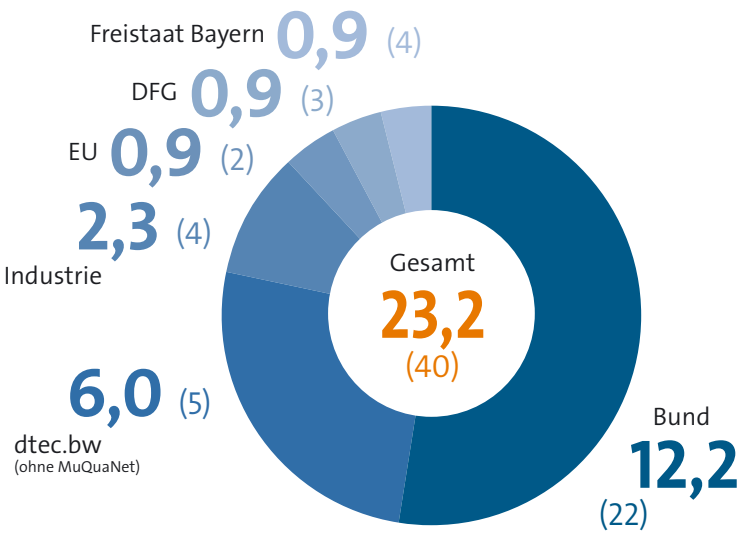

der Bundeswehr
Universität München
CODE
JAHRESBERICHT
2021
FI
CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Projektförderung

2021 wurden insgesamt 40 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

Beteiligte Professuren

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 2021 aus 15 Ländern.

Kooperationspartner***

Im Jahr 2021 arbeitete das FI CODE mit 70 Partnern in 25 Ländern zusammen.

Legende

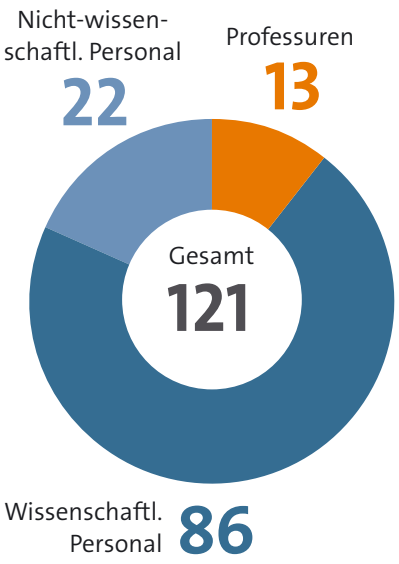
- Standort FI CODE
- 1 — Anzahl von CODE-Mitarbeitenden aus den Herkunftsländern
- 1 — Anzahl internationaler Kooperationspartner im betreffenden Land
- Länder mit Kooperationspartnern und Mitarbeitenden

*** Weitere Informationen zu Kontakten und Kooperationspartnern finden Sie ab S. 66.

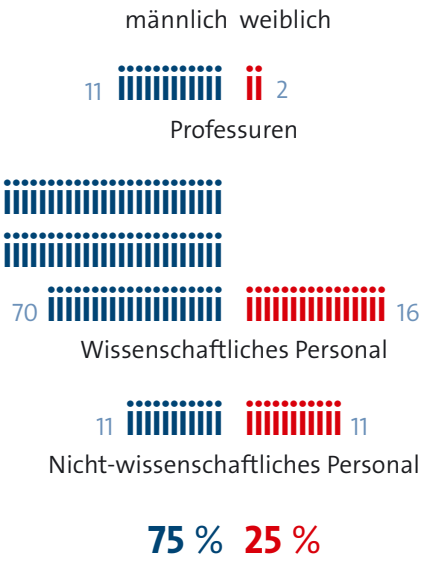
Personalstruktur

Das FI CODE hatte 2021 insgesamt 121 Mitarbeitende. Der Frauenanteil betrug 25 %.

Mitarbeitende



Geschlechteranteil

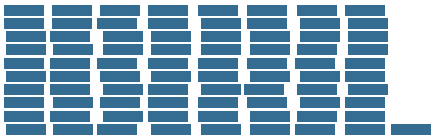


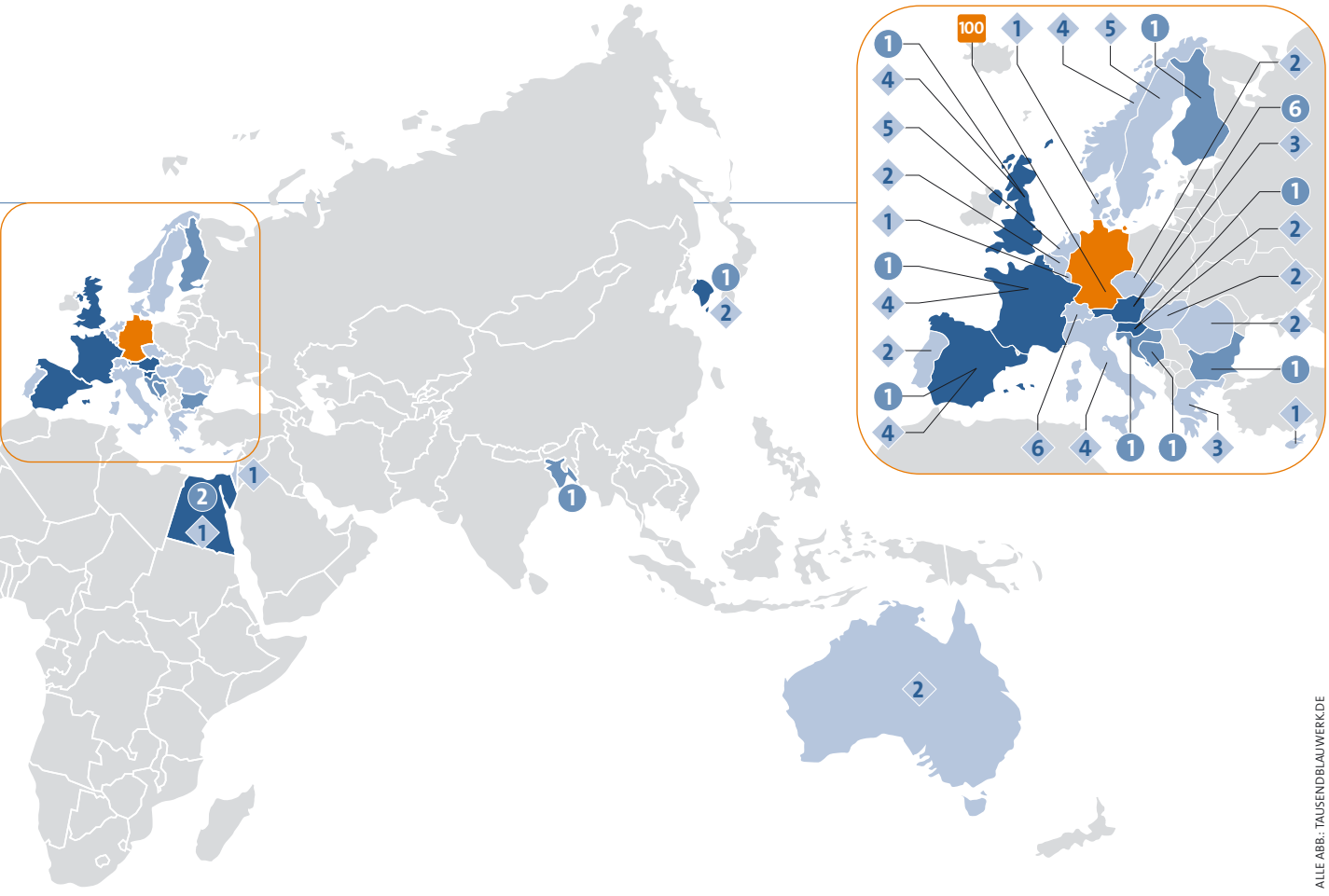
Forschungsarbeit

Übersicht der Promotionen und Publikationen am FI CODE 2021

Promotionen

Publikationen





ALLE ABB.: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
JAHRESBERICHT
2021

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Vorwort der Präsidentin

Die weltweiten Krisen nehmen zu und damit auch die Bedrohungen für unsere freie, demokratische Gesellschaft. Die COVID-19-Pandemie ist noch nicht vorüber, da hält uns der militärische Konflikt zwischen Russland und der Ukraine in Atem, für den Wladimir Putin verantwortlich ist. Es gibt wieder einen Krieg mit viel Leid und Zerstörung in Europa, was nach dem Fall des Eisernen Vorhangs unvorstellbar schien. Die gefährlichen politischen Entwicklungen führen uns einmal mehr vor Augen, wie groß der Bedarf an wissenschaftlich fundierten Erkenntnissen ist.

