unsere Lösung für dieses Problem besteht darin, Funktionsnamen in aussagekräftige Token aufzuteilen. Beispielsweise würde eine Funktion mit dem Namen make_smooth_colormap der Labelmenge {make, smooth, color, map} entsprechen. Die Gesamtzahl der Labels kann so gesteuert werden, dass jede Funktion mindestens ein beschreibendes Label hat, aber auch ausreichend viele Samples pro Label zur Verfügung stehen. Wir kommen daher zu dem Problem, jeder Funktion einen Satz von Labels zuzuweisen.

Extreme Multi-Label Learning

Ein ähnliches , zweites Problem ist das Markieren von Text mit einem Satz relevanter Labels, was Multi-Label-Lernen und Extreme Multi-Label Learning (XML) motiviert. Wir zeigen, wie sich modernste Algorithmen aus XML nutzen lassen, um Funktionen mit unserem eXtreme Function Labeling (XFL) Ansatz zu benennen. XFL wird durch ein bestimmtes Funktions-Embedding parametrisiert, das jede binäre Funktion auf eine Vektordarstellung abbildet. XFL ist mit aktuellen Embeddings wie PalmTree, SAFE und Asm2Vec kompatibel, die höchste Genauigkeit wird aber mit unserem eigenen, neuartigen Embedding DEXTER erreicht. DEXTER erfasst sowohl lokale Eigenschaften des Codes einer Funktion, als auch den Kontext innerhalb des Programms. In einer umfangreichen Evaluierung mit 741.724 Funktionen aus 10.047 Binärdateien von Open-Source-Projekten zeigen wir, dass unsere Implementierung den Stand der Technik deutlich übertrifft. Das manuelle Feature Engineering von DEXTER ist dabei Deep-Learning-Ansätzen überlegen, die nur die reine Syntax des Programmes verarbeiten. Wir beschreiben XFL ausführlich in einem Artikel, den wir auf dem 44. IEEE Symposium on Security and Privacy (S&P), einem führenden Forum für Forschung in der Cybersicherheit, vorstellen werden.

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

ABB.: FI CODE



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 der 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. Dazu gehören homomorphe Verschlüsselungsverfahren, attributbasierte Verschlüsselungsverfahren sowie Protokolle und Operationen (z. B. Suchanfragen) auf verschlüsselten Daten, und deren Einsatz in verteilten Anwendungen.

PEC für Benutzer: Authentisierung und Nachrichtenaustausch

Digitale Signaturen bilden das Rückgrat moderner PKI. Damit können Benutzer sich authentisieren bzw. Ende-zu-Ende sichere Verbindungen aufbauen. Die Verifikation von PKI basierten Signaturen gibt viele sensible Informationen preis, wie z. B. Identitäten, öffentliche Schlüsseln und sämtliche Attribute. PACY Lab forscht an erweiterten Signaturverfahren, um Authentisierung mit Anonymität bzw. Unverfolgbarkeit zu kombinieren. Aktuelle Forschung umfasst hierarchische attributbasierte Signaturverfahren zum Aufbau von Privatheit schützenden PKIs, Gruppensignaturen sowie verwandte Anonymous-Credentials-Verfahren. Zudem erforscht PACY Lab Sicherheitsprotokolle zum privaten Nachrichtenaustausch in dynamischen Gruppen, die neben Ende-zu-Ende Verschlüsselung auch Privatheit gewährleisten. Protokolle zur verteilten und delegierbaren Authentisierung, etwa in Zusammenhang mit dem neuen FIDO2 Standard, bilden ebenfalls Gegenstand der Forschung.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

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

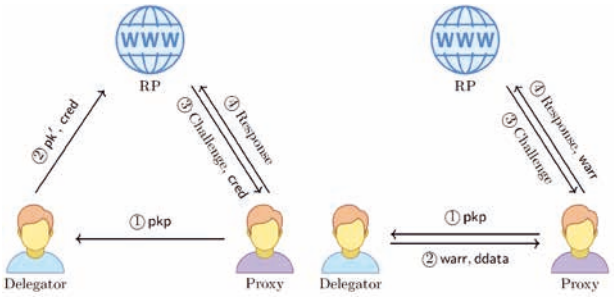
Delegation der Zugangsdaten in WebAuthn / FIDO2

Starke Authentisierung mit Delegationsmöglichkeiten für private Webkonten

Im neuesten Standard für Webauthentisierung werden Passwörter und Einmalcodes durch kryptographisch-sichere digitale Unterschriften ersetzt, die nur mit geeigneten privaten Schlüsseln erstellt werden können. Diese Schlüssel werden von hardwaregestützten Security Keys im Besitz der Benutzer verwaltet. Im Projekt geht es darum, neue Möglichkeiten für Benutzer zu schaffen, Zugangsrechte auf ihre Webkonten an andere Personen sicher zu delegieren.

WebAuthn und Backup von Security Keys

Der seit 2019 entwickelte WebAuthn-Standard (auch bekannt als FIDO2) soll die Nutzeridentifikation in Webdiensten sowohl sicherer als auch benutzerfreundlicher machen. Der Standard ist bereits weit verbreitet. Anders als weniger sichere Authentisierungsmethoden, wie etwa Passwörter oder Einmalcodes, setzt WebAuthn auf digitale Signaturen. Durch WebAuthn wird zudem die Privatheit der Nutzer verbessert – für jedes Webkonto wird ein unabhängiges Schlüsselpaar verwendet, somit können unterschiedliche Webkonten eines Nutzers nicht miteinander verlinkt werden. Die kryptographischen Schlüsselpaare des Nutzers für seine Webkonten werden durch Security Keys verwaltet. Ein Verlust würde den Nutzer aus seinen Konten aussperren. Im Jahr 2020 hat PACY Lab in Kooperation mit Yubico bereits eine standardkonforme Lösung zum Backup von Security Keys entwickelt. Teil dieser Lösung war ARKG, ein neues Protokoll zur asynchronen verteilten Erzeugung von kryptographischen Schlüsselpaaren bestehend aus einem private und einem öffentlichen Schlüssel.



Ansätze zur Delegation in WebAuthn.

Delegation von Zugriffsrechten mittels Security Keys

Im Jahr 2022 hat PACY Lab nun ein weiteres Problem erforscht, nämlich wie man den Zugriff auf eigene Webkonten mittels WebAuthn an andere Personen delegieren kann, ohne die Sicherheit und Privatheit einzubüßen. Das Problem besteht darin, dass die andere Person womöglich überhaupt kein eigenes Webkonto beim gleichen Webdienst besitzt. Und, anders als bei Passwörtern, die man im Notfall teilen könnte, können die kryptographischen Schlüssel aus Sicherheitsgründen weder exportiert noch geteilt werden. Es ist uns gelungen dieses Problem aufbauend auf ARKG elegant und Standards konform zu lösen.

Es wurden zwei Ansätze zur Delegierung von Zugriffsrechten in WebAuthn erarbeitet. Beim ersten Ansatz (im Bild links) konfiguriert der Besitzer bzw. die Besitzerin des Webkontos die Zugriffsrechte direkt beim Webdienst. Dabei werden bestimmte kryptographische Zugangsdaten – ein durch ARKG erzeugter öffentlicher Signaturschlüssel sowie Hilfsdaten – durch den Security Key der Besitzenden beim Webdienst hochgeladen. Beim Fernzugriff der berechtigten Person werden diese Zugangsdaten durch den Security Key der Person verarbeitet, um den passenden geheimen Signaturschlüssel zu berechnen und die Signatur für den Zugriff zu erstellen. Der zweite Ansatz (im Bild rechts) sieht vor, dass die Zugangsdaten direkt an den Security Key der anderen Person weitergeleitet werden, ohne dass der Besitzer oder die Besitzerin diese beim Webdienst hochladen muss. Dieser Ansatz basiert auf einer neuen Klasse von Proxy-Signaturen, die im Vergleich zu früheren Konstruktionen zusätzliche Privatheitseigenschaften bieten.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

ABB.: FI CODE / M. MANULIS

Privacy in Signaturverfahren und PKI

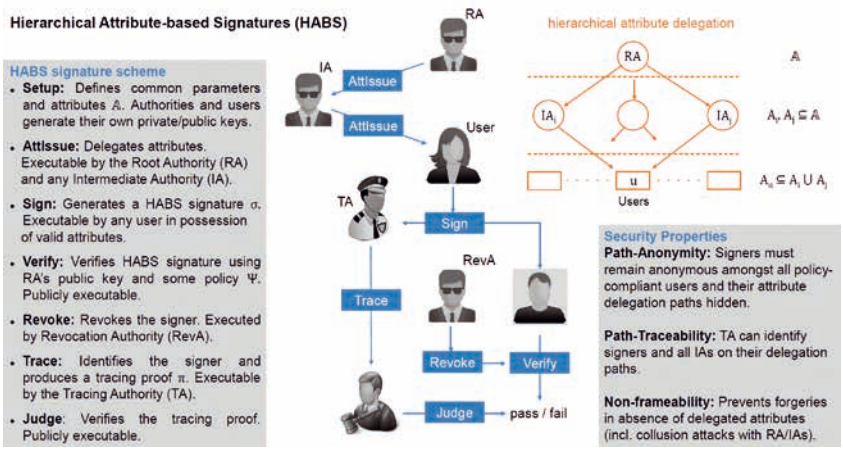
Anonyme digitale Unterschriften und ihre Verifizierbarkeit

Digitale Zertifikate, die in modernen Public Key Infrastrukturen eingesetzt werden, sind kryptographisch mit Nutzeridentitäten verknüpft. Diese können bei der Verifizierung von Zertifikaten nicht verschleiert werden. Für einen besseren Schutz der Privatheit werden in diesem Projekt neue Signaturverfahren entwickelt, mit denen ausgestellte Unterschriften in Bezug auf die Eigenschaften und Rechte anonymer Unterzeichner verifiziert werden können.

Probleme mit Privacy

Digitale Signaturen und Zertifikate (nach X.509-Standard) bilden das Rückgrat moderner Public Key Infrastrukturen (PKI) und werden vielfältig eingesetzt. Sie bieten Authentisierung und somit Schutz gegen Impersonifizierungs- und man-in-the-middle Angriffe in zahlreichen IT-Sicherheitsprotokollen und -anwendungen, darunter Schutz der E-Mail-Nachrichten, Dokumenten sowie in Identifikations- und Zugangskontrollverfahren. X.509 Zertifikate erhalten Informationen über deren Halter, wie z. B. öffentliche Schlüssel, Identitäten sowie weitere Eigenschaften, die bei der Verifizierung der Signatur alle mitausgelesen und überprüft werden können.

In Anwendungen, die lediglich auf die Überprüfung bestimmter Rechte und Eigenschaften der Zertifikathaltenden ausgerichtet sind, etwa in rollen- bzw. policy-basierten Authentisierungs- und Zugangskontrollverfahren, bieten X.509 Zertifikate und moderne PKI keinen ausreichenden Schutz der Privatheit. Attributbasierte Signaturverfahren (ABS) wurden gerade für solche Szenarien entwickelt. Sie bieten verbesserten Schutz der Privatheit für Zertifikathaltende, indem sie alle Eigenschaften (Attribute) während der Verifizierung geheim halten und lediglich bekanntgeben, ob die gestellten Überprüfungskriterien erfüllt sind. Weil diese Kriterien potenziell von einer Vielzahl von unterschiedlichen Individuen mit passenden Attributen erfüllt werden kann, wird die Privatheit jedes Individuums, wie z. B. die Geheimhaltung eigener Identität, deutlich verbessert. ABS-Verfahren bieten dennoch die Möglichkeit einer kontrollierbaren Aufhebung der Anonymität des Individuums, um potenzielle Missbräuche aufzudecken.



Hierarchische attributbasierte Signaturverfahren.

Hierarchische ABS-Verfahren

PACY Lab forscht an ABS-Verfahren zur Realisierung von Privatsphäre-schützenden PKI. Dafür ist es nötig die Funktionalität bestehender ABS-Verfahren hinsichtlich hierarchischer Verwaltung von ABS-Zertifikaten auszubauen, um diese näher an die hierarchische Struktur und Funktionalität klassischer PKI zu bringen. Schon 2018 wurden die ersten hierarchischen ABS-Verfahren von Mitgliedern des PACY Lab vorgestellt und seitdem ständig weiterentwickelt. Im Jahr 2022 wurde die erste Realisierung von hierarchischen ABS mittels gitterbasierter kryptographischer Methoden präsentiert, von denen angenommen wird, dass sie gewünschte Sicherheit gegenüber den künftigen Quantenrechnern gewährleisten. Zudem erlaubt das Verfahren die Signaturrechte sowie Attribute von Parteien zurückzuziehen.

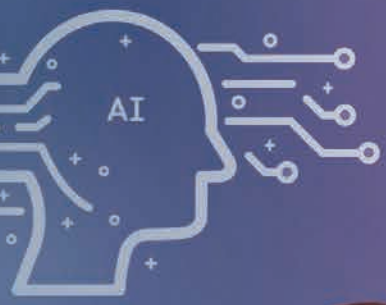
Prof. Dr.-Ing. Mark Manulis
+49 89 6004 7365
mark.manulis@unibw.de
www.unibw.de/pacy

ABB.: FI CODE / M. MANULIS

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

Die Gruppe für Künstliche Intelligenz und Maschinelles Lernen (AIML) wurde im August 2022 von Prof. Dr. Eirini Ntoutsi gegründet. Ihr Ziel ist es, Methoden der Künstlichen Intelligenz und des Maschinellen Lernens zu entwickeln, die reale Herausforderungen adressieren und das gesellschaftliche Wohl fördern.