Die Universität der Bundeswehr München konzentriert sich mit ihren Forschungszentren dezidiert auf Themen der Sicherheit und Krisenbewältigung. Dabei geht es sowohl um technische Aspekte, wie etwa die Problematik der digitalen Angriffe auf Computersysteme, als auch um den gesellschaftlichen Umgang mit den neuen Herausforderungen. Unser Forschungsinstitut CODE (FI CODE) für Cyber Defence und Smart Data liegt thematisch mitten im Fokus dieser universitären Schwerpunkte und kann seit seiner Gründung als Forschungszentrum im Jahr 2013 auf eine erfolgreiche Entwicklung zurückblicken, die zuletzt zu einer Profilschärfung in Richtung der Bedarfe des Bundesministeriums der Verteidigung (BMVg) und der Bundeswehr geführt hat.

Global wächst die Zahl der Cyberangriffe, unter anderem auf Softwaresysteme, die für die Versorgung mit Lebensmitteln und anderen essenziellen Rohstoffen eingesetzt werden. Zudem häufen sich Desinformationskampagnen und das systematische Verbreiten von Fake News, was schlimmstenfalls zur Destabilisierung ganzer staatlicher Systeme führen kann. Um diesen Herausforderungen zu begegnen, sind Bundeswehr und Gesellschaft auf wissenschaftlich ausgebildete, gut geschulte Fachkräfte und innovative Forschungsergebnisse angewiesen. Das FI CODE als eines der führenden Forschungsinstitute bietet hier sowohl grundlagen- als auch anwendungsorientierte universitäre Forschung in den Bereichen Cybersicherheit, Smart Data/KI und Quantentechnologie.

Es freut mich daher außerordentlich, dass das Institut weiter auf Wachstumskurs ist: Im Jahr 2021 wurden in den teils noch sehr jungen Forschungsgruppen mehr als ein Dutzend Projekte an den Start gebracht und über 80 Publikationen verfasst. Die Zahl der Mitarbeitenden ist auf 121 gestiegen.

Im Jahr 2021 gab es am FI CODE einen Wechsel an der Spitze: Wolfgang Hommel, bis Oktober 2021 Technischer Direktor, übernahm das Amt des Leitenden Direktors und folgte Gabi Dreo Rodosek nach, die sich nach acht Jahren neuen Forschungsschwerpunkten widmen wird. Neue Technische Direktorin ist Michaela Geierhos. Dem neuen Direktorium wünsche ich viel Erfolg und alles Gute für die vielversprechende Zukunft des Instituts!

Die hervorragende Zusammenarbeit mit dem BMVg zeigt sich auch am Wechsel des bisherigen Geschäftsführers von CODE ins Referat CIT I 2, wo Volker Eiseler die Weiterentwicklung des FI CODE und des Cyber-Clusters an der Universität der Bundeswehr München aus ministerieller Perspektive koordinieren wird.

Gerne empfehle ich Ihnen die informative Lektüre des vorliegenden Jahresberichts und verbleibe mit besten Grüßen und Wünschen

Prof. Dr. Merith Niehuss
Präsidentin Universität der Bundeswehr München

Marcus Knüpfer, Michaela Geierhos, Wolfgang Hommel

Liebe Leserinnen und Leser,

nichts ist so beständig wie der Wandel. Im vergangenen Jahr prägten CODE zahlreiche Neuerungen und einige personelle Veränderungen. Mit dem vorliegenden Jahresbericht möchten wir Ihnen einen Überblick über die Aktivitäten unserer Forschungsgruppen und über unsere Jahreshighlights geben.

Besonders freut es uns, dass sich der stetige Aufwuchs von CODE im Jahr 2021 fortsetzte. An den CODE-Professuren wurden zahlreiche Qualifikationsstellen für den wissenschaftlichen Nachwuchs in mehr als einem Dutzend neuer Forschungsvorhaben geschaffen – überwiegend mit Partnern aus der Bundeswehr, Bundesbehörden und dem Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw). Hinzu kamen weitere Kooperationsprojekte der Kollegen Prof. Dr.-Ing. Helmut Mayer und Prof. Dr. Stefan Pickl. Unter wissenschaftlicher Leitung von Dr. Sabine Tornow wird seit April 2021 unsere neue Forschungssäule im Bereich Quantentechnologien kontinuierlich ausgebaut. Mehr über die technischen Grundlagen des Quantencomputings und unsere neuesten Aktivitäten in diesem Bereich erfahren Sie im Kapitel „Highlights“.

Ein Highlight im Jahr 2021 war auch die CODE-Jahrestagung, diesmal zum Thema „Supply Chain Sovereignty“. Hunderte Gäste wählten sich virtuell zu der dreitägigen Veranstaltung ein, um hochkarätig besetzten Paneldiskussionen zu folgen, an Workshops teilzunehmen oder Pitches zu innovativen Ideen im Bereich Cyber/IT zu lauschen. Im Herbst waren Teilnehmende aus sieben Nationen zu Gast am FI CODE, um bei der „Multi-Lateral Cyber Defense Exercise“ gemeinsam für die Cybersicherheit zu üben. Am jährlichen „Capture the Flag“-Event des FI CODE, das zum ersten Mal erfolgreich hybrid stattfand, beteiligten sich 14 Teams vor Ort und 15 im Online-Wettbewerb.

Die Koordination virtueller und hybrider Veranstaltungen und vielfach im Homeoffice durchgeführter Forschung erweist sich trotz zunehmender Routine als aufwendiger Kraftakt. Wir danken deshalb allen Mitgliedern der CODE-Geschäftsstelle und den Kolleginnen und Kollegen, die sich mit ihren Forschungsgruppen für den gemeinsamen Erfolg von CODE engagieren. Besonderer Dank gilt auch dem Abteilungsleiter CIT, Generalleutnant Vetter, dem Inspekteur CIR, Vizeadmiral Dr. Daum, unseren direkten Ansprechpersonen im BMVg und in der Leitung der Universität der Bundeswehr München für den großen Rückhalt im vergangenen Jahr.

Als neue CODE-Leitung – zu der auch Marcus Knüpfer als kommissarischer Geschäftsführer gehört – bedanken wir uns für das in uns gesetzte Vertrauen, welches wir künftig mit der erfolgreichen, gemeinsamen Weiterentwicklung des FI CODE bestätigen möchten und wünschen viel Freude und spannende Impulse bei der Lektüre des Jahresberichts 2021!

ABB.: PRIVAT; FI CODE

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Leitung des Forschungsinstituts CODE

Inhalt

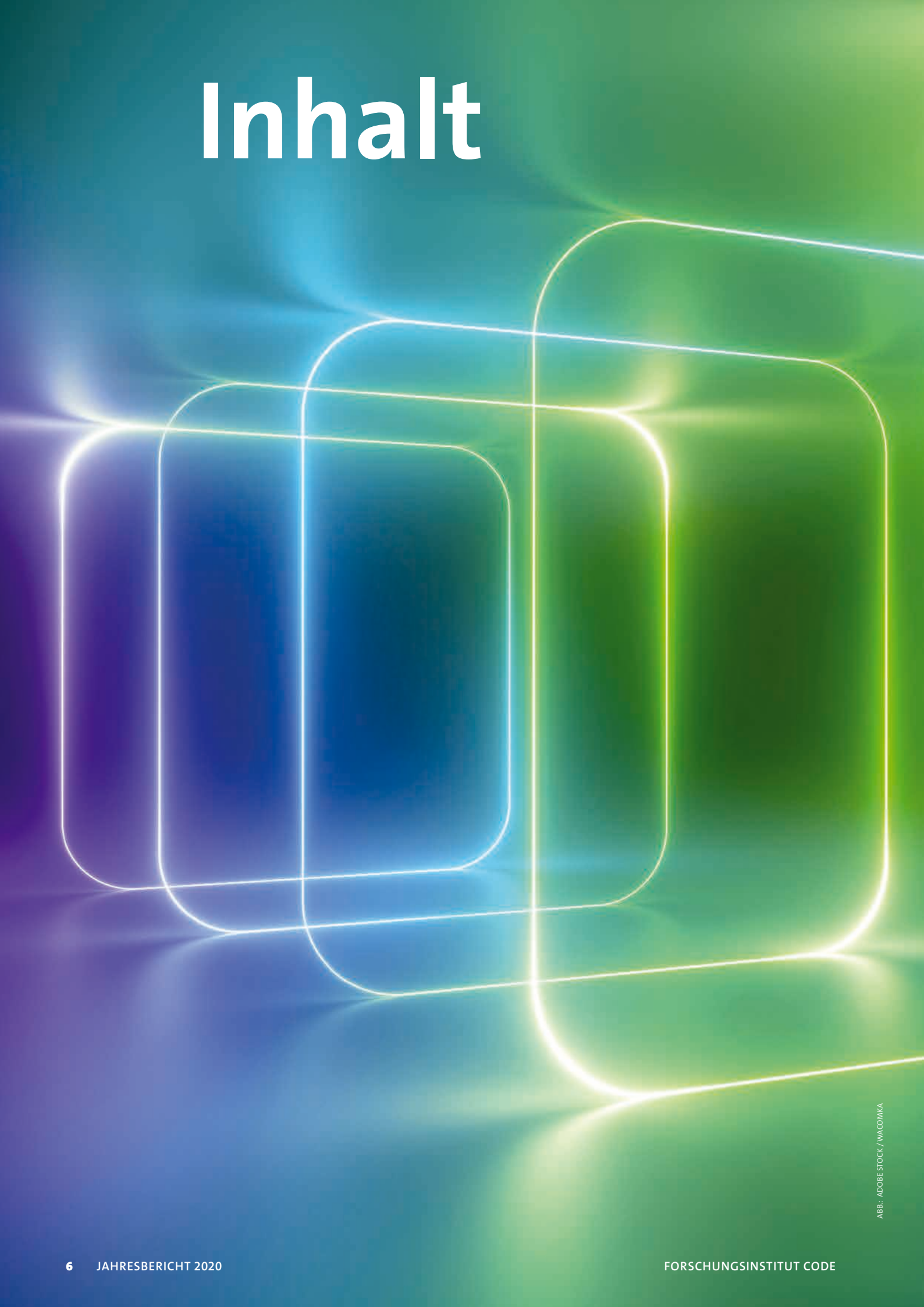


ABB.: ADOBE STOCK / WACOMKA

Highlights
Aus dem Institut

Forschung
Porträts und Projekte

Weitere Projekte

Kooperationen
Deutschland und die Welt

Nachwuchsförderung
Chancen und Angebote

Addendum
Publikationen und Aktivitäten

Organigramm

Rubriken

UNSER LEITBILD

MISSION

Unser Ziel ist es, technische Innovationen und Konzepte zum Schutz von Daten, Software und Systemen ganzheitlich und interdisziplinär zu erforschen und zu entwickeln.

FORSCHUNG

Wir betreiben Grundlagen- sowie anwendungsnahe Forschung und Technologie-Entwicklung in den Themenfeldern Cyber Defence, Smart Data und Quantum Technology zum Nutzen der Gesellschaft und der Bundeswehr.

WERTE

Unser Selbstverständnis ist geprägt von Zusammenhalt, Wertschätzung für das Individuum, einer echten Diskussionskultur und Loyalität.

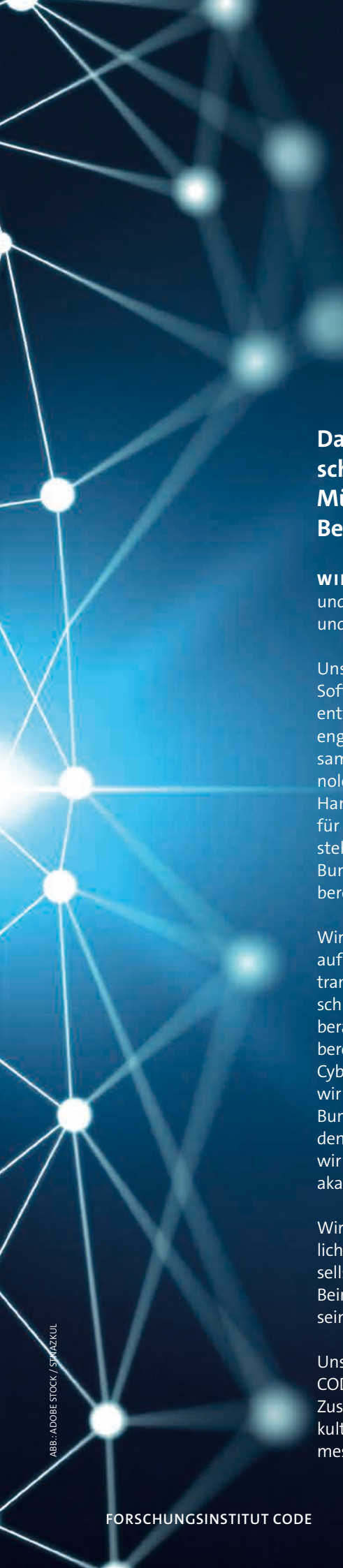


ABB.: ADOBE STOCK / SIMAZKUL

Das Forschungsinstitut CODE ist eine zentrale wissenschaftliche Einrichtung der Universität der Bundeswehr München und schafft mit seiner Expertise Innovation im Bereich Cyber/IT für die Bundeswehr.

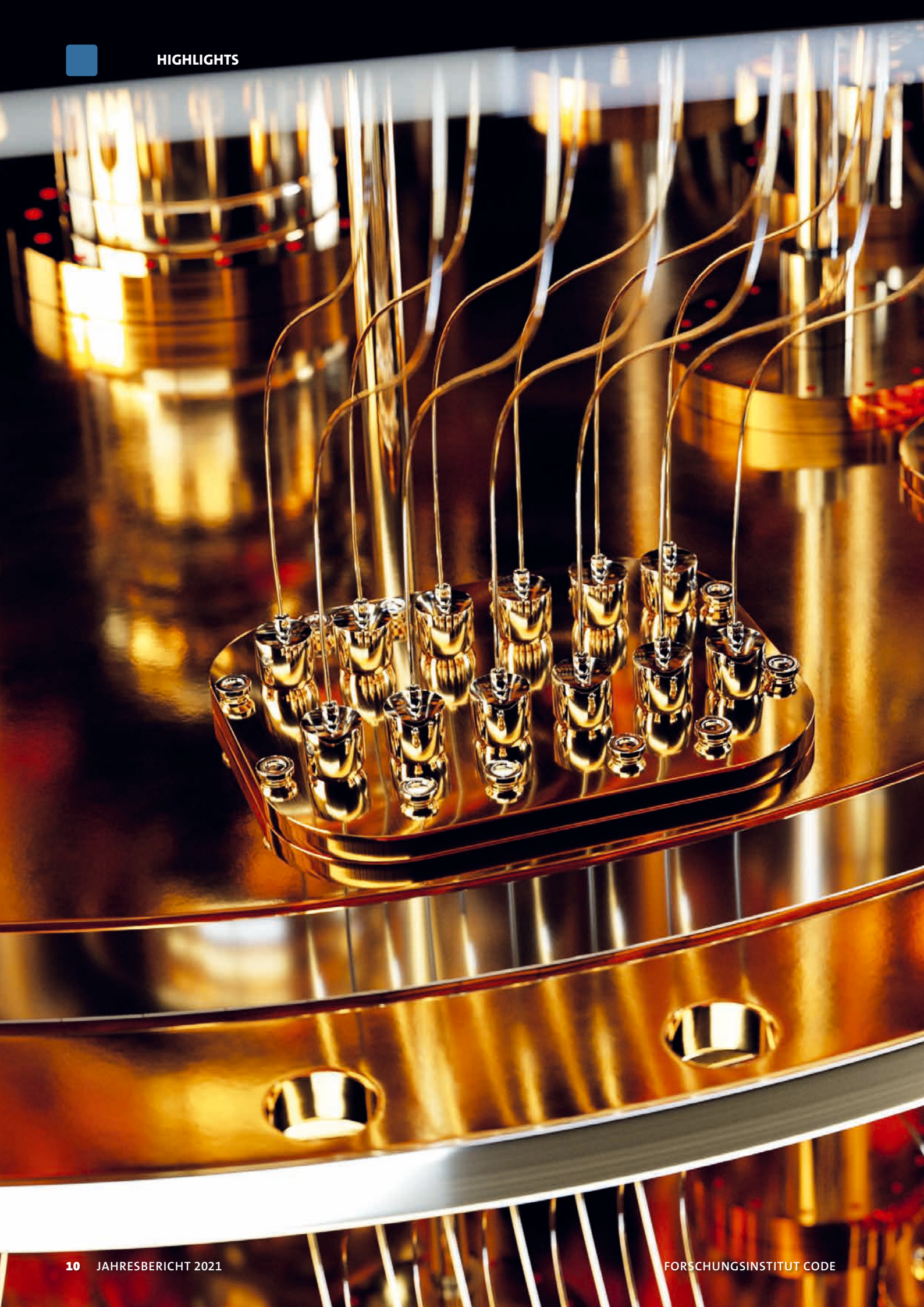
WIR BETREIBEN sowohl Grundlagen- als auch anwendungsnahe Forschung und Technologie-Entwicklung in den Themenfeldern Cyber Defence, Smart Data und Quantum Technology zum Nutzen der Gesellschaft und der Bundeswehr.

Unser Ziel ist es, technische Innovationen und Konzepte zum Schutz von Daten, Software und Systemen ganzheitlich und interdisziplinär zu erforschen und zu entwickeln. Hierzu bündeln wir wissenschaftliche Kompetenzen und arbeiten eng mit Partnern aus Bundeswehr, Behörden, Forschung und Wirtschaft zusammen. Wesentlich ist hierbei der Transfer von Ergebnissen und neuen Technologien in die Praxis, sodass diese wertschöpfend bzw. einsatzbereit für die Handlungsfelder unserer Partner sind. Darüber hinaus möchten wir Akzeptanz für datenschutzkonforme und sichere Technologien von morgen schaffen und stehen nicht nur in der Lehre, in der wir Studierende an der Universität der Bundeswehr München auf die IT-Herausforderungen ihres Berufslebens vorbereiten, zu unserer Vorbildfunktion.