DIE GRUPPE FÜR Künstliche Intelligenz und Maschinelles Lernen (AIML) entwickelt neue KI/ML-Methoden, die reale Herausforderungen wie Nicht-Stationarität und Datenknappheit angehen und gleichzeitig vertrauenswürdige Entscheidungsfindung fördern. Kontinuierliches Lernen über sich entwickelnde Daten, vertrauenswürdige KI (einschließlich fairnessbewusster und erklärbarer KI) sowie generative KI für neue Daten und Lösungen sind laufende Forschungsrichtungen.

Kontinuierliches Lernen

Dynamische Umgebungen mit kontinuierlich eintreffenden und sich ändernden Daten wie Kommunikations- und Stromnetzen bieten viele Anwendungen. Wir entwickeln intelligente Algorithmen, die Ressourcenbeschränkungen wie Speicher und Reaktionszeit berücksichtigen, und erforschen, wie man ML-Modelle aktualisiert, Fehler vermeidet, sich an veränderte Merkmalsräume anpasst und Änderungen überwacht und erklärt.

Vertrauenswürdige KI

Heutzutage werden AI-basierte Systeme weit verbreitet eingesetzt, um Entscheidungen zu treffen, die weitreichende Auswirkungen haben und Bedenken hinsichtlich potenzieller Menschenrechtsfragen aufwerfen. Um sicherzustellen, dass diese Systeme der Gesellschaft zugute kommen, ist es unerlässlich, über traditionelle Algorithmen hinauszugehen, die auf Vorhersageleistung optimiert sind, und ethische und rechtliche Grundsätze in ihr Design, ihre Schulung und ihre Implementierung zu integrieren. Ein Bereich des Fokus ist das fairnessbewusste Lernen, das die Schaffung von ML-Modellen umfasst, die nicht auf geschützten Merkmalen wie Geschlecht, Ethnizität oder Alter diskriminieren. Ein weiterer Bereich von Interesse ist die erklärbare KI (XAI), die Endbenutzern hilft, AI-Entscheidungen zu verstehen und Designern hilft, robustere Modelle zu erstellen.

Generative KI

KI ist nicht mehr auf die Analyse historischer Daten beschränkt. Sie kann nun auch neue Inhalte generieren, darunter Texte, Bilder und tabellarische Daten. Generative KI kann der Gesellschaft zugute kommen, indem sie Ingenieuren hilft, bessere Produkte zu entwerfen, neue Produkte zu schaffen und sogar Bücher zu schreiben. Wie bei jeder Technologie gibt es jedoch Nachteile, einschließlich Sicherheitsprobleme, voreingenommenem Inhalt, Urheberrechtsproblemen und Kreativitätsbeschränkungen. Ein Bereich von Interesse ist die Verwendung von generativer KI zur Bewältigung von Datenherausforderungen wie Datenknappheit und fehlender repräsentativer Daten. Ein weiterer Bereich von Interesse ist die Generierung von realen Strukturen, wie Windturbinen, durch die Kombination von Simulationsmodellen, analytischen Modellen und datengesteuerten Modellen.

Entwicklung der Forschungsgruppe

Die Gruppe wird im Jahr 2023 mit neuen Promotionsstudierenden und Postdocs erweitert, die in München beitreten werden, während einige Mitglieder in Berlin (an der Freien Universität) und Hannover (an der Leibniz Universität/L3S Research Centers), wo Prof. Ntoutsi zuvor tätig war, verbleiben werden. Im Jahr 2022 wuchs das Drittmittelförderportfolio der Gruppe um zwei neue EU-Projekte: MAMMOth, das sich auf Fairness-aware Machine Learning für komplexe Daten konzentriert, und STELAR, das sich auf KI-Methoden für intelligente Landwirtschaft konzentriert.

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

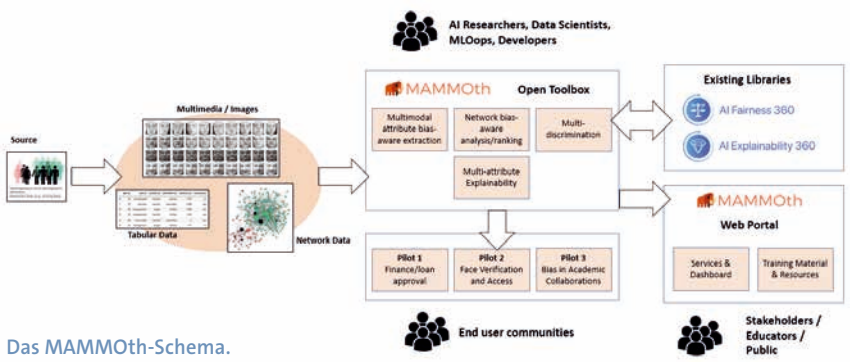
https://go.unibw.de/aiml

ABB.: ADOBESTOCK / PARRADEE, PINKEYES

Projekt MAMMOth

Entschärfung von Multi-Diskriminierung in KI-Systemen

MAMMOth entwickelt Tools und Techniken zur Entdeckung und Entschärfung von („Multi-) Diskriminierung“, um die Verantwortlichkeit von KI-Systemen für mehrere geschützte Attribute und für traditionelle tabellarische Daten und komplexere Netzwerk- und visuelle Daten zu erreichen.



Das MAMMOth-Schema.

KI-Diskriminierung

Die KI-basierte Entscheidung bietet große Chancen für die Automatisierung in verschiedenen Sektoren und im täglichen Leben, birgt aber gleichzeitig die Gefahr der Diskriminierung von Minoritäten und marginalisierten Bevölkerungsgruppen auf der Grundlage sogenannter geschützter Attribute, wie Geschlecht, Ethnie und Alter. Fairness-aware Machine Learning entwickelt Methoden zur Erkennung und Abschwächung von Vorurteilen, jedoch funktionieren die vorgeschlagenen Methoden nur in begrenzten Umgebungen und unter sehr eingeschränkten Annahmen und spiegeln nicht die Komplexität und Anforderungen realer Anwendungen wider. Zu diesem Zweck konzentriert sich MAMMOth auf die Erkennung und Abschwächung von Mehrfachdiskriminierung für tabellarische, Netzwerk- und multimodale Daten. Die entwickelten Lösungen werden in folgenden Bereichen demonstriert: a) Finanz-/ Kreditanwendungen, b) Identitätsverifikationssysteme und c) akademische Evaluierung.

Die Hauptziele

- Fairness-Definitionen und Methoden zur Abschwächung von Bias, die über die einfache Definition eines einzigen geschützten Attributs auf viele geschützte Attribute hinausgehen.
- Erkennung von Bias in Netzwerkdaten, z. B. als Ergebnis der Ungleichheiten, die sich aus der unterschiedlichen Position von Individuen im Kontext eines zugrunde liegenden Netzwerks von Verbindungen oder Interaktionen ergeben.
- Erkennung von Bias in multimodalen Daten, mit Schwerpunkt auf visuellen Medien, wo verschiedene Formen von Bias, die oft schwer zu bewerten sind, auftauchen und die Leistung kritischer KI-Systeme (z. B. Gesichtsverifizierung) beeinträchtigen oder der Grund für die Aufrechterhaltung und Verbreitung schädlicher Verhaltensweisen im Internet sein könnten (z. B. durch Bilder, die in stereotyper und schädlicher Weise auf bestimmte marginalisierte Gemeinschaften abzielen).
- Erklärungsmethoden, die den oben genannten Komplexitäten von KI-Systemen berücksichtigen.

Ein multidisziplinäres Team von Informatikern und KI-Experten wird zusammen mit Sozialwissenschaftlern und Ethikexperten sowie verschiedenen Gemeinschaften von schwachen und/oder unterrepräsentierten Gruppen in der KI-Forschung zusammenarbeiten, um sicherzustellen, dass die tatsächlichen Bedürfnisse der Nutzer im Mittelpunkt der Forschungsagenda stehen.

MAMMOth
Multi-attribute, Multimodal Bias Mitigation in AI Systems

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

Gefördert durch: EU H2020

ABB.: MAMMOTH PROPOSAL (2)

Sonderforschungsbereich 1463

Design von Offshore-Windturbinen der Zukunft mit AI

Der Sonderforschungsbereich (SFB) erforscht die Entwurfs- und Betriebsbedingungen von Offshore-Megastrukturen der Zukunft, wobei der gesamte Life-Cycle eines Bauwerkes von der Planung und Herstellung über den Betrieb bis zum Abbau und Recycling dargestellt werden kann.

Offshore-Windturbinen der Zukunft

Moderne Offshore-Windturbinen (OWTs) sollen einen wesentlichen Beitrag zum Erfolg der Energiewende leisten. Zukünftige Anlagen werden deutlich größer sein als die heutigen: über 300 Meter Gesamthöhe und mit Rotoren von mehr als 280 Metern Durchmesser. Das bedeutet, dass sie kaum den bekannten Einflüssen und Bedingungen ausgesetzt sein werden, die in Höhen von über hundert Metern auftreten können. Aufgrund ihrer Dimensionen und der dafür erforderlichen filigraneren Bauweise gewinnen Umwelteinflüsse sowie Wechselwirkungen zwischen einzelnen Komponenten an Relevanz. Die heute etablierten Methoden für die Auslegung und den Betrieb von Windenergieanlagen sind auf Bauwerke dieser Größe nicht mehr anwendbar. Deshalb werden im SFB 1463 neue Konzepte für Offshore-Megastrukturen entwickelt.

Teilprojekt B1: Integrierter Entwurfsprozess für Offshore-Strukturen

Unsere Gruppe ist Teil des Teilprojekts B1, das darauf abzielt, die Konstruktion von OWT-Tragstrukturen zu verbessern, einem der Hauptkostentreiber für OWTs, die traditionell von Ingenieuren hauptsächlich auf der Grundlage ihres Betriebsverhaltens entworfen werden.

Offshore-Windturbinen

Die Hauptziele

- Entwicklung einer integrierten Entwurfsmethodik, die den gesamten Life-Cycle von OWTs berücksichtigt.
- Entwicklung von ML-Modellen, die die Qualität eines Entwurfs unter Berücksichtigung des gesamten Life-Cycle sowie der Erfahrung und Intuition der Ingenieure vorherberechnen können.
- Bereitstellung von umsetzbarem Feedback für die Ingenieure durch erklärbare KI (XAI), z. B. in Form von Merkmalszuweisungen oder kontrafaktischen Erklärungen.
- Generierung neuer Offshore-Strukturentwürfe.

Wichtigste Herausforderungen und Methodik

- Datenknappheit, da es nur wenige Instanzen von realen OWTs gibt und diese nicht die verschiedenen Phasen des Life-Cycles abdecken. Zu diesem Zweck kombinieren wir traditionelle evolutionäre Methoden mit generativen KI-Methoden.
- Beschriftungserfassung für bestehende reale und synthetische Designs. Zu diesem Zweck wird das Feedback von Experten gesammelt, wobei die Variation der menschlichen Labels und die Knappheit der Labels berücksichtigt werden.
- Bewertung neuer Designs unter Berücksichtigung des gesamten Life-Cycle. Zu diesem Zweck wird ein multikriterieller Optimierungsansatz verfolgt, der zu einer Reihe von Pareto-optimalen Lösungen führt.
- XAI-Methoden, um den Ingenieuren verwertbare Erkenntnisse zu liefern und die Trade-offs zwischen den verschiedenen Lösungen zu verstehen.
- Kreativität der neu generierten Designs: Kann KI neuartige, unerwartete und dennoch nützliche Entwürfe erstellen?

SFB Offshore–Megastrukturen

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

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

Gefördert durch: DFG

ABB.: SFB1463; UNSPLASH / N. DOHERTY

Prof. Dr. Arno Wacker

Datenschutz und Compliance

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

EINES UNSERER WICHTIGSTEN Ziele ist es, den Datenschutz und die IT-Sicherheit nicht nur zu erforschen und zu lehren, sondern auch im Alltag zu leben. Nur so lassen sich diese Themenkomplexe den Studierenden überzeugend und authentisch vermitteln. Darüber hinaus möchten wir auch der breiten Öffentlichkeit demonstrieren, dass datenschutzfördernde Technologien in den Alltag integrierbar sind, im privaten wie 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 Studenten unter anderem, was Privacy ist und warum sie sowohl für Einzelne als auch für demokratische Gesellschaften von Bedeutung ist. Pentesting behandelt das Überprüfen einzelner Systeme, komplexerer IT-Dienste und ganzer IT-Infrastrukturen sowie praxisrelevante Angriffsvarianten mit Orientierung an bewährten Good-Practice-Dokumentationen. Kryptologie vermittelt die Grundlagen der Kryptographie sowie das Wissen über die verschiedenen Methoden zur sicheren Datenübertragung in modernen Kommunikationsnetzen.

Forschung

Ein besonderer Fokus der Professur liegt auf Privatheit sowie den Datenschutz unterstützenden Methoden und Mechanismen und gliedert sich in drei unterschiedliche Forschungsschwerpunkte:

- Privatheit unterstützende Mechanismen haben als Ziel, die Privatheit des Einzelnen zu stärken, sowie 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 z. B. Verfahren und Werkzeuge zur Steigerung des Sicherheitsbewusstseins bei der Entwicklung von Softwarewerkzeugen bzw. im Umgang mit diesen.