Wir wollen Deutschland ein Stück sicherer machen. Hierfür forschen wir, pflegen auf Dauer ausgelegte Kooperationen und stimulieren Vernetzung und Wissenstransfer. Mit den breit gefächerten Kompetenzen unserer Professuren und Forschungsgruppen stehen wir Entscheidungsträgern aus Bundeswehr und Politik beratend zur Seite. Der direkte Zugang zu Quantencomputern ermöglicht uns bereits heute, Lösungen für die Herausforderungen von morgen zu finden. Unsere Cyber Range und die Lehrinfrastruktur genügen den neuesten Standards, womit wir unserem satzungsgemäßen Auftrag der Weiterbildungsangebote für die Bundeswehr nachkommen. Nicht nur in diesem Zusammenhang ist unser akademischer Nachwuchs unser wertvollstes Kapital. Gemeinsam mit ihm gestalten wir die Zukunft und treiben Innovationen voran. Darum ist uns die individuelle akademische Weiterqualifizierung am FI CODE ein großes Anliegen.

Wir sind offen für den wissenschaftlichen Diskurs und betreiben aktiv Öffentlichkeitsarbeit. Dabei sind wir uns unserer Verantwortung gegenüber der Gesellschaft und der Bundesrepublik Deutschland bewusst. Der wissenschaftliche Beirat mit seiner breiten fachlichen Expertise unterstützt das FI CODE aktiv bei seiner strategischen Weiterentwicklung.

Unsere Organisationsstruktur ist auf Kooperation ausgelegt. Dabei bildet das FI CODE keine bloße Arbeitsgemeinschaft: Unser Selbstverständnis ist geprägt von Zusammenhalt, Wertschätzung für das Individuum, einer echten Diskussionskultur und Loyalität. Wir geben jeden Tag unser Bestes und sind bereit, uns daran messen zu lassen. ■



Highlights

Aus dem Institut

ABB.: ADOBE STOCK / BARTEK WROBLEWSKI

Die Teilnehmenden der mehrtägigen Übung kamen aus sieben Nationen.

Multi-Lateral Cyber Defense Exercise am FI CODE

Trainieren für die Cybersicherheit

24 Teilnehmende, sieben Nationen, sechs Teams und fünf Tage: Das sind die Eckdaten der Multi-Lateral Cyber Defense Exercise (MLCD), die vom 4. bis 8. Oktober 2021 vom Kommando Cyber- und Informationsraum (CIR) der Bundeswehr am Forschungsinstitut CODE durchgeführt wurde. Die MLCD ist eine defensiv ausgerichtete internationale Übung im Bereich der Cybersicherheit, die Wissensaustausch und Zusammenarbeit fördert. Im Jahr 2021 fand sie zum zweiten Mal statt.

Teamwork in der Cyber Range

Die Cyber Range „ICE & T“ des FI CODE bot ein ideales Umfeld für die internationale Veranstaltung: In den technisch bestens ausgestatteten Räumlichkeiten gab es für die Beteiligten Gelegenheit, sich auszutauschen und gemeinsam Lösungsansätze für die komplexen Cybersicherheitsszenarien zu entwickeln. Eine Besonderheit der MLCD-Übung: Die nationalen Delegationen wurden dem kooperativen Charakter der Übung entsprechend untereinander gemischt. Die Idee der Kooperation spiegelte sich auch im Verzicht auf eine Punktewertung sowie in einer gemeinsamen Nachbesprechung zu den einzelnen Szenarien in Form einer offenen Diskussion wider. So konnten die Teilnehmenden unterschiedliche Herangehensweisen und Techniken zur Bewältigung der Aufgaben kennenlernen.

Individualisierter Ansatz und persönliche Betreuung

Bereits im Vorfeld entwickelte das Trainerteam die Szenarien, passte diese den Bedürfnissen der Teilnehmenden an und evaluierte verschiedene Möglichkeiten der Auswertung und Nachbesprechung. Während der Veranstaltung übernahmen die Trainer die morgendlichen Briefings zur Einführung, steuerten die Szenarien, um einen größtmöglichen Lerneffekt zu generieren, förderten die Teamarbeit und gaben den Teilnehmenden Denkanstöße. Beim täglichen „Debriefing“, also der Nachbesprechung, wurden die gewonnenen Erkenntnisse in einem Lehrgespräch mit allen Teams gesammelt, eine mögliche Lösung sowie die Angriffsvektoren vorgestellt und gemeinsam geeignete Maßnahmen zur Abwehr entwickelt. Die Evaluation der Übung trug dazu bei, Szenarien, technische Infrastruktur sowie den didaktischen Ansatz weiterzuentwickeln und zu verbessern.

Malware, Phishing, Ransomware: vielfältige Szenarien

Die während der Übung trainierten Szenarien zielten auf Erkennung, Analyse und Mitigation (Abwehr) der simulierten Cyberangriffe ab. Alle fünf basierten auf realen Vorfällen oder waren an diese angelehnt. Dabei umfassten sie komplette Abläufe vom initialen Angriff über die Exfiltration von Daten bis zum Verwischen von Spuren. Das Szenario „Hi Jack!“ beispielsweise hatte einen Cyberangriff auf ein Online-Banking-Portal zum Inhalt, bei dem Teile des internen Netzes mithilfe einer Malware übernommen und Zugangsdaten entwendet wurden. Bei der Aufgabe „Dirty Dancing“ gelangte ein manipuliertes Word-Dokument auf ein ungesichertes Dateiablagesystem, was die Verschlüsselung der Daten

ABB.: UNIBW M / SIEBOLD

Der Inspekteur CIR, Vizeadmiral Dr. Thomas Daum, informierte sich persönlich über Ablauf und Inhalte der Übung.

durch die bekannte WannaCry-Ransomware samt einer Lösegeldforderung verursachte. „The Whole Nine Yards" stellte das komplexeste Szenario der Übung dar: Hier wurde die Kompromittierung eines Smartphones zum initialen Erlangen von Zugangsdaten mittels einer Phishing-E-Mail simuliert. Eine Vielzahl von weiteren Angriffsvektoren führte in diesem Szenario letztlich zum Diebstahl sensibler Unternehmensdaten.

Alle Cyberangriffe liefen teilautomatisiert ab und jedes der sechs Teams, die gemeinsam an der Gefahrenabwehr arbeiteten, wurde parallel in die gleiche Lage versetzt. Im Verlauf der Übung zeigte sich, dass die Gruppen die gestellten Aufgaben unterschiedlich angingen und auf ganz verschiedenen Wegen zum Erfolg gelangten.

Hochranginge Gäste aus ganz Europa

Insgesamt stieß die Übung mit ihrer internationalen Ausrichtung auf großes Interesse: Am zweiten Tag folgten hochranginge Militärvertreter aus Großbritannien, Frankreich, Polen, Luxemburg, Österreich, den Niederlanden, der Schweiz und Deutschland der Einladung des Inspekteurs Cyber- und Informationsraum (CIR), Vizeadmiral Dr. Thomas Daum, und besuchten das Forschungsinstitut CODE sowie den Campus der Universität der Bundeswehr München in Neubiberg. Während des Aufenthalts informierten sich Dr. Daum und die Gäste einerseits über Ablauf und Inhalte der MLCD, andererseits über die Ausrichtung der Cyber Range des FI CODE: Nicht nur im Rahmen der Übung ermöglicht ICE & T die Ausbildung und das Training von Cybersicherheitsexpertinnen und -experten. Die Studiengänge Informatik und Cyber-Sicherheit der Universität der Bundeswehr München beinhalten zum Beispiel verschiedene Praktika, die in der Cyber Range durchgeführt werden. Zudem dient ICE & T als Labor für wissenschaftliche Projekte mit verschiedenen technischen Fragestellungen, unter anderem im Rahmen des EU-Projekts CONCORDIA. ■

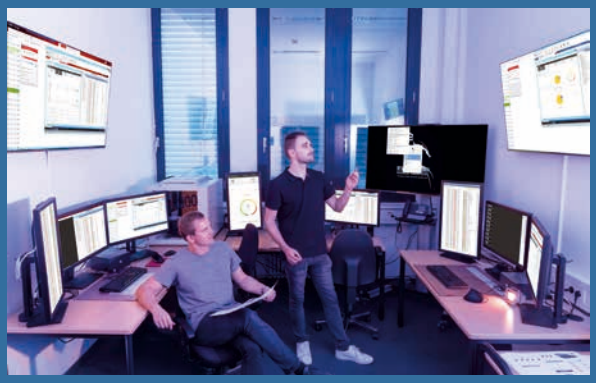
Mehr über die MLCD Exercise

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

Militärvertreter aus Großbritannien, Frankreich, Polen, Luxemburg, Österreich, den Niederlanden, der Schweiz und Deutschland.

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

ICE & T Cyber Range am FI CODE



Trainer analysieren die Übungen und greifen unterstützend ein.

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

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

ICE & T ist auf einem Server-Cluster unter Verwendung des VMware ESXi Hypervisors vollständig virtualisiert. Mehr als 400 virtuelle Maschinen werden eingesetzt, um mehrstufige Szenarien sowie über 80 individuelle Übungen und Backoffice-Dienste abzubilden. Die modulare Architektur ermöglicht außerdem die Integration physischer Hardwarekomponenten wie IoT und SCADA-Geräte.

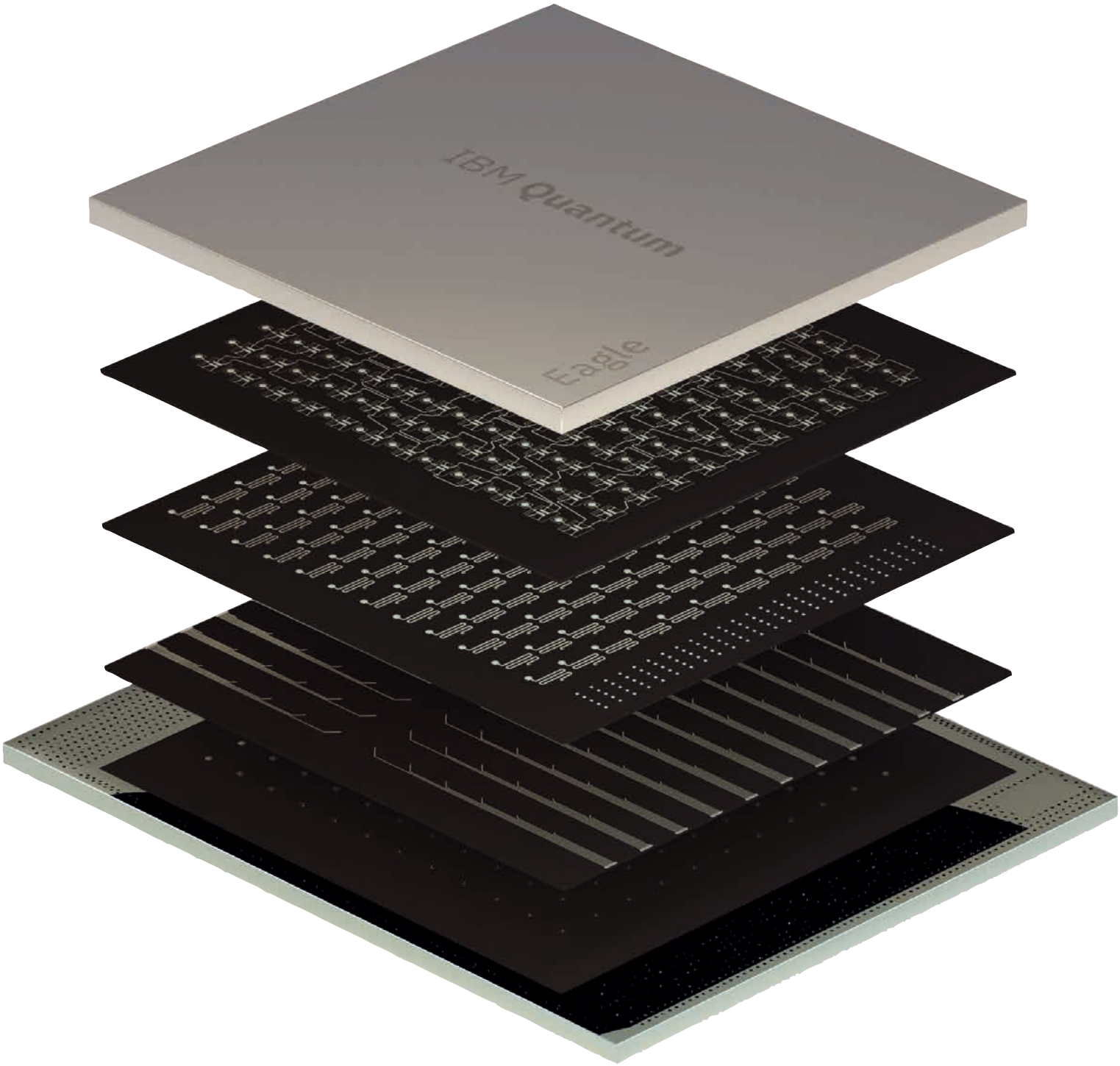
Weitere Informationen

ICE T
IT Competence Education & Training

code@unibw.de

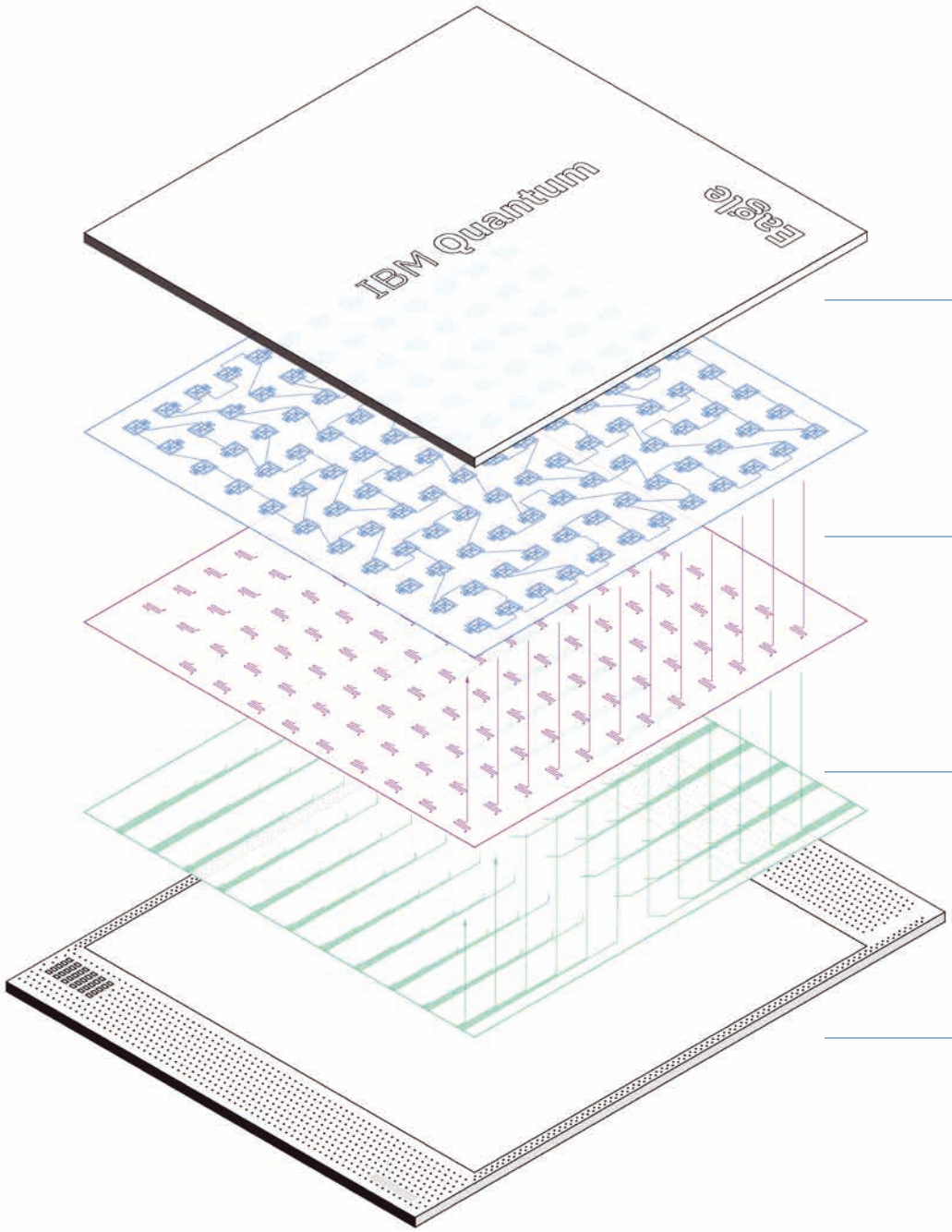
Informationsflyer „Cyber Range": https://go.unibw.de/84

ALLE ABB.: UNIBW M / SIEBOLD



Quantentechnologien

Auf dem Weg zur Praxisrelevanz des Quantencomputings



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

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

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

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

ABB.: CARL DE TORRES OF STORYTK FOR IBM

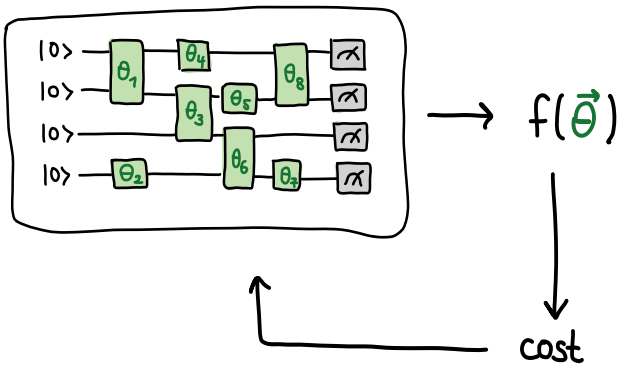
Die experimentelle Kontrolle von Quantensystemen macht es möglich, dass insbesondere durch Nutzung der Quanteneigenschaften Superposition und Verschränkung neue Quantentechnologien entwickelt werden können. Dies führt zu einer neuen Art der Navigation, Sensorik, Datenübertragung und Datenverarbeitung, die potenziell auch für die Bundeswehr von großer Relevanz sein kann.