ABB.: ISTOCK / MATEJMO, M. BUHLINGER

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

Wissenstransfer

Ein besonderes Anliegen unserer Professur ist es, interessierte Bürger fortzubilden, aufzuklären und in Fragen der IT-Sicherheit zu schulen und zu informieren. Diese Aufgabe verfolgen wir mit Hilfe von Vorträgen und Workshops, welche sich z. B. mit Pentesting, sicherem E-Mail-Verkehr im Alltag und Aufspüren von Sicherheitslücken befassen.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

CrypTool

CrypTool ab 2023 bei Datenschutz und Compliance

Ziel des CrypTool-Projektes ist die Entwicklung der E-Learning Applikation CrypTool für die Bereiche Kryptographie und Kryptoanalyse. Mit Hilfe von CrypTool lassen sich viele kryptographische Verfahren anwenden und analysieren, um dem Anwender grundlegende und fortgeschrittene Konzepte der Kryptologie praktisch zu verdeutlichen.

Kryptographie spielt auch im Alltag eine immer größere Rolle.

DAS PROJEKT umfasst unter anderem mit CrypTool2 und JCrypTool mehrere aktiv entwickelte Programme für den PC, sowie das Internetangebot CrypTool-Online. Insgesamt bietet CrypTool einen spannenden Einblick in die Welt der Kryptologie. Eine Vielzahl von Chiffrierverfahren sowie Kodierungen und Analysetools werden auf einfache Weise und durch Beispiele ergänzt vorgestellt. Der Schwerpunkt liegt dabei auf einer verständlichen Erläuterung, die Interesse an der Kryptografie und der Kryptoanalyse wecken soll. Mit vielen der vorgestellten Verfahren kann direkt in der Applikation oder auf der Website selbst probiert und experimentiert werden.

Interessierte können in kurzer Zeit die Funktionsweise von historisch bedeutsamen Kryptografieverfahren erlernen und mit den angebotenen Tools selber Texte verschlüsseln. Sie können sich beispielsweise die moderne Chiffre AES ansehen oder sich gute Passworte generieren lassen. Möchte man etwas tiefer einsteigen, bietet CrypTool auch Möglichkeiten zur Entschlüsselung und Analyse von Geheimtexten an, um z. B. Schwachstellen einer Chiffre ausfindig zu machen.

Historie

Die Entwicklung von CrypTool begann 1998 im Rahmen einer IT-Sicherheitsinitiative zur betrieblichen Ausbildung bei der Deutschen Bank. Ab 2000 wurde CrypTool als Freeware zur Verfügung gestellt und beispielsweise 2002 auf der Bürger-CD des Bundesamts für Sicherheit in der Informationstechnik (BSI) „Sicher ins Internet“ verteilt. Nach drei Jahren als Freeware wurde CrypTool schließlich im Jahr 2003 zu einem Open-Source-Projekt. Während Firmen und Universitäten CrypTool bereits als Freeware einsetzten, wurde erst durch die Veröffentlichung des Quelltextes die direkte Mitwirkung von freiwilligen Entwicklern möglich. Der Open-Source-Ansatz verbesserte insbesondere die Zusammenarbeit mit Universitäten, so dass im Rahmen von Seminar- oder Abschlussarbeiten zahlreiche Erweiterungen für CrypTool entwickelt wurden und werden.

Die Professur Datenschutz und Compliance an der Universität der Bundeswehr, geleitet von von Prof. Dr. Arno Wacker, unterstützt das CrypTool-Projekt seit vielen Jahren und stellt unter anderem die für die Webseite nötige Infrastruktur zur Verfügung.

Ab 2023 wird die Leitung des Projektes von Prof. Esslinger (Universität Siegen) an Prof. Wacker (Universität der Bundeswehr München) übergeben.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

CrypTool im Netz:
https://www.cryptool.org

ABB.: ISTOCK / NICOELNINO

Trusted Platform Module (TPM)

TPM-Kommunikation unter Windows 11 und Linux

TPMs können Daten vor fremdem Zugriff schützen, ohne dass der Benutzer sich intensiv mit den dahinterliegenden Sicherheitsmechanismen auseinandersetzen muss. Voraussetzung dafür ist jedoch eine vollständige Unterstützung dieser Mechanismen durch das Betriebssystem.

ZUM SCHUTZ SENSIBLER DATEN werden diese auf Datenträgern oft verschlüsselt gespeichert. Um Zugriff zu erhalten, ist dann eine Entschlüsselung erforderlich. Typischerweise ist das durch die Eingabe des entsprechenden Schlüssels (Passwortes) über die Tastatur möglich. Ein Trusted Platform Module (TPM) in Form eines separaten Bausteins auf der Hauptplatine kann den Schlüssel sicher speichern, und ihn dem Hauptprozessor für die Entschlüsselung über einen Datenbus mitteilen. Unter Windows kann die Software BitLocker das TPM nutzen, um die Daten auf die angegebene Art und Weise zu schützen. Mit TPM 2.0 besteht die Möglichkeit, den Schlüssel nur noch verschlüsselt zu übertragen und die Abfrage des Schlüssel vorab mit einer PIN zu bestätigen.

Im letzten Jahr entdeckte die DOLOS Group, dass unter Windows 10 das TPM den Schlüssel im Klartext überträgt [1]. Dies war nicht überraschend, da bis zur TPM-Version 1.2 die Spezifikation keine verschlüsselte Kommunikation über den Datenbus zuließ. Mit der Version 2.0 der TPM-Spezifikation wurde die Unterstützung für verschlüsselte Kommunikation über den Bus hinzugefügt.

Da Microsoft mit Windows 11 das Vorhandensein eines TPM in der Version 2.0 voraussetzt, war anzunehmen, dass dieser Angriffsvektor durch die Verschlüsselung eingeschränkt würde. Dies ist jedoch nicht der Fall. Auch mit Windows 11 wird der Schlüssel nach wie vor im Klartext übertragen. Microsoft ist sich dessen bewusst und empfiehlt die Verwendung einer zusätzlichen PIN [2], die vom Anwender eingegeben wird. Doch auch damit bleibt die Parameterverschlüsselung ungenutzt. Der Schlüssel wird nach wie vor im Klartext über den Datenbus übertragen.

Des Weiteren wird die TPM-basierte Verschlüsselung mit dem Linux Unified Key Setup (LUKS), wie sie von systemd genutzt wird, analysiert. Bis zur Version v250 von systemd wird weder die Verwendung einer PIN noch die Parameterverschlüsselung unterstützt. Unter der Version v251 sind beide Möglichkeiten implementiert und die Parameterverschlüsselung ist verpflichtend, wodurch der Angriffsvektor stark eingeschränkt wird.

Quellen

[1] https://dolosgroup.io/blog/2021/7/9/from-stolen-laptop-to-inside-the-company-network

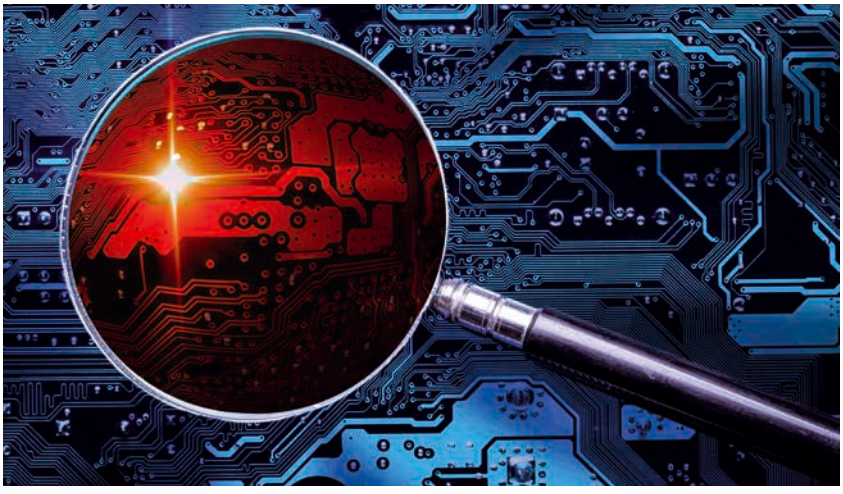
[2] https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures\#attacker-with-skill-and-lengthy-physical-access

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom



TPMs schützen vor neugierigen Blicken.

ABB.: ISTOCK / ELEN11

Hon.-Prof. Dr. Udo Helmbrecht

Quanten-kommunikation

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

Einblicke in das MuQuaNet Labor

Quantensichere Kommunikation in der Praxis

Das MuQuaNet baut im Großraum München ein Quantennetzwerk auf. Hierfür wurden im Juni 2022 die jüngsten QKD-Geräte geliefert, welche ab dem nächsten Jahr zwei Gebäude auf dem Campus der UniBw M verbinden werden. Zuvor wurden die QKD-Geräte ausführlich im Labor getestet. Dabei konnte im Rahmen der Untersuchung militärischer Anwendungsfälle von QKD die quantensichere Fernsteuerung eines Roboters demonstriert werden.

EIN QUANTENSCHLÜSSELAUSTAUSCH (kurz: QKD) erlaubt es abhörsicher symmetrische Schlüssel, sog. Quantenschlüssel, auszutauschen. Während die Funktionsweise von QKD oft erklärt wird, bleibt die Praxis, wie ein QKD-Gerät von innen aussieht, oder wie ein Versuchsaufbau zur quantensicheren Verschlüsselung gestaltet ist, meist im Verborgenen. Deshalb zeigt dieser Beitrag Einblicke in das MuQuaNet Labor.

Quantenschlüssel im Einsatz

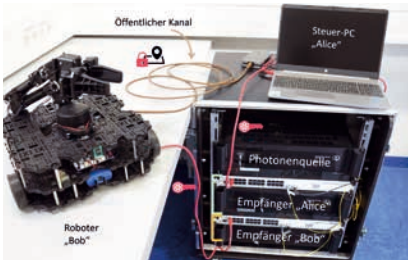
In diesem Jahr wurde die quantensichere Fernsteuerung eines Roboters mit Hilfe von verschränkungsbasiertem QKD demonstriert.

Hierfür wurde ein Kontroll-PC (genannt „Alice“) und der Roboter (genannt „Bob“) jeweils mit einem Empfänger für Photonen verbunden. Eine Photonenquelle, die sich auf der Strecke zwischen Alice und Bob befindet, verteilt verschränkte Qubits an die beiden Empfänger.

Die Empfänger analysieren die Photonen und erzeugen basierend auf einem QKD-Protokoll einen sicheren Schlüssel. Damit Alice und Bob den Schlüssel allerdings für die verschlüsselte Kommunikation benutzen können, müssen sie diesen bei ihren Empfängern abfragen. Die Übertragung der Schlüssel erfolgt momentan kabelgebunden, da QKD-Geräte noch nicht in Endgeräte integriert werden können.

Kompakte Senderelektronik in einem 3D-gedruckten Gehäuse.

Deshalb wird im Projekt MuQuaNet in Kooperation mit der LMU an der Miniaturisierung von QKD-Geräten geforscht.



Eine Photonenquelle verteilt über Glasfaserkabel verschränkte Photonen an die beiden Empfänger. Diese analysieren die Lichtteilchen und erzeugen daraus einen Schlüssel. Der Steuer-PC und der Roboter können über die roten Ethernet-Kabel von ihrem lokalen Empfänger einen Quantenschlüssel abfragen. Mit diesen kann der Roboter über einen öffentlichen Kanal quantensicher gesteuert werden.

Entwicklung miniaturisierter QKD-Geräte

Damit QKD als Technologie weiter verbreitet wird, müssen die eingesetzten Geräte handlicher werden. Die im Rahmen des Projekts entwickelten QKD Geräte sollen eine Freistrahlstecke zwischen dem Kooperationspartner Airbus und der UniBw M Fakultät ETTI realisieren. Das gezeigte Sendermodul ist im Stande die erforderlichen Quantenzustände für ein polarisationsbasiertes Decoy-State BB84 Protokoll zu präparieren. Das Modul kann mittels USB-C an einen PC angeschlossen werden und wird dadurch auch mit Strom versorgt. Das Sendermodul ist ca. 11 x 11 cm^2 groß und wiegt inklusive Mikrooptik in silberfarbigen Kovar Gehäuse ca. 200 g. Diese hohe Integration ermöglicht es den Sender vielseitig einzusetzen.

Hon.-Prof. Dr. Udo Helmbrecht
udo.helmbrecht@unibw.de
+49 89 6004 7308
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 / M. AUER, S. KASTRUP

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.

Umfeldstudie Quantum Computing

Das mediale und wirtschaftliche Interesse an der neuen Technologie des Quanten Computings wächst beständig. Dabei steht die angewandte Forschung hier noch relativ am Anfang und in vielen Bereichen ist nicht klar, wie und ab wann entsprechende Techniken und algorithmische Optimierungsverfahren eingesetzt werden können. Die Bundesbank hat mit Accenture und wissenschaftlicher Unterstützung einen ersten Schritt gewagt.

Quantum Computing – Machine Learning: Forschung & Anwendung

Bereits die rasche Entwicklung des Machine Learning hat gezeigt, dass gesteigerte Rechenleistung ein guter Katalysator sein kann. In den letzten fünf Jahren hat sich auch das Quantum Computing den Weg von reiner Theorie zur algorithmen- und anwendungsnaher Entwicklung gebahnt. Vor allem mit der breiten Verfügbarkeit erster Hardware findet diese neuartige Technologie immer mehr Aufmerksamkeit.