DAS QUANTENCOMPUTING bildet im Prinzip das Rückgrat der Quantentechnologien: Daten aus Quantensensoren können verarbeitet und in Quantenspeichern kurz zwischengesichert werden. Quantencomputer lassen sich über Quantennetze in verteilten Systemen zusammenschließen und mit klassischen Computern verbinden. Obwohl sich die meisten dieser Technologien noch in einem sehr frühen Stadium befinden, ist es am Forschungsinstitut CODE möglich, sie zu erforschen. Das FI CODE der Universität der Bundeswehr München hat seit

IBM Q Computation Center.

2018 als IBM Quantum Hub einen von weltweit nur wenigen exklusiven Zugängen zur IBM-Quantencomputer-Infrastruktur. Die derzeitige Verfügbarkeit von kleinen, mit Rauschen behafteten Quantencomputern (bis 127 Qubits) ermöglicht es den Forscherinnen und Forschern am FI CODE, Quantenalgorithmen und -heuristiken sowie Fehlerminderungsschemata zu testen und Experimente zur Erforschung und Anwendung der Quanteninformationsverarbeitung auszuführen.

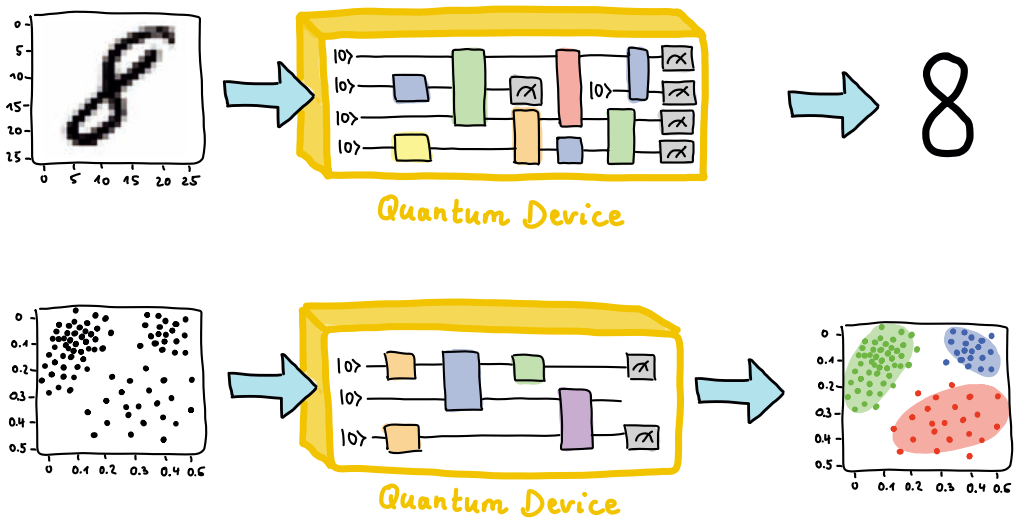
Man kann Quantencomputer mit Qiskit, einem Software-Entwicklungskit, auf der Ebene von Schaltkreisen, Pulsen und Algorithmen programmieren. Dabei ist zu beachten, dass bei der Programmierung von Quantenalgorithmen nicht einfach „Jobs“ abgesendet werden können. Hierfür muss etwas mehr Arbeit investiert werden, indem die Wissenschaftlerinnen und Wissenschaftler etwa Fehlerminderungstechniken und Transpileroptimierungen anwenden. Auf dem Weg zur Praxisrelevanz des Quantencomputings werden am FI CODE verschiedene Anwendungen in den Bereichen Optimierung, Machine Learning und Quantensimulation verfolgt und Methoden zur Schaltkreisoptimierung und Fehlerminderung entwickelt.



Visualisierung eines Quanten-Variationsalgorithmen-Schaltkreises.

Eine dieser wichtigen Anwendungen ist die **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 ist. Für viele dieser Probleme können nur Näherungslösungen mithilfe von Höchstleistungsrechnern gefunden werden.

Schon kleine Verbesserungen durch heuristische Quantenalgorithmen sind so von wirtschaftlichem Interesse. Quanten-Variationsalgorithmen ermöglichen einen lernbasierten Ansatz. Die Parameter des Schaltkreises werden durch Optimierung einer Kostenfunktion gefunden. Die Quanten-Variationsalgorithmen werden kontinuierlich in Theorie und experimenteller Umsetzung verbessert.

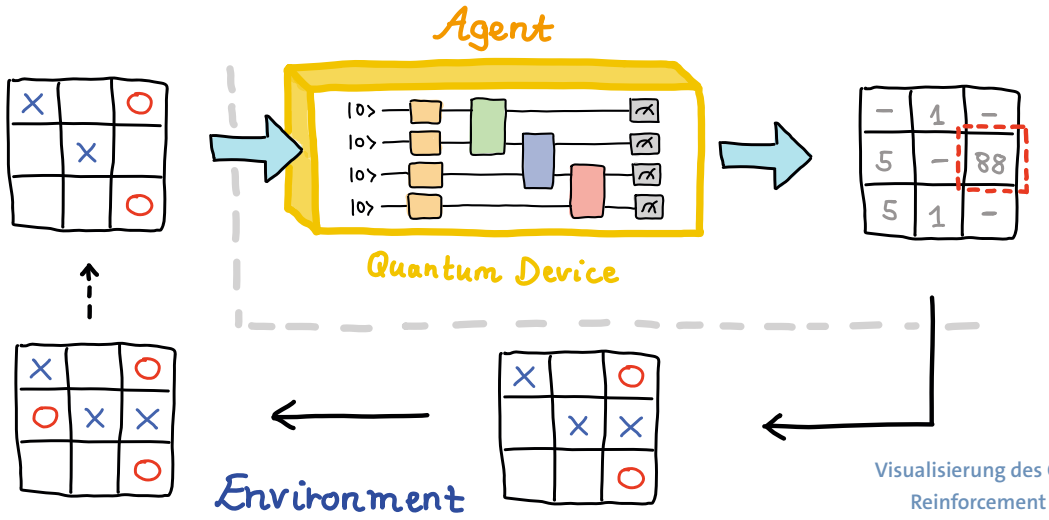


Visualisierung von Supervised and Unsupervised Quantum Machine Learning.

Mithilfe von Quantenvariationsalgorithmen können auch **Supervised** sowie **Unsupervised Quantum Machine Learning** realisiert werden. Dazu gehören konkret Quantum Clustering, Quantum Boltzmann Machines, Kernel Methods, Quantum Convolutional Neural Networks, Quantensupport-Vektormaschinen, Quanten-Autoencoder oder generative adversarische Quantennetze.

Generative adversarische Netze sind ein leistungsfähiges Werkzeug für das klassische Maschinelle Lernen: Ein sogenannter Generator versucht, Statistiken für Daten zu erzeugen, die denen eines echten Datensatzes ähneln, während ein Diskriminator versucht, zwischen echten und gefälschten Daten zu unterscheiden. Der Lernprozess für den Generator und den Diskriminator kann als sich widersprechendes Spiel betrachtet werden, und unter vernünftigen Annahmen nähert er sich bis zu dem Punkt an, an dem der Generator dieselben Statistiken wie die echten Daten erzeugt und der Diskriminator nicht in der Lage ist, zwischen echten und generierten Daten zu unterscheiden. In ähnlicher Weise funktionieren generative kontradiktorische Quantennetzwerke, bei denen die Daten entweder aus Quantenzuständen oder klassischen Daten bestehen und der Generator und der Diskriminator durch Quantenschaltungen dargestellt werden. Zu ihren Anwendungen gehört zum Beispiel die Detektion von Anomalien.

Reinforcement Learning, ein weiterer Hauptbereich des Maschinellen Lernens, beschäftigt sich mit der datenbasierten Optimierung von mehrstufigen Entscheidungsprozessen innerhalb eines gegebenen Systems, angewendet auf verschiedene Angreifer-Verteidiger-Szenarien. Ziel der Algorithmen ist es, eine Strategie zu identifizieren, die über mehrere Zeitschritte hinweg einen bestimmten Zustand des Systems erreicht. Das Besondere im Reinforcement Learning ist, dass der Algo-



Visualisierung des Quantum Reinforcement Learning.