FI CODE: Zentrale Rolle in deutscher Forschungslandschaft

Seit 2018 spielt das Forschungsinstitut CODE als erster Hub im Netzwerk von IBM in Deutschland eine Schlüsselrolle, da seine Forschenden schon frühzeitigen Zugriff auf die neuste Hardware hatten. Die Geschwindigkeit, in der die Größe und Qualität der einzelnen Prozessoren wächst, macht dies zu einem essentiellen Vorteil in der Forschung.

NISQ-Ära

Für sinnvolle Anwendungen ist dieses Wachstum essentiell, da sich das Quantum Computing zurzeit in der NISQ-Ära befindet, in der nur mittelgroße, fehlerbehaftete Prozessoren existieren. Entwickelte Lösungen müssen also mit wenig Rechenleistung und ungenauen Ergebnissen umgehen können.

Deutsche Bundesbank als Vorreiter

Wegen der grundsätzlichen Unterschiede zur klassischen Informatik ist es für Unternehmen wichtig, sich frühzeitig mit dem Potential für Quantum Computing auseinanderzusetzen. Die Deutsche Bundesbank hat hier ihre Vorreiterrolle wahrgenommen und eine entsprechende Studie bei Accenture in Auftrag gegeben.

Optimierungspotentiale und Intelligentes Benchmarking

Das Forschungsinstitut CODE vertreten durch Maximilian Moll und Stefan Pickl war Teil der wissenschaftlichen Begleitung. Dabei wurden fundierte Einschätzungen für die Anwendbarkeit, mögliche Benchmarks und den zeitlichen Horizont des Quantum Computings für Banken im Allgemeinen und die Bundesbank in ihrer Aufsichtsfunktion erarbeitet. Die Forschungsgruppe COMTESSA hatte bereits 2010 erste Kontakte zu IBM in Rüschlikon in diesem Themenfeld von Seiten der UniBw M aufgebaut, um insbesondere OR-Anwendungen und Optimierungspotentiale zu evaluieren.

Quantencomputer „IBM Q System One“.

ABB.: ADOBE STOCK / TIERNEY; IBM / ANDREW LINDEMANN

Use Cases & Empfehlungen

Um die Bundesbank vorzubereiten, wurde eine Übersicht über Hardware, OR-nahe Algorithmen und die Forschungslandschaft in Deutschland erstellt. Wesentlich zentraler war jedoch die Ausarbeitung konkreter Use Cases, die mit der Bundesbank identifiziert wurden. Für jeden wurde die Dringlichkeit, der Mehrnutzen durch Quantentechnologien, sowie die zu verwendende Algorithmik eingeschätzt.

Schließlich wurde eine zeitliche Entwicklungslinie erarbeitet, die auszubildende Kompetenzen und passende Teamgrößen und -konstellationen übersichtlich und plausibel darstellt.

Juniorprof.
Dr. Maximilian Moll

maximilian.moll@unibw.de

+49 89 6004 2248

https://www.unibw.de/comtessa

Kooperationspartner:
Deutsche Bundesbank & Accenture

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 steht die Analyse und Simulation komplexer Systeme sowie die Entwicklung von datengetriebenen Optimierungsverfahren zur IT-basierten Entscheidungsunterstützung.

Projekt REAVRS

Identifikation bestehender Angriffspotentiale für das System Bahn

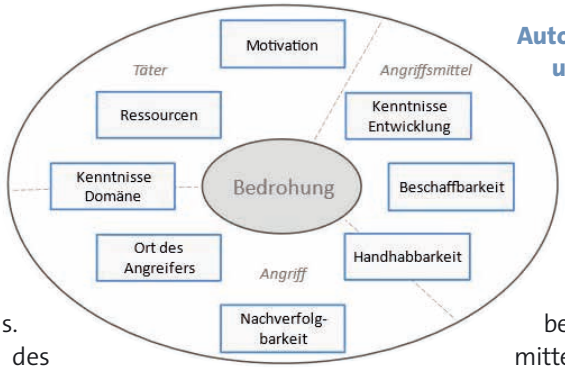
Basierend auf der zunehmenden Anwendung von Big Data, IT etc., weist das System Bahn eine erhöhte Vulnerabilität gegenüber Angriffen von Dritten auf. Ein generelles Vorgehen bzgl. einer einheitlichen Angriffssicherheit hat sich bis dato nicht durchgesetzt. REAVRS identifiziert Gefahrenpotentiale des Systems Bahn, um anschließend intelligente 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 einer detaillierten Systemdefinition. Eine funktionale Abbildung des (deutschen) Eisenbahnsystems wird entwickelt, gefolgt von einer präzisen Charakterisierung und Analyse erfolgter Angriffe sowie einer Beschreibung typischer Kontexte. Angriffsmöglichkeiten bzw. Bedrohungsszenarien werden systematisiert, und eine Gefährdungsidentifikation wird auf Basis einer OR-basierten Systemanalyse 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 Cyber-Angriffe identifiziert. Eine Ursachenanalyse wird mit einer Selektion von repräsentativen Vignetten durchgeführt. Im finalen Schritt wird die entwickelte Methodik in eine komfortable IT-basierte Entscheidungsunterstützung Umgebung und ein zukunftsweisendes Managementcockpit eingebettet.

Identifikation von Kenngrößen

Werden die Vignetten im Detail betrachtet, so lassen sich die in der Abbildung dargestellten Kenngrößen ableiten.

Automatisierung, Lagebild und Management Cockpit

Nach der Identifikation der Kenngrößen für die Bedrohung werden die einzelnen Kenngrößen der Bedrohung mit den Werten 1–5 versehen (von kaum bedrohlich (1) bis höchst bedrohlich (5)) und die Ergebnisse mittels eines sogenannten Fischgrätendiagramms veranschaulicht.

Diese detaillierte Ursachenanalyse geht in die anschließende komplexe Risikoanalyse ein. Aktuell wird 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.

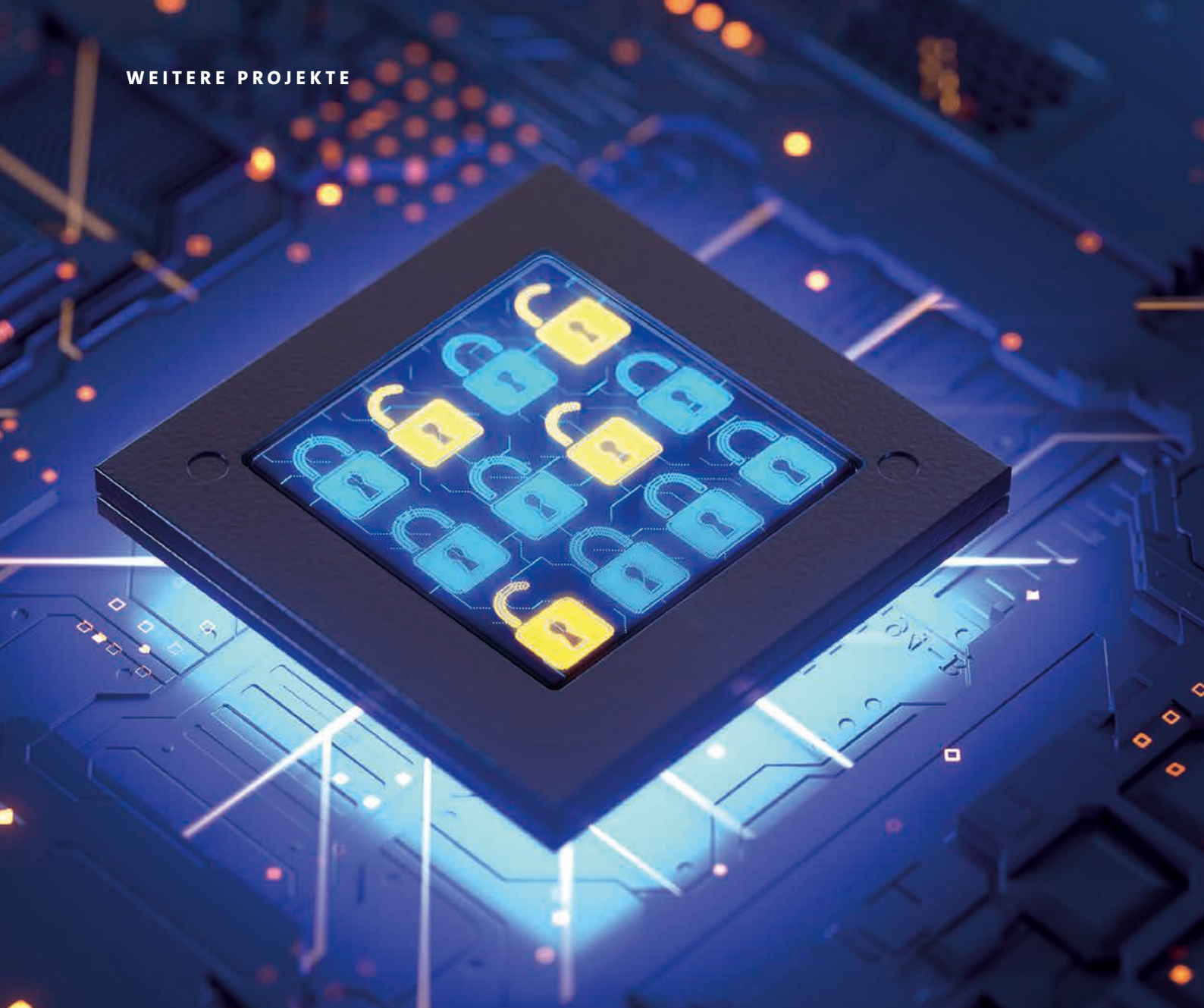
Prof. Dr. Stefan Pickl

stefan.pickl@unibw.de

+49 89 6004 2400

www.unibw.de/comtessa/forschung/reavrs

Gefördert durch: Deutsches Zentrum für Schienenverkehrsforschung (DZSF)



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 Softwareverifikationen für Betriebssysteme und graphenorientierte Modellierung von IoT-Netzwerken. Die Forschung erfolgt im Rahmen von Doktorarbeiten und Industrieprojekten.

Mathematik bringt Sicherheit

Anwendung von formaler Programmverifikation in industrieller Software-Entwicklung

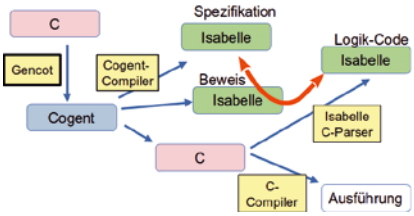
Programmierfehler beeinträchtigen die Sicherheit von softwarebasierten Systemen. Die formale Programmverifikation verspricht dies zu ändern, erfordert aber einen extremen Aufwand für reale Programme wie die besonders sicherheitskritischen Betriebssysteme. In den Projekten HoBIT und SW_GruVe erhöht das Team der Forschungsgruppe zusammen mit einem Industriepartner den Automatisierungsgrad von formaler Verifikation, um sie näher zur Praxis zu bringen.

SYSTEME UND GERÄTE mit eingebetteten IT-Funktionen sind höchstens so sicher wie das Betriebssystem (BS), das als zentrale Basis aufbauend auf der Hardware verwendet wird. Der BS-Kern läuft im freizügigsten Modus der Hardware. Wenn er kompromittiert wird, kann das Verhalten aller Hard- und Softwarekomponenten im System modifiziert werden. Um diese Gefahr zu verringern werden in mikrokern-basierten BS die Systemteile strikt voneinander isoliert.

Aber auch hier können Programmierfehler in den Systemteilen direkt zu unerwünschtem Verhalten führen oder ein Einfallstor für Angriffe bilden. Die wirksamste Maßnahme gegen Fehler ist ein formaler Beweis der Fehlerfreiheit. Für den Mikrokern seL4 wurde ein solcher Beweis erfolgreich durchgeführt, der Aufwand war aber extrem hoch. Andere Systemteile haben zum Teil erheblich höheren Umfang, damit ist ein Beweis der Fehlerfreiheit bei kommerzieller Entwicklung bisher nicht praktikabel.

Formale Verifikation

Bei formaler Verifikation eines Programms wird ein mathematischer Beweis dafür erstellt, dass es sich gemäß einer abstrakten mathematischen Spezifikation verhält. Wegen der Komplexität des Beweises ist dafür der Einsatz von Rechnerunterstützung entscheidend. Diese bieten Beweisassistenzsysteme wie Isabelle oder Coq.



Gencot übersetzt von C nach Cogent und erleichtert dadurch die formale Verifikation.

Formale Verifikation funktioniert am besten, wenn ein Programm von vornherein für dieses Ziel entwickelt wird, möglichst in einer dafür geeigneten höheren Programmiersprache. Für die von einer australischen Forschungsgruppe entwickelte Sprache Cogent erzeugt der Compiler neben dem ausführbaren Code sogar die abstrakte Spezifikation und den Beweis, dass sich der Code entsprechend verhält.

In der Praxis werden BS-Komponenten aber meist in C programmiert, einer maschinennahen Programmiersprache, die für die Anwendung formaler Verifikation denkbar ungeeignet ist. Auch im Dezember 2022 steht C im Tiobe-Index der meistgenutzten Programmiersprachen noch auf Platz zwei, daher ist die formale Verifikation von C-Code für die Software-Industrie von besonders hoher Relevanz.

Projekte HoBIT und SW_GruVe

In den Projekten HoBIT und SW_GruVe war das Ziel, die Praxistauglichkeit der formalen Verifikation von C-Code zu verbessern. Dazu entwickelten die Forscherinnen und Forscher das Werkzeug Gencot für die weitgehend automatische Übersetzung von C nach Cogent. Die Korrektheit der Übersetzung wird dabei nicht bewiesen. Für das resultierende Cogent-Programm ist also nicht zu 100 % sicher, dass es dasselbe macht wie das Originalprogramm. Dafür erhält man aber eine bewiesenermaßen korrekte abstrakte Beschreibung des Verhaltens. Als Demonstration wurde Gencot erfolgreich verwendet, um für Komponenten des BS TRENTOS entsprechende Implementierungen in Cogent zu erzeugen. Der C-Code dieser Komponenten wurde von den Entwicklern des Projektpartners Hensoldt Cyber bereitgestellt.

Prof. Dr. Gunnar Teege

gunnar.teege@unibw.de

+49 89 6004 3353

https://go.unibw.de/fomset

Gefördert durch:
Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi)

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

Kooperationen

Deutschland und die Welt

ABB.: ADOBE STOCK / GREENBUTTERFLY

Nationale Partner

Das FI CODE arbeitet in Deutschland mit 52 Partnern in 32 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 52 Institutionen in 32 Städten und Gemeinden zusammen. Besondere Schwerpunkte liegen dabei auf Bayern bzw. dem Münchner Raum, Nordrhein-Westfalen und Hessen. ■

	Institution	Ort
1	Hochschule Aalen	Aalen
2	Universität Bamberg	Bamberg
3	Universität Bayreuth	Bayreuth
4	IOTA-Stiftung	Berlin
5	Moysies & Partners GmbH	Berlin
6	Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN)	Berlin
7	Fachhochschule Bielefeld	Bielefeld
8	Ruhr-Universität Bochum (RUB)	Bochum
9	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Bonn
10	Technische Universität Chemnitz	Chemnitz
11	Hochschule Darmstadt (h_da)	Darmstadt
12	Nationales Zentrum für angewandte Cybersicherheit ATHENE	Darmstadt
13	Technische Universität Darmstadt	Darmstadt
14	Technische Universität Dresden (TUD)	Dresden
15	Universität Duisburg-Essen (UDE)	Duisburg/Essen
16	Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)	Erlangen/Nürnberg
17	secunet Security Networks AG	Essen
18	Frankfurt University of Applied Sciences	Frankfurt a. M.
19	neosfer GmbH	Frankfurt a. M.
20	nuix	Frankfurt a. M.
21	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ)	Garching
22	Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg (HSU)	Hamburg
23	Leibniz Universität Hannover (LUH)	Hannover
24	Technische Universität Ilmenau	Ilmenau

	Institution	Ort
25	SoSafe GmbH	Köln
26	Deutsches Zentrum für Luft- und Raumfahrt (DLR)	Köln/Oberpfaffenhofen
27	BWI GmbH	Meckenheim
28	Bayerisches Landesamt für Steuern (BayLfSt)	München
29	Bayerisches Staatsministerium für Digitales (BayStMD)	München
30	BMW AG	München
31	Center for Digital Technology and Management (CDTM)	München
32	ESG Elektroniksystem- und Logistik-GmbH	München
33	FAST-DETECT GmbH	München
34	Google München	München
35	H&D GmbH	München
36	Ludwig-Maximilians-Universität München (LMU)	München
37	Rohde & Schwarz GmbH & Co. KG	München
38	Technische Universität München (TUM)	München
39	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	München
40	Bayerisches Landesamt für Sicherheit in der Informationstechnik (BayLSI)	Nürnberg
41	IABG Industrieanlagen-Betriebsgesellschaft mbH	Ottobrunn
42	Universität Paderborn (UPB)	Paderborn
43	Universität Passau	Passau
44	Universität Siegen	Siegen
45	Airbus Cybersecurity GmbH	Taufkirchen
46	HENSOLDT Cyber GmbH	Taufkirchen
47	Airbus Defence and Space GmbH	Taufkirchen/Ottobrunn/ Manching
48	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE	Wachtberg/Bonn
49	Hessisches Landeskriminalamt (HLKA)	Wiesbaden
50	Hessisches Polizeipräsidium für Technik (HPT)	Wiesbaden
51	Bundeskriminalamt (BKA)	Wiesbaden/Berlin
52	Julius-Maximilians-Universität Würzburg (JMU)	Würzburg

ABB.: TAUSENDBLAUWERK.DE


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

Internationalität

Auch international pflegt CODE ein großes Netzwerk. Im Jahr 2022 stammten die Mitarbeitenden aus 17 Ländern. In 25 Ländern gab es 80 Kooperationspartner.

Mitarbeitende

Nationalität	Anzahl
Ägyptisch	2
Argentinisch	1
Bangladeschisch	1
Beninisch	1
Bosnisch	1
Britisch	1
Bulgarisch	1
Deutsch	105
Finnisch	1
Französisch	2
Griechisch	1
Indisch	1
Italienisch	1
Kroatisch	1
Österreichisch	8
Slowenisch / Deutsch	1
Südkoreanisch	1

Internationale Kooperationspartner

Land	Partner
Ägypten	European Universities in Egypt
	German University in Cairo
Australien	University of Melbourne
	University of New South Wales
Belgien	EIT Digital
	Katholieke Universiteit Leuven
Dänemark	Aarhus Universitet
Frankreich	Centre de Recherche de l'Ecole de l'Air (CREA)
	CyberDetect
	INRIA/Université de Lorraine
	Université catholique de l'Ouest (UCO)
Griechenland	ATHENA Research Center
	Foundation for Research and Technology Hellas

ABB.: ISTOCK / BLUE PLANET STUDIO

Land	Partner
Griechenland	National Cyber Security Authority of the Ministry of Digital Governance
	Ubitech
Israel	Ben-Gurion-Universität des Negev
Italien	Centro Ricerche Fiat
	Telecom Italia
	Università degli Studi dell'Insubria
	Università degli Studi di Milano
Kanada	evolutionQ Inc.
	University of Waterloo
Luxemburg	Université du Luxembourg
Niederlande	Arthur's Legal B.V.
	SIDN - Stichting Internet Domeinregistratie Nederland
	SURFnet
	Universiteit Twente
	Universiteit Utrecht
Norwegen	Norges teknisk-naturvitens-kapelige universitet
	Oslo Metropolitan University
	Telenor Group
	Universitetet i Oslo
Österreich	Johannes Kepler Universität Linz
	Österreichisches Bundesheer
	Plasser & Theurer GmbH
	PwC Österreich GmbH
	SBA Research
	Software Competence Center Hagenberg
Portugal	Efacec Electric Mobility
	Universidade de Lisboa
Rumänien	Universitatea Babeș-Bolyai
	Bitdefender
Schweden	Chalmers tekniska högskola
	Ericsson
	RISE Research Institutes of Sweden
	Göteborgs universitet
	Uppsala universitet

Land	Partner
Schweiz	École Polytechnique Fédérale de Lausanne
	ID Quantique SA
	RUAG
	Université de Lausanne
	Universität St. Gallen
	Universität Zürich
Slowenien	Jožef Stefan Institute
	Univêrza v Máriboru
Spanien	Atos Spain S.A.
	CaixaBank
	i2CAT
	IMDEA Software Institute
	NTT Data
	Telefonica I+D
	Universitat Autònoma de Barcelona
Südkorea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Tschechien	Flowmon Networks
	Masarykova univerzita
Ungarn	Budapesti Műszaki és Gazdaságtudományi Egyetem
	Eötvös Loránd Tudományegyetem
USA	Auburn University, College of Engineering
	Davidson College
	George Marshall Center
	University of Arizona, College of Engineering
	University of North Carolina at Charlotte
Vereinigtes Königreich	Imperial College London
	King's College London
	Lancaster University
	University College London
	University of Glasgow
	University of Surrey
Zypern	Cyprus University of Technology

Nachwuchs-förderung

Chancen und Angebote

ABB.: ADOBE STOCK / MONTRI

Studienpreis des Forschungsinstituts CODE 2022

Effiziente Nutzbarmachung von Schwachstellen in Telekommunikations-endgeräten

Das Forschungsinstitut Cyber Defence und Smart Data (CODE) zeichnet zusammen mit der Firma Giesecke + Devrient GmbH in diesem Jahr Herrn Lars Fuchs mit dem CODE-Studienpreis aus. In seiner Masterarbeit befasste sich der Informatiker mit der effizienten Nutzbarmachung von Schwachstellen in Telekommunikationsendgeräten.

DIE ENDE-ZU-ENDE Verschlüsselung auf mobilen Endgeräten gewinnt zunehmend an Bedeutung. In Direktnachrichtenanwendungen wie Signal und WhatsApp kommt die Technik zum Einsatz, wo sie die User vor unerwünschtem Mitlesen schützt. Dies hat große Vorteile. Doch wie jede Technik, die Neuerungen mit sich bringt, hat sie auch Nachteile. Die Verschlüsselungstechnik gibt Kriminellen und Terrorverdächtigen die Möglichkeit, sich dem Präventionsschutz und der Strafverfolgung durch Behörden zu entziehen. Dabei ist die Telekommunikationsüberwachung ein wichtiges Werkzeug im Repertoire der Behörden. Sie kann sowohl repressiv als auch präventiv eingesetzt werden. Die Maßnahmen helfen bei der Strafverfolgung und haben das Potenzial terroristische Angriffe auf die Bundesrepublik Deutschland zu verhindern. In Einzelfällen kann als Alternative zur klassischen Methode die sogenannte Quellen-Telekommunikationsüberwachung zum Einsatz kommen. Dabei wird eine Software auf dem Gerät der Zielperson installiert, um entsprechende Daten auszuleiten.

Die Masterarbeit von Herrn Fuchs, die in Zusammenarbeit mit der ZITiS angefertigt wurde, trägt zur Vereinfachung und Effizienzsteigerung solcher Operationen bei. In seiner Arbeit entwickelte er ein System zur Identifizierung, Bewertung, Auswahl und Nutzung von Schwachstellen. Dadurch können für bekannte Schwachstellen schneller verwendungsfähige Exploits gefunden bzw. entwickelt werden. Während die Suche und Entwicklung von sogenannten Zero-Day-Exploits – also Schwachstellen, die den Unternehmen bislang unbekannt sind – sehr aufwendig ist, können mit Hilfe des in der Arbeit entwickelten Systems bekannte Schwachstellen schnell und effizient nutzbar gemacht werden.

Des Weiteren trägt die Arbeit zur verantwortungsvollen Nutzung von Schwachstellen bei. Das System zur Bewertung der Schwachstellen bezieht unter anderem gesetzliche Rahmenbedingungen sowie Auswirkungen auf das Zielgerät mit ein, um eine Umgangsempfehlung für bestimmte Schwachstellen ausstellen zu können. So wird sichergestellt, dass die Ausnutzung von Exploits nicht zu einer unnötigen Beeinträchtigung des Zielgerätes führt.

Der CODE-Studienpreis wurde im Rahmen der großen Masterfeier am 10. Dezember 2022 auf dem Campus der Universität der Bundeswehr durch Vizepräsidentin Prof. Eva-Maria Kern im Beisein des leitenden Direktors des FI CODE Prof. Wolfgang Hommel und Dr. Michael Tagscherer von G+D verliehen. ■

Für ihre exzellenten Leistungen wurden insgesamt 18 Absolventinnen und Absolventen des Abschlussjahrgangs 2022 mit Studienpreisen ausgezeichnet.

ABB.: ADOBE STOCK/ KANNAPAT; 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 FI 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

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/8o

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

Auszeichnung

Schwärzel-Preis für Leonhardt Kunczik

„Reinforcement Learning with Hybrid Quantum Approximation in the NISQ context“

DER HEINZ SCHWÄRZEL-PREIS für Grundlagen der Informatik wird seit 2006 jährlich vergeben und richtet sich an hervorragende Promovierte der drei Münchener Universitäten. Dem Stifter und Ehrenmitglied der Gesellschaft für Informatik e. V., Prof. Heinz Schwärtzel, ist es ein besonderes Anliegen, die grundlagenorientierte Informatik-Forschung mit diesem Preis zu fördern. Das Forschungsinsitut CODE freut sich, dass im Jahr 2022 das CODE-Mitglied Dr. Leonhard Kunczik die Auszeichnung erhielt. Der Preis wurde von Prof. Heinz Schwärtzel am 2. Dezember 2022 an der TU München überreicht.

Quanten-Reinforcement-Ansatz

Die prämierte Dissertation geht von der Beobachtung aus, dass komplexe Optimierungsumgebungen selbst mit modernen Methoden des sog. Reinforcement Learning immer noch an ihre Komplexitätsgrenzen stoßen und dadurch kaum algorithmisch handhabbar sind. In seiner primär grundlagenorientierten Arbeit erweiterte Herr Kunczik einerseits die theoretischen Ansätze im klassischen Reinforcement-Learning-Kontext, andererseits versuchte er gezielt, „anwendbare“ Methoden des Quantencomputing in die umfassenderen Lösungsansätze und -verfahren zu integrieren, um die Komplexität „algorithmisch beherrschbar“ zu machen. Leonhardt Kunczik entwickelte insbesondere einen sog. Quanten-Reinforcement-Ansatz, der sich dadurch auszeichnet, dass das theoretische Konzept von Circuits Quantum Variational als zentrales Element in das entsprechende komplexe algorithmische Optimierungs-Framework eingebettet wird.

Interdiction Games: Attacker-Defender Scenario

In seiner Arbeit evaluierte er seine Verfahren gegenüber klassischen etablierten Optimierungsansätzen. Hierbei ging er von den allgemeinen Frozen-Lake-Szenarien aus, die durch seine Untersuchungen auf allgemeine komplexere Interdiction-Beispiele übertragen werden konnten. Die Modellentwicklungen zeichnen sich dadurch aus, dass sie Verfahren im entsprechenden Kontext erstmals praxisnah auf einer aktuellen Quantumcomputer-Architektur (von IBM) betrachtet werden: Dies geschieht im Rahmen der Noisy Intermediate-Scale-Quanten (NISQ)-Hardwareumgebung.