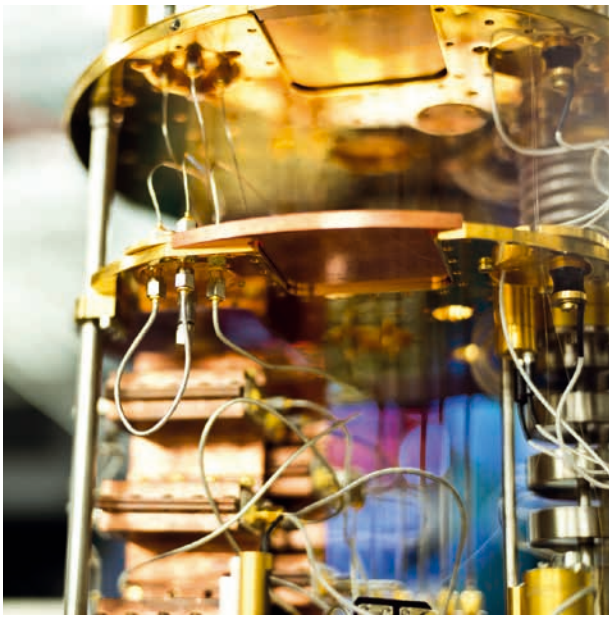
ABB.: IBM CORPORATION / CORINNE ZHOU; FI CODE (3)

rithmus keine Informationen über das System besitzt, mit dem er interagiert. Allein durch die Interaktion und eine Bewertung der ausgeführten Aktionen lernt der Algorithmus im Training, das Ziel zu erreichen.

Quantencomputing bietet durch die Konzepte der Superposition (s. Infobox „Quantencomputing“, S. 21) und der Verschränkung ein enormes Potenzial, die benötigte Rechenleistung im Reinforcement Learning zu reduzieren. Mithilfe von Policy-Gradient-basierten Reinforcement Learning-Ansätzen wurden Quantenhybrid-Algorithmen entwickelt, die die klassischen neuronalen Netze durch Quanten-Variationsschaltkreise ersetzen. Dadurch wird der rechenintensive Teil des Algorithmus auf den IBM-Quantencomputer ausgelagert. Die Ergebnisse zeigen einen enormen Vorteil des neuen Algorithmus in Bezug auf die notwendige Rechenleistung und dadurch ein schnelleres Training.

Ein universeller Quantencomputer kann ein Quantensystem nachbilden, indem er dessen natürliche Dynamik simuliert (**Quantensimulation**). 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.

Zur Erforschung der Quanteninformationsverarbeitung können verschiedene **Experimente auf einem supraleitenden Quantencomputer** durchgeführt werden,



IBM-Quantencomputer.

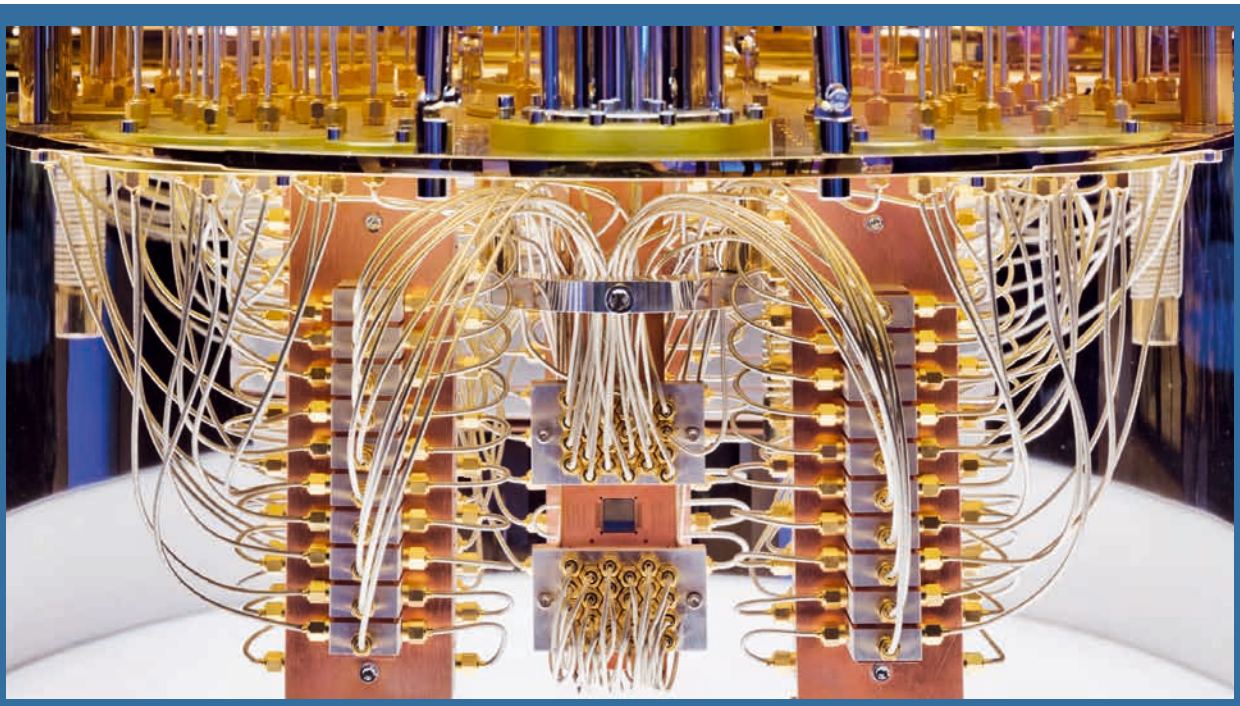
wie zum Beispiel Entanglement Measurement, Tomography, Quantum Optimal Control, Calibration oder Pulse Level Programming, Learning from Experiments oder Quantum Algorithmic Measurement. Außerdem können **Fehlerminderungstechniken** getestet werden, um die beim Ausführen von Quantencomputer-Algorithmen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

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.

Methodischen Aspekten des Quantencomputings wird mit Tensornetzwerkmethoden, für die entsprechende Simulatoren im IBM-Quantennetzwerk zur Verfügung stehen, und dem ZX-Kalkül, einer grafischen Sprache, mit der sich beliebige lineare Abbildungen zwischen Qubits darstellen lassen können, nachgegangen. Die ZX-Diagramme sind mit einem vollständigen Satz von grafischen Umschreibregeln ausgestattet, die eine diagrammatische statt einer gleichheitsorientierten Argumentation ermöglichen. Dieser Kalkül wurde erfolgreich zur Optimierung von Quantenschaltungen eingesetzt.

Die Themen aus der angewandten Forschung wurden mithilfe praxisorientierter **Lehrveranstaltungen** an Münchner Hochschulen und auf **Workshops** an Studierende und Mitarbeitende von bundeswehrnahen Dienstleistern weitergegeben und durch Vorträge auf Konferenzen und Seminaren vorgestellt. Zudem wurden Bachelor- und Masterarbeiten betreut. Zu den Themen Quantensensorik, Quantencomputing und Quantenkommunikation organisierten die Wissenschaftlerinnen und Wissenschaftler drei Online-Workshops. ■

BEIDE ABB.: IBM CORPORATION



Quantencomputing

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

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

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

Kontaktpersonen zum Quantencomputing am FI CODE

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

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

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

Bericht zur Jahrestagung „CODE 2021“

Sichere Lieferketten, digital souveränes Europa?

Vom 20. bis 22. Juli 2021 fand die Jahrestagung des Forschungsinstituts CODE unter dem Motto „Supply Chain Sovereignty: Reality or Illusion?“ pandemiebedingt in rein virtueller Form statt. Thema der CODE 2021 waren Lieferketten, die einerseits durch analoge Bedrohungen gefährdet sind, andererseits aber auch zunehmend im Fokus von Hackern stehen. Mehrere hundert Gäste wählten sich zu der dreitägigen Veranstaltung ein.

DIE CORONA-PANDEMIE hat gezeigt, wie wichtig Zusammenarbeit und digitale Prozesse in unserem Alltag geworden sind. Mehr denn je ist klar, dass wir die großen Herausforderungen in Europa nur gemeinsam bewältigen können. Von Bedeutung sind dabei auch internationale Lieferketten: Wird ein Partner kompromittiert, wirkt sich das auf alle Teile der Lieferkette aus. So können ganze Produktionslinien ausfallen oder Geschäftsbereiche, die von einer bestimmten Software abhängig sind, arbeitsunfähig werden. Beispiele sind der SolarWinds-Hack im Jahr 2020 oder die Angriffe auf die Software Kaseya, die im Sommer 2021 zu Lebensmittelengpässen in Schweden führten. Grund genug, das Thema „Supply Chain Sovereignty" in den Fokus der CODE-Jahrestagung 2021 mit renommierten Expertinnen und Experten aus Industrie, Forschung, Militär und Behörden zu stellen.