Prof. Dr. Heinz Schwärzel, Dr. Leonhardt Kunczik, Prof. Dr. Stefan Pickl (v. l. n. r.)

ABB.: UNIBW M

Komplexe Optimierungsszenarien

Die Arbeit stellt insgesamt ein sehr umfassendes Grundlagenwerk mit hoher wissenschaftlicher Qualität innerhalb der Informatik dar. Sie geht von einer zentralen aktuellen Fragestellung im CODE-Kontext innerhalb von komplexen Optimierungsszenarien („Frozen-Lake-Umgebungen“) aus, und leitet daraus zunächst mit der Formulierung der beiden Kern-Forschungsfragen einen sehr hohen wissenschaftlichen Anspruch ab. Beide Themenkomplexe werden überzeugend behandelt, und auch im Rahmen der aktuellen wissenschaftlichen theoretischen Möglichkeiten sicher beantwortet.

Herr Kunczik hat nicht nur Perfomanceverbesserungen sehr ansprechend entwickelt, er hat auch Problemzusammenhänge in der Arbeit überzeugend analysiert, und damit die theoretischen Grundlagen für weitere Untersuchungen erstmals zur Verfügung gestellt.

Optimierungsframework

Mit der vorgelegten Arbeit hat Herr Kunczik eindrucksvoll ein umfassendes Optimierungsframework präsentiert und nachvollziehbar in eine neuartige theoretische Behandlung von komplexen Optimierungsszenarien eingebettet, die sich für weitere Untersuchungen anbietet:

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

Leonhardt Kunczik

PROMOTIONEN 2022

Gonzalo Barbeito

„Design eines Frameworks zur Verteilung von Hilfsgütern in Antizipation eines katastrophalen Stromausfalls“

EIN ZENTRALES THEMA bei humanitären Einsätzen während schwerwiegender Stromausfälle ist die rechtzeitige Verteilung von Hilfsgütern an Notleidende. Diese Arbeit modelliert die dabei auftretenden Herausforderungen als Rich-Vehicle-Routing-Problem mit einer neuen Kombination von taxonomischen Attributen und präsentiert eine interaktive Experimentierumgebung für profunde Analysen der Problemlösungen.

Gonzalo Barbeito wurde im Juni 2022 bei Prof. Pickl promoviert. Derzeit ist er bei Amazon Web Services als Professional Services Consultant beschäftigt. ■

Michael Fröhlich

„Usable Cryptocurrency Systems“

MICHAEL FRÖHLICHS Forschung untersucht die Herausforderungen der Benutzerfreundlichkeit von Kryptowährungen und der Blockchain-Technologie und stellt verschiedene Ansätze zur Bewältigung dieser Herausforderungen vor. Seine Dissertation ist in drei Hauptabschnitte unterteilt: eine systematische Übersicht über die bestehende Human-Computer-Interaction-Forschung zu Kryptowährungen, eine Untersuchung des Nutzerverhaltens und der Herausforderungen sowie eine Bewertung verschiedener Ansätze zur Verbesserung der Benutzerfreundlichkeit von Anwendungen. Die Dissertation schließt mit einer Reflexion über die zukünftige Rolle der Human-Computer-Interaction-Forschung im Bereich der Kryptowährungen und der Blockchain-Technologie.

Michael Fröhlich promovierte im Dezember 2022 bei Prof. Alt promoviert. Derzeit ist er am Center for Digital Technology and Management (CDTM), einem gemeinsamen Institut der LMU und TUM, beschäftigt. ■

Sarah Prange

„Usable Privacy and Security in Smart Homes“

DIE DOKTORARBEIT von Sarah Prange trägt dazu bei, benutzbare Privatsphäre- und Sicherheitsmechanismen im Kontext des „intelligenten Zuhauses” zu entwickeln. Insbesondere werden a) die Wahrnehmung von Privatsphäre sowie Anforderungen an potenzielle Mechanismen untersucht, sowie b) Konzepte und Prototypen für Privatsphäre- und Sicherheitsmechanismen vorgestellt. Der Fokus liegt hierbei auf zwei Zielgruppen: den Bewohnern sowie den Gästen eines intelligenten Zuhauses.

Die Ergebnisse dieser Doktorarbeit legen den Grundstein für zukünftige Entwicklung und Evaluierung von benutzbaren Privatsphäre- und Sicherheitsmechanismen im intelligenten Zuhause.

Sarah Prange promovierte im Dezember 2022 bei Prof. Dr. Florian Alt. Derzeit ist sie beim Forschungsinstitut CODE als wissenschaftliche Mitarbeiterin beschäftigt. ■

ABB.: ADOBE STOCK; PRIVAT (5)

Radiah Rivu

„Out-of-the-Lab Virtual Reality Studies“

RADIAH RIVU untersucht in ihrer Dissertation, wie Virtual-Reality-Studien außerhalb von Laborumgebungen durchgeführt werden können. Die Arbeit ist dadurch motiviert, dass heute viele Personen ein VR-Setup besitzen – entsprechend können sie von zu Hause aus an Studien teilnehmen, was nicht nur den Aufwand für Studienteilnehmer reduziert, sondern auch größere und diversere Stichproben ermöglicht. Die Dissertation beschäftigt sich sowohl mit den Herausforderungen von technischer Seite (z. B. Plattformen zur Studienumsetzung und Datenerhebung) als auch von Nutzerseite (z. B. Herausforderungen beim Recruiting, Durchführung ohne physikalische Präsenz eines Studienleiters etc.).

Radiah Rivu promovierte im Oktober 2022 bei Prof. Dr. Florian Alt. Derzeit ist sie beim Forschungsinstitut CODE als wissenschaftliche Mitarbeiterin beschäftigt. ■

Robert Rödler

„Profilzuordnung über soziale Netze anhand von Metadaten“

PROFILZUORDNUNG ÜBER soziale Netze anhand von Metadaten untersucht, inwiefern sich zwei oder mehr Profile in unterschiedlichen sozialen Netzen ein und derselben Person zuordnen lassen, und dies nur anhand von Metadaten. Anhand eines Metamodells werden verfügbare und abrufbare Metadaten in sozialen Netzen diskutiert und basierend hierauf drei verschiedene Ansätze zur Profilzuordnung evaluiert. Hierbei konnte je nach Ansatz gezeigt werden, dass bereits geringe Mengen bestimmter Metadaten eine nahezu 100%ige Zuordnungsgenauigkeit ermöglichen. Daher schließt die Arbeit mit möglichen Maßnahmen zur Gewährleistung des persönlichen Datenschutzes.

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. ■

Michael Steinke

„Framework-Konzepte für Managementplattformen in föderierten softwarebasierten Netzen“

IN DER DISSERTATION werden geeignete Architekturbausteine für Managementplattformen für moderne virtuelle und zentral steuerbare Computernetze beschrieben. Ihre Eignung zielt primär auf das Management von Netzkomponenten im föderierten Kontext mit mehreren unabhängigen Organisationen ab. Die einzelnen Bausteine sind in Form von Softwareframeworks mit definierten Schnittstellen untereinander beschrieben und können dazu genutzt werden entweder bestehende Managementplattformen zu erweitern oder aber von Grund auf neu zu entwickeln. Die Arbeit trägt so zu einem sicheren Betrieb moderner dezentralisierter IT-Infrastrukturen wie der „Cloud“ bei.

Michael Steinke wurde im Juli 2022 bei Prof. Wolfgang Hommel promoviert. Derzeit ist er am Institut für Softwaretechnologie als Postdoktorand beschäftigt und ist im dtec.bw-Projekt DEFINE tätig. ■

Capture the Flag 2022

„The Spanning Tree – Catching B8tes“

Bei der achten Auflage des vom Forschungsinstitut CODE mit Unterstützung von ITIS e.V. und Team localos ausgerichteten „Capture the Flag“-Wettbewerbs traten auch 2022 wieder über 40 Teams online und in Präsenz auf dem Campus der UniBw M in zahlreichen spannenden Challenges gegeneinander an.

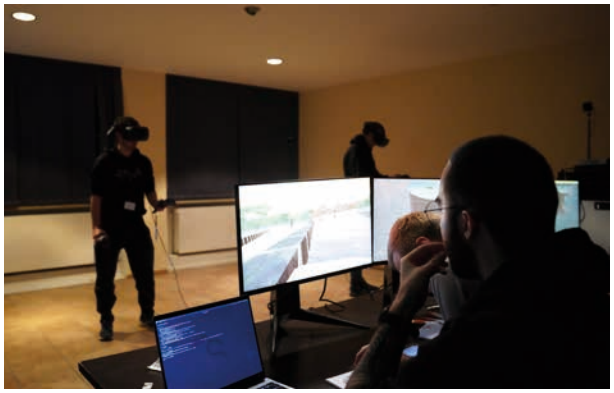
AM 25. UND 26. NOVEMBER 2022 fand im UniCasino auf dem Campus der Universität der Bundeswehr München der alljährliche Hacking-Wettbewerb „Capture the Flag“ (CTF) statt. Seit 2015 ist die Veranstaltung für viele ein gesetzter Termin. Hier können die Teilnehmenden nicht nur ihre Kompetenzen im Bereich der Cybersicherheit trainieren und ihr Wissen und Geschick zeigen, sondern das Ganze auch gleichzeitig mit viel Spaß und Action verbinden.

Von den über 80 Teams, die am Qualifying im Oktober teilnahmen, erhielten nur knapp die Hälfte eine Einladung, um beim Wettbewerb Ende November ihr Können zu zeigen. Neben den 21 Teams vor Ort nahmen wie bereits im Vorjahr weitere 20 Teams virtuell an einem separaten Online-Track teil.

In diesem Jahr stand der CTF unter dem Motto „The Spanning Tree – Catching B8tes“. In Anlehnung an den Film „The Hunger Games – Catching Fire“ waren während des rund 18-stündigen Events eine Reihe von Aufgaben, sog. Challenges, aus verschiedenen Kategorien zu lösen und so Punkte zu sammeln. Die einzelnen Challenges waren dabei auf einem virtuellen Spielfeld angeordnet. Analog zur Filmvorlage bestand dieses aus einer runden Spielarena mit unterschiedlichen Sektoren, wobei jeder der Sektoren eine der Kategorien Krypto, Web, Forensik, Misc, Reversing/Pwning sowie Virtual Reality/Hardware repräsentierte.

Unter den insgesamt 41 Challenges, die es für die Teams vor Ort zu lösen galt, waren es insbesondere die fünf Hardware-Challenges, die den Teilnehmenden alles abverlangten. So mussten beispielsweise Daten, die in einem Zigbee-Netz verschlüsselt übertragen wurden, zunächst mitgeschnitten und entschlüsselt werden, bevor für das Abgreifen des Keys von den Teilnehmenden ein neuer Netzknoten eingebracht werden konnte. In einer anderen Aufgabe war eine Torsteuerung zu überwinden, welche das gleichzeitige Öffnen zweier Tore verhindert. Unter geschicktem Ausnutzen des Modbus-Protokolls war der Steuerung vorzutäuschen, dass eines der Tore geschlossen ist, obwohl dieses bereits geöffnet wurde.

Die ganze Nacht hindurch arbeiteten die Teams intensiv an den gestellten Aufgaben und lieferten sich einen spannenden Wettkampf. Gegen Morgen dann setze sich langsam eine Gruppe von vier Teams ab, die sich bis kurz vor Schluss am Samstagmittag um 12:00 Uhr ein Kopf-an-Kopf-Rennen lieferten. Am Ende konnte der Vorjahressieger Team Nemesis den Vierkampf für sich entscheiden und die Teams 0x90, 40 Jahre die Bitflippers und Sabobatage hinter sich lassen. Den Online-Track gewann das Team Winnie the pwnd vor rckwrtz und Ignorital. Nach der Siegerehrung durch Wolfgang Hommel und Marcus Knüpfer konnten sich die glücklichen Titelverteidiger auf der Flag-of-Fame mit ihren Unterschriften verewigen. Zudem konnten sich die drei bestplatzierten Teams über Sachpreise wie bspw. Fachbücher freuen. Bei der Siegerehrung hob der Leitende Direktor des FI CODE, Wolfgang Hommel, hervor: „Es ist uns ein besonderes Anliegen, dass die Cybersecurity-Expertinnen und -Experten von morgen möglichst praxisnah ausgebildet werden – sei es über Veranstaltungen wie diese, unseren Masterstudiengang Cyber-Sicherheit, die Angebote unserer Cyber Range oder über externe Trainings“. Für alle Teilnehmenden war das CTF-Event wieder ein großer Spaß und viele Teams haben bereits ihre Teilnahme für das nächste Jahr angekündigt. ■



Volle Konzentration der teilnehmenden Teams während der Virtual-Reality-Challenge.

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 Studierende ihr theoretisches Wissen bereits anhand verschiedener praktischer Herausforderungen testen.

Wolfgang Hommel (l.), Leitender Direktor des FI CODE, und Marcus Knüpfer (r.), Kommissarischer CODE-Geschäftsführer, zusammen mit dem erfolgreichen Titelverteidiger „Team Nemesis“.

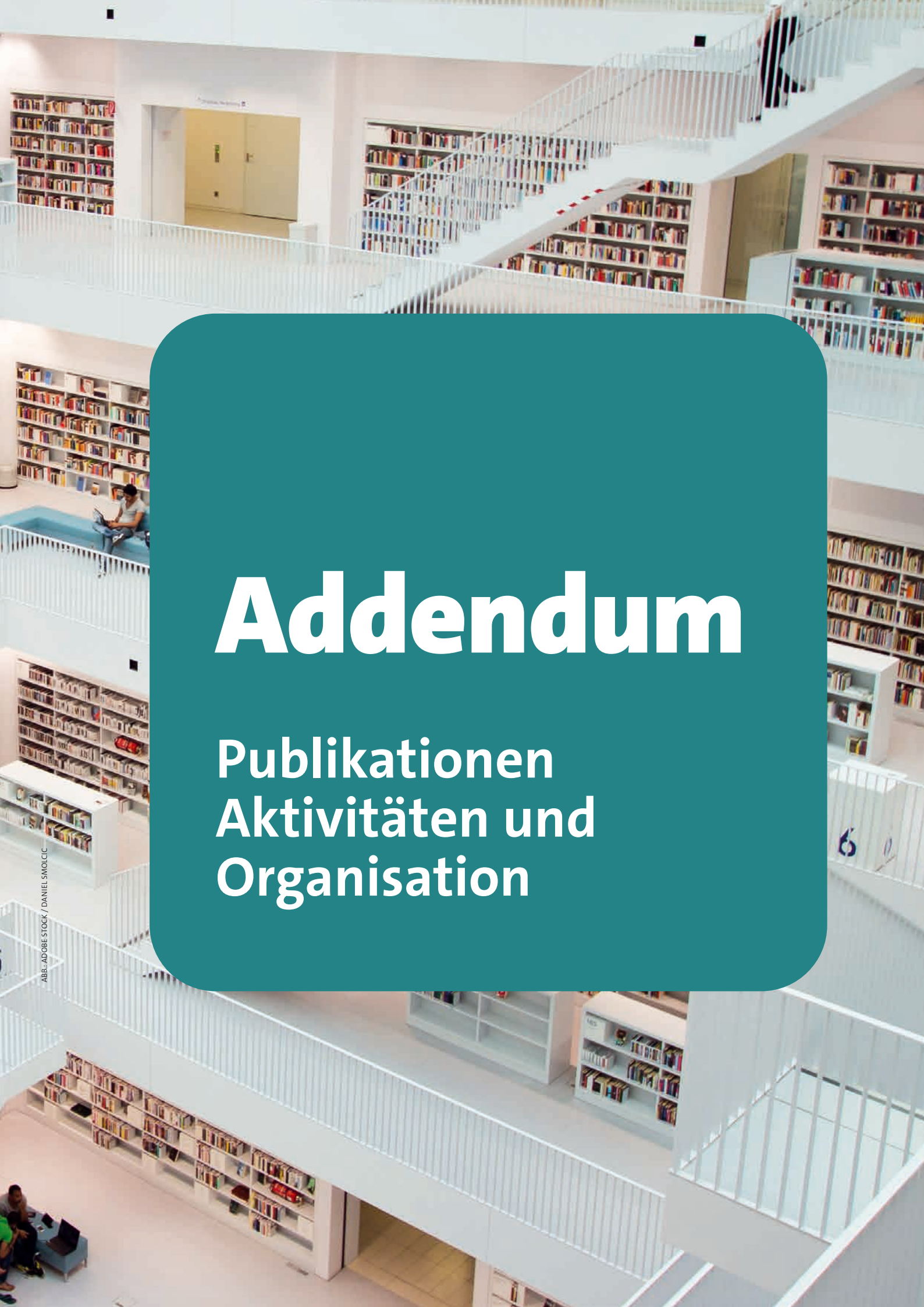
Mehr Informationen:

www.unibw.de/code/events/ctf

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

ctf@unibw.de

ALLE ABB.: FI CODE / B. BELLGRAU



Addendum

Publikationen
Aktivitäten und
Organisation

ABB.: ADOBE STOCK / DANIEL SMOLCIC

Prof. Dr.
Florian Alt

Benutzbare Sicherheit und Privatsphäre

PUBLIKATIONEN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FORSCHUNGSPROJEKTE

Voice of Wisdom

Im Projekt „Voice of Wisdom" werden Ansätze zur Verhinderung menschzentierter 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 – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGeneration EU finanziert.
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 Inc.
Laufzeit: 12/2021 – 12/2022

Scalable Biometrics

Dieses Projekt untersucht, wie Pervasive-Computing-Umgebungen verhaltensbiometrische 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

3665-V1	**Sichere Mensch-Maschine-Schnittstellen (WT)**
36651	**Benutzbare Sicherheit (WT)**
36653	**Praktikum Design sicherer und benutzbarer Systeme (FT)**
10123	**Software-Ergonomie (HT)**

MESSEN, TAGUNGEN, SEMINARE

- Mensch und Computer 2022: Inclusive Security by Design Workshop
- Mensch und Computer 2022: (Be-)Greifbare Interaktionen Workshop
- AFCEA Fachausstellung 2022: Vertretung des Forschungsinstituts CODE

PREISE UND AUSZEICHNUNGEN

- ACM SIGMM Test of Time Honorable Mention in the category of Multimedia Interfaces and Applications – MÜLLER, J., ALT, F., MICHELIS, D., SCHMIDT, A.: Requirements and Design Space for Interactive Public Displays
- ICL 2022 Best Paper Award – FRÖHLICH, M., VEGA VERMEHREN, J. A., PAHL, A., LOTZ, S., ALT, F., SCHMIDT, A., WELPE, I.: Prototyping with Blockchain: A Case Study For Teaching Blockchain Application Development at University

WEITERE FUNKTIONEN

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

Prof. Dr. Harald Baier

Digitale Forensik

PUBLIKATIONEN

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

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

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

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

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

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

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

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

LEHRE

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

MESSEN, TAGUNGEN, SEMINARE

Vorbereitung und Moderation des CAST-Workshops Forensik / Internetkriminalität am 15.12.2022, URL: https://cast-forum.de/workshops/infos/318

WEITERE FUNKTIONEN

- Gutachter für Journal of Digital Investigation und Computers & Security
- Mitgliedschaft in Programmkomitees Digital Forensics Research Workshop (DFRWS) EU 2022, Digital Forensics Research Workshop (DFRWS) APAC 2022, GI Sicherheit 2022, CAST Förderpreis 2022, CAST-GI Promotionspreis 2022, SKILL 2022
- Unterstützung des Programmdirektors bei der Einrichtung des Studiengangs ‚IT Security‘ an der Vietnamese-German University in Ho-Chi-Minh City, Vietnam

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

FORSCHUNGSPROJEKTE

ACSE – Airborne Cybersecurity Enhancement

Das Forschungsinstitut CODE und Airbus Defence and Space erforschen in diesem Projekt ausgewählte Fragestellungen zur Vermeidung von Sicherheitslücken in Avioniksystemen. Es behandelt Herausforderungen, die durch die Einführung neuer Technologien in bestehenden und zukünftigen Flugsystemen entstehen. Hauptziel ist ein umfassendes Verständnis relevanter Bedrohungen und deren Abwehr.

Gefördert durch: Airbus Defence and Space
Laufzeit: 2020 – 2024

APERITIF – Analysis Pipeline for Effective Vulnerability Identification Through Fuzzing

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

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021 – 2023

DEMISEC – Detecting Malicious Implants in Source Code

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

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021 – 2023

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

ECOOP 2022

WEITERE FUNKTIONEN

Mitglied des Programmkomitees

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

Prof. Dr. Michaela Geierhos

Data Science

PUBLIKATIONEN

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

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

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

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

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

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

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

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

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

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

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 Twitter und Facebook. Insbesondere Kampagnen, die von staatlichen Akteuren vorangetrieben werden, stehen im Fokus.

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

KI-basierter Sprachsignal-Decoder

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

Laufzeit: 09/2021 – 12/2024

NAWI – News-Artikel und Wissen

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

Laufzeit: 12/2021 – 11/2024

Synthetische Datengenerierung und -Detektion

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

Gefördert durch: Zentrale Stelle für Informationstechnik im Sicherheitsbereich
Laufzeit: 06/2022 – 05/2025

VIKING – Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen

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

Gefördert durch: Bundesministerium für Bildung und Forschung
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 (HT + WT + FT)**

3853 **Analyse unstrukturierter Daten (HT)**

WEITERE FUNKTIONEN

- Mitglied im Fakultätsrat INF (seit 10/2022)
- Mitglied im Beirat „Deutsche Biographie“ der Historischen Kommission bei der BAdW
- Gutachterin für die Europäische Kommission
- Gutachterin für VDI/VDE Innovation + Technik

Mitglied des Programmkomitees

- CLEF 2022 – Conference and Labs of the Evaluation Forum Information Access Evaluation meets Multilinguality, Multimodality, and Visualization
- DHd 2022 – 8. Jahrestagung des Verbands Digital Humanities im deutschsprachigen Raum (Vorsitzende)
- EMNLP 2022 – The 2022 Conference on Empirical Methods in Natural Language Processing
- PATTERNS 2022 – The Fourteenth International Conference on Pervasive Patterns and Applications
- SEMANTiCS 2022 – 18th International Conference on Semantics Systems

Hon.-Prof. Dr. Udo Helmbrecht

Quanten-kommunikation

PUBLIKATIONEN

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

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

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

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

LEHRE

3695 **Quantenkommunikation (WT)**

MESSEN, TAGUNGEN, SEMINARE

- Quantum Industry Days Switzerland
- Quantum Business Network Meeting on Quantum Communication
- Quantensymposium zur Operationalisierung Quantentechnologien für die Bundeswehr (QT4Bw)
- QR.X Faserstreckenworkshop Berlin
- Pan-European Quantum Internet Hackathon 2022 Amsterdam

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

PUBLIKATIONEN

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

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

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

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

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

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

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

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

FORSCHUNGSPROJEKTE

ACSE – Airborne Cybersecurity Enhancement

Airborne Cybersecurity Enhancement (ACSE) ist ein Forschungskooperationsprojekt zwischen FI CODE und Airbus Defence and Space. Das Projekt untersucht Herausforderungen im Bereich Cybersicherheit, die sich aus Entwicklung und Betrieb komplexer und vernetzter Systemverbände luftgestützter Plattformen ergeben. Der Fokus unseres Teams liegt auf Konzepten für sichere Softwareentwicklung im Entwicklungsprozess sowie Netzwerksicherheit.

Gefördert durch: Airbus Defence and Space
Laufzeit: 12/2019 – 12/2023

DEFINE – DC-Netze für eine sichere Energieversorgung

Gleichstromnetze stellen eine effiziente Variante für heute gängige Wechselstromnetze für die Stromverteilung dar und können somit ein Baustein zur Energiewende sein. In diesem Projekt werden Mittelspannungsgleichstrom-(MVDC)-Netze für den Praxiseinsatz erforscht. Der Schwerpunkt des FI CODE liegt in der Entwicklung von geeigneten Managementlösungen für den zuverlässigen Betrieb von MVDC-Netzen.

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

LIONS – Ledger Innovation and Operation Network for Sovereignty

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

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

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 Informationssicherheitsmanagement (HT)**
5501	**Seminar Sicherheitsaspekte von Wide Area Networks über LoRa (HT)**
5507	**Sichere vernetzte Anwendungen (FT)**
5508	**Sicherheitsmanagement (FT)**

WEITERE FUNKTIONEN

- Mitglied im Fakultätsrat INF (bis 09/2022)
- Prüfungsausschuss Master of Intelligence & Security Studies
- Mitglied im Betriebsausschuss des Deutschen Forschungsnetzes

Mitglied des Programmkomitees

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

Prof. Dr. Johannes Kinder

PATCH: Programmanalyse, -transformation, -verstehen und -härtung

PUBLIKATIONEN

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

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

LEHRE

38191 **Reverse Engineering (FT)**

38192 **Praktikum Reverse Engineering (FT)**

38491 **Dynamische Programmanalyse (HT)**

38492 **Praktikum Fuzzing (HT)**

38381 **Statische Programmanalyse (WT)**

38382 **Praktikum Statische Programmanalyse (WT)**

55011 **Seminar Softwarehärtung (HT)**

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

WEITERE FUNKTIONEN

Beiratsmitglied, Centre for Doctoral Training in Cyber Security for the Everyday, Royal Holloway, University of London

Mitglied des Programmkomitees

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

Prof. Dr.-Ing. Mark Manulis

PACY: Privacy and Applied Cryptography

PUBLIKATIONEN

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

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

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

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

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 **Research Trends in Cryptography (HT)**

MESSEN, TAGUNGEN, SEMINARE

- 20th International Conference on Applied Cryptography and Network Security (ACNS) 2022 (Teilnahme, Leitung der Sitzung Cryptographic Protocols)

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

- 20th International Conference on Applied Cryptography and Network Security (ACNS) 2022
- 25th Information Security Conference (ISC) 2022
- 17th ACM Symposium on Information, Computer, and Communications Security (ACM ASIACCS) 2022
- 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2022

Juniorprof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

PUBLIKATIONEN

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

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

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 – 03/2025

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

Tagung der GOR Arbeitsgruppe: Simulation und Optimierung komplexer Systeme, House of Logistics and Mobility, Frankfurt

WEITERE FUNKTIONEN

- Forschungsgruppenleiter „Data-driven Aviation Management", Munich Aerospace
- Arbeitsgruppenleiter „Simulation und Optimierung komplexer Systeme", Deutsche Gesellschaft für OR

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLIKATIONEN

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

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

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

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

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

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

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

FORSCHUNGSPROJEKTE

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

STELAR wird ein innovatives Knowledge Lake Management System entwerfen, entwickeln und evaluieren, um einen ganzheitlichen Ansatz für FAIR (Findable, Accessible, Interoperable, Reusable) und KI-fähige (qualitativ hochwertige, zuverlässig beschriftete) Daten für den Agrifood Bereich zu unterstützen und zu erleichtern.

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

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

Das Ziel ist ein Rahmenwerk für die lernende 5-Achsen-Kompensation von Formfehlern in Fräsprozessen, basierend auf einer prozessparallelen Abtragssimulation und AI/ML. Außerdem soll die Fähigkeit des Wissenstransfers zwischen verschiedenen Werkstückgeometrien, Fräswerkzeugen und Werkzeugmaschinen für eine verbesserte Prozessplanung untersucht werden.

Gefördert durch: DFG
Laufzeit: 04/2021 – 12/ 2023

ITN NoBIAS – Artificial Intelligence Without Bias

Ziel ist die Erforschung und Entwicklung von Methoden für die KI-gestützte Entscheidungsfindung ohne Vorurteile. 15 Forscher sind darin geschult, voreingenommene und diskriminierende KI-Entscheidungen zu erkennen und Lösungen anzubieten, die die KI voll ausschöpfen und gleichzeitig die Einhaltung ethischer Grundsätze gewährleisten.

Gefördert durch: EU
Laufzeit: 01/2020 – 12/2024
Teilnahme über Forschungszentrum L3S, Hannover

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

Eine Gruppe von technischen Experten, Philosophen und Rechtsexperten, die sich mit der gemeinsamen Frage befasst: Wie können die Standards für unvoreingenommene Einstellungen und nichtdiskriminierende Praktiken bei der Big-Data-Analyse und algorithmengestützten Entscheidungsfindung erfüllt werden?

Gefördert durch: Volkswagen Stiftung
Laufzeit: 12/2018 – 05/2023
Teilnahme über Forschungszentrum L3S, Hannover

Prof. Dr. Stefan Pickl

Operations Research – Forschungsgruppe COMTESSA

LEHRE

10245	**Praktikum Operations Research - Entscheidungsunterstützung (WT + FT + HT)**
10252	**Seminar BINF+BWIN (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 (WT + FT + HT)**
12326	**Seminar Ausgewählte Kapitel des Operations Research (FT)**
2038-V1	**KI und datenbasierte Optimierung (FT)**
3481-V1	**Datenwissenschaft und -analyse (FT)**

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

MESSEN, TAGUNGEN, SEMINARE

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

WEITERE FUNKTIONEN

- Vize-Präsident Deutsches Komitee Katastrophenvorsorge DKKV
- Beiratsvorsitzender der Deutschen OR Gesellschaft
- Mitglied DEU NATO SAS Panel

Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

FORSCHUNGSPROJEKTE

MiKscHA – Mikrokernel für statische und cloudbasierte Hochsicherheits-Anwendungen

Im Projekt werden State-of-the-Art-Methoden evaluiert für den hochsicheren Betrieb von mikrokernbasierten 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 (WT)**

5505 **Betriebssystemsicherheit (FT)**

Prof. Dr. Arno Wacker

Datenschutz und Compliance

LEHRE

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

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

55041 **Datenschutz (WT)**

55042 **Privacy Enhancing Technologies (FT)**

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

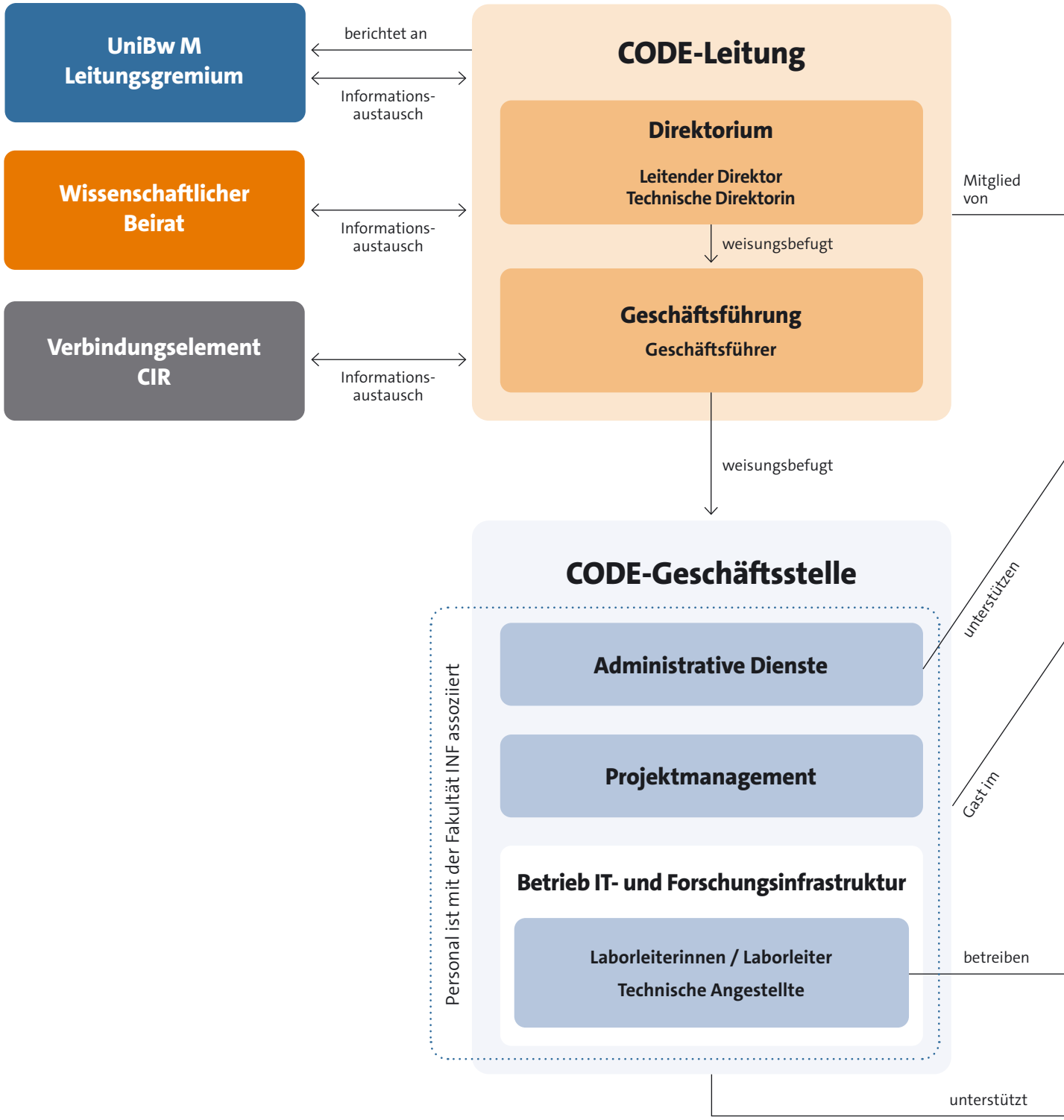
55091 **Penetration Testing (HT)**

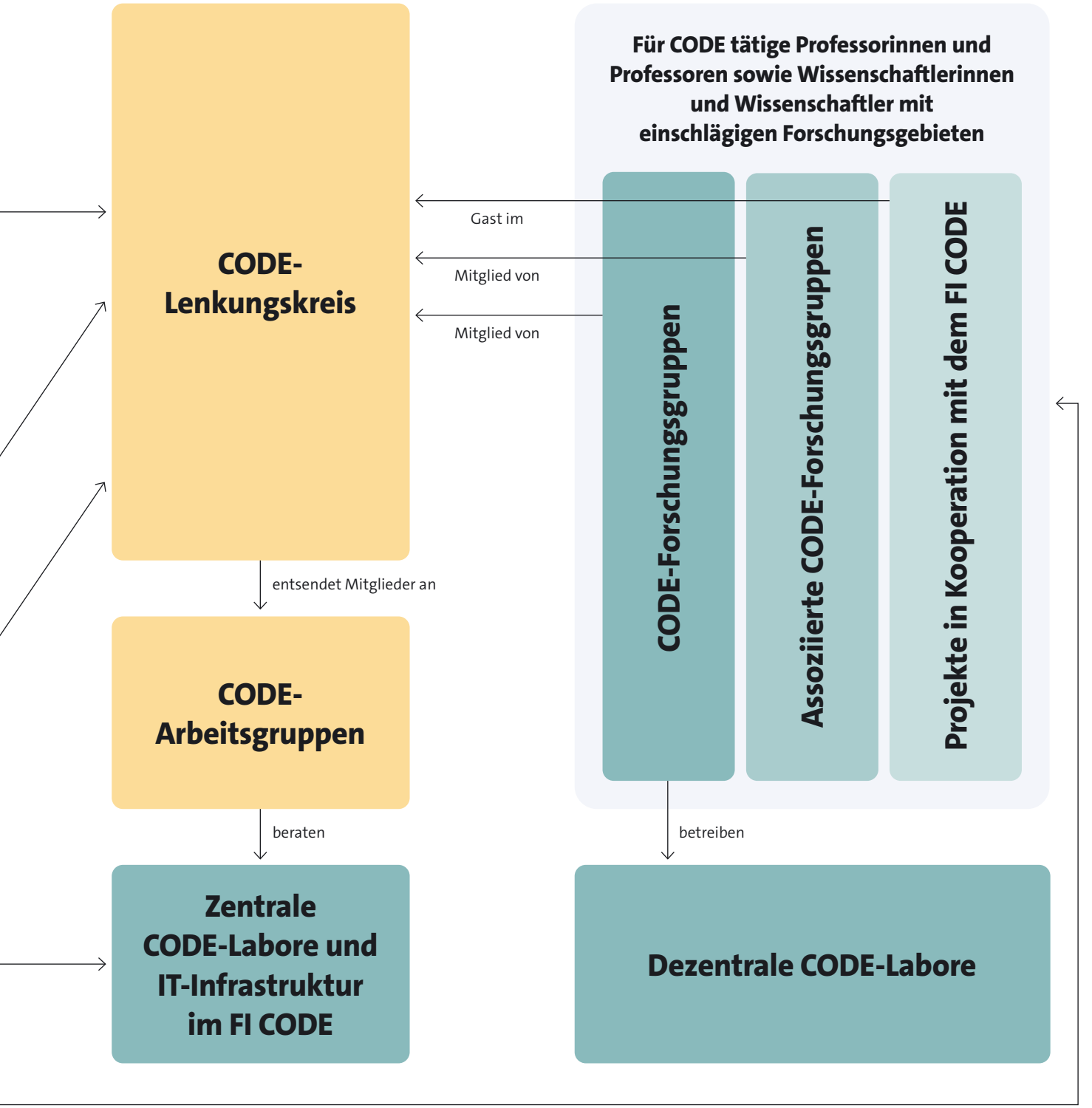
55093 **Praktikum Penetration Testing (WT + FT)**

WEITERE VERANSTALTUNGEN

- 01.03.2022 – You're being watched – Tricks und Tools der Hacker
  - Schülerinnen und Schüler des Anton-Bruckner-Gymnasiums Straubing und des Max-Mannheimer-Gymnasiums Grafing berichten über aktuelle Forschungsprojekte an der Universität der Bundeswehr München
- 05.10.2022 – Data-at-Rest – Also at Risk?
  - Vortrag am Gymnasium Ulricianum Aurich im Rahmen des IT Security Day 2022, Kassel
- 06.10.2022 – Data-at-Rest – Also at Risk?
  - Vortrag am Gymnasium Ottobrunn, München

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 7301 oder 7306
www.unibw.de/code

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

Lageplan

Impressum

HERAUSGEBER

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.,
Kommissarischer 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 Software-Entwicklung

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

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

Prof. Dr. Michaela Geierhos,
Professorin für Data Science

Prof. Dr. Udo Helmbrecht,
Honorarprofessor am FI CODE

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

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

Prof. Dr. Johannes Kinder,
Professor für Härtung von IT-Systemen

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. Oliver Rose,
Dekan der Fakultät für Informatik an der UniBw M,
Professor für Modellbildung und Simulation

Prof. Dr. Gunnar Teege,
Professor für Verteilte Systeme

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

MITGLIEDER DES BEIRATS (IM JAHR 2022)

Aus der Fakultät für Informatik der
Universität der Bundeswehr München

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Weitere Mitglieder

Prof. Dr. Johann Pongratz,
TU Dortmund

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

Dr. Norbert Gaus,
Executive Vice President der Siemens AG

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

REDAKTION

Benjamin Bellgrau, M. Sc.,
Kommissarischer Referent für Öffentlichkeitsarbeit

ART DIRECTION

Tausendblauwerk, Agentur für Gestaltung
Michael Berwanger

www.tausendblauwerk.de

LEKTORAT

Dr. Michelle Ruth Büscher,
Fachübersetzerin/Lektorin

DRUCK

Holzer Druck und Medien

www.druckerei-holzer.de

REGULARIEN

Redaktionsschluss: März 2023

Titelabbildung: Adobe Stock / KanawatTH

ISBN: 978-3-943207-70-5 | ISSN: 2748-8780

Auch erschienen als elektronische Publikation
(ISBN: 978-3-943207-71-2 | ISSN: 2748-8799)
sowie in englischer Sprache
(ISBN: 978-3-943207-72-9 | ISSN: 2748-9485).


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