Die Begrüßung der Präsidentin der Universität der Bundeswehr München, Prof. Dr. Merith Niehuss, bildete den Auftakt zu der dreitägigen Veranstaltung. Prof. Dr. Gabi Dreo Rodosek hieß als Leitende Direktorin des FI CODE anschließend die Gäste herzlich willkommen und präsentierte in einem kurzen Vortrag die neuesten Entwicklungen am Institut. Thema war unter anderem der erstmals erschienene CODE-Jahresbericht, der auf rund 70 Seiten Highlights, Forschungsprojekte und weitere Aktivitäten des Instituts im Berichtsjahr 2020 darstellt.

Eröffnungsstatements und Impulse

Es folgten Eröffnungsstatements von Bundesverteidigungsministerin Annegret Kramp-Karrenbauer, der bayerischen Digitalministerin Judith Gerlach sowie Dr. Florian Herrmann, dem Leiter der Bayerischen Staatskanzlei. Verteidigungsministerin Kramp-Karrenbauer äußerte sich positiv über das Forschungsinstitut CODE: „Zu Recht gehört CODE zu den ersten Adressen in Europa, wenn es um Fragen der Cyberverteidigung geht. Mit groß angelegten Projekten wie CONCORDIA bringen Sie die Akteure der Cybersicherheit zusammen, bündeln IT-Kompetenz, fördern Innovation und stärken so Europas digitale Souveränität." Dr. Florian

ABB.: ADOBE STOCK / MAHA HEANG 245789; UNIBW M / SIEBOLD

Bundesverteidigungsministerin Annegret Kramp-Karrenbauer äußerte sich nach der Begrüßung durch Präsidentin Prof. Dr. Merith Niehuss (l.) und Prof. Dr. Gabi Dreo Rodosek in einem Videostatement.

Dr. Annegret Bendiek (l. o.) moderierte die Paneldiskussion mit Laura Carpini, StS Benedikt Zimmer und StS Dr. Markus Richter.

Herrmann betonte die Relevanz der CODE-Jahrestagung: „Dieses internationale Format zu Cybersicherheit und Digitalisierung zeigt deutlich, wo dringender Handlungsbedarf besteht."

Auf dem weiteren Programm des Vormittags standen Impulsvorträge unter anderem von Benedikt Zimmer, Staatssekretär im Bundesministerium der Verteidigung, sowie Dr. Markus Richter, Staatssekretär im Bundesinnenministerium und Beauftragter der Bundesregierung für Informationstechnik. Richter stellte neben weiteren Punkten die Wichtigkeit des Schutzes kritischer Infrastrukturen heraus: „Wir müssen unsere kritischen Infrastrukturen sichern, insbesondere die 5G-Netze. 5G schafft ein starkes industrielles Ökosystem im Bereich der Mobilfunknetze in Deutschland und Europa."

Debatten um funktionsfähige Lieferketten für Europa

In insgesamt drei hochkarätig besetzten Paneldiskussionen sprachen Gäste aus Forschung, Wirtschaft, Militär und Behörden im weiteren Verlauf des Tages unter anderem über folgende Fragen: Wie können Regierungen und Unternehmen den Sicherheitsrisiken in Lieferketten begegnen? Was sind die größten Hindernisse, die es zu beseitigen gilt? Wie lässt sich die Resilienz erhöhen?

Die Antworten der Panelisten nahmen immer wieder auf drei Punkte Bezug, die wichtige Voraussetzungen für funktionsfähige Lieferketten darstellen: die Bereitschaft zu Innovation und Flexibilität, die Notwendigkeit der Etablierung europäischer Standards oder Zertifikate für wichtige Bestandteile kritischer Infrastrukturen sowie die Zusammenarbeit auf internationaler Ebene, vor allem innerhalb Europas. Laura Carpini, Cybersecurity-Koordinatorin des italienischen Ministeriums für auswärtige Angelegenheiten und internationale Zusammenarbeit, sagte dazu: „Wir leben in einer vernetzten Welt – internationale Beziehungen sind ein Schlüssel. Sie können einen bedeutenden Unterschied machen. Gemeinsam sind wir stärker."

Workshop-Session und Innovationstagung

Als Technischer Direktor leitete Prof. Dr. Wolfgang Hommel den zweiten Tag der CODE-Jahrestagung: Im Rahmen von Workshops und der Innovationstagung wurden aktuelle Fragestellungen unter anderem zum Motto „Supply Chain Sovereignty" adressiert. Auf der parallel stattfindenden virtuellen Fachmesse konnten die Gäste wie schon am ersten Tag der „CODE" neue Entwicklungen im Bereich Cybersicherheit kennenlernen und mit Partnern aus der Industrie in Kontakt kommen. Daneben bot eine soziale

Plattform Gelegenheit für lockeren Austausch und Networking.

Im Vorfeld der Jahrestagung fand im Jahr 2021 erstmals ein „Call for Workshop Proposals“ statt. Zahlreiche Vertreter aus Instituten, Behörden und Wirtschaftsunternehmen folgten dem Aufruf und reichten Ideen zu technischen sowie politischen Aspekten von Cybersicherheit und Smart Data ein. Die Vorschläge waren vielfältig und behandelten Bereiche wie internationale Politik und Wirtschaft, Methoden künftiger Verteidigungspolitik, den Gesundheitssektor und Quantencomputing. Im Resultat war die Zahl der parallel stattfindenden Workshops besonders hoch: Insgesamt gab es 10 Workshops mit reger Teilnahme. Detailliertere Einblicke in zwei Angebote liefern die folgenden exemplarischen Beschreibungen.

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

Bio Cyber Security (BCS) ist ein relativ neuer Forschungsbereich, der darauf abzielt, digitalisierte Bio- und Gesundheitsdaten zu schützen. Ziel ist es dabei, Einzelpersonen, die Öffentlichkeit, die Infrastruktur des Gesundheitswesens sowie die Entwicklung biotechnologischer Innovationen zu sichern. Das exponentielle Wachstum bei der Digitalisierung von Biologie und Biotechnologie ist für eine Reihe von Sektoren in der Forschung und der Bioökonomie von Vorteil. Diese Fortschritte sollten jedoch auch Anlass zur Sorge über neue Risiken und Bedrohungen geben, die weder ausschließlich der Cyber- noch der „Biosicherheit“ zuzuordnen sind, sondern einen eigenen, hybriden Bereich darstellen. Daher beschäftigte sich dieser Workshop mit den folgenden Fragen: Wie muss ein BCS-Index gestaltet sein, damit er für technische, sicherheitstechnische und politische Zwecke nutzbar ist? Wo sollte der Schwerpunkt liegen, um Schwachstellen zu ermitteln, und wo können die Anstrengungen zur Bekämpfung von BCS-Bedrohungen gebündelt werden (zum Beispiel in der Gesundheitsinfrastruktur und Cybersicherheit)? Wie könnte ein umfassender interdisziplinärer Mechanismus der Zusammenarbeit von technischen, industriellen und politischen Fachleuten aussehen, um BCS-Bedrohungen über die nationale Sicherheit hinaus zu entschärfen und neue Paradigmen für die Informationsbeschaffung, Aufklärung und Analyse zu entwickeln? Abschließend kam man zu dem Konsens, dass BCS in Zukunft immer wichtiger wird und daher ein sehr hohes Entwicklungspotenzial zeigt.

Workshop „Security and Sovereignty of Cloud Systems“

Digitale Souveränität beschreibt die Fähigkeit einer Gemeinschaft, digitale Produkte und Dienste zu entwickeln, zu nutzen, zu betreiben und zu kontrollieren. Dazu gehört die Fähigkeit, den Einsatz vertrauenswürdiger Technologie (sowohl Hardware als auch Software, unter Berücksichtigung der gesamten Lieferkette), sichere Konnektivi-

BEIDE ABB.: FI CODE

Auf der virtuellen Fachmesse konnten die Gäste neue Entwicklungen im Bereich der Cybersicherheit kennenlernen und sich vernetzen.

tät, einen vertrauenswürdigen Betrieb der Infrastruktur und eine kontinuierliche Sicherheitsüberwachung zu gewährleisten. Was Cloud-Dienste betrifft, so akzeptieren Nutzerinnen und Nutzer offenbar weitgehend die Vorherrschaft außereuropäischer Anbieter (etwa Google oder Amazon). Einzelne Regierungen und europäische Schlüsselinitiativen haben zuletzt jedoch die Forderung nach nationaler Souveränität insbesondere im Hinblick auf ihre eigenen Cloud-Anwendungen erkannt, was zur GAIA-X[1]-Initiative für den Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa geführt hat. Darüber hinaus expandieren Cloud-Dienste weiter in den staatlichen („Bundescloud“) und auch in den militärischen Bereich, wo die Notwendigkeit, nationale Interessen zu schützen, noch dominanter wird. Die Teilnehmenden dieses Workshops diskutierten daher Strategien und Lösungen zur Gewährleistung von Sicherheit und Souveränität für Cloud-Systeme. Ein besonderer Fokus lag dabei auf dem staatlichen und militärischen Sektor.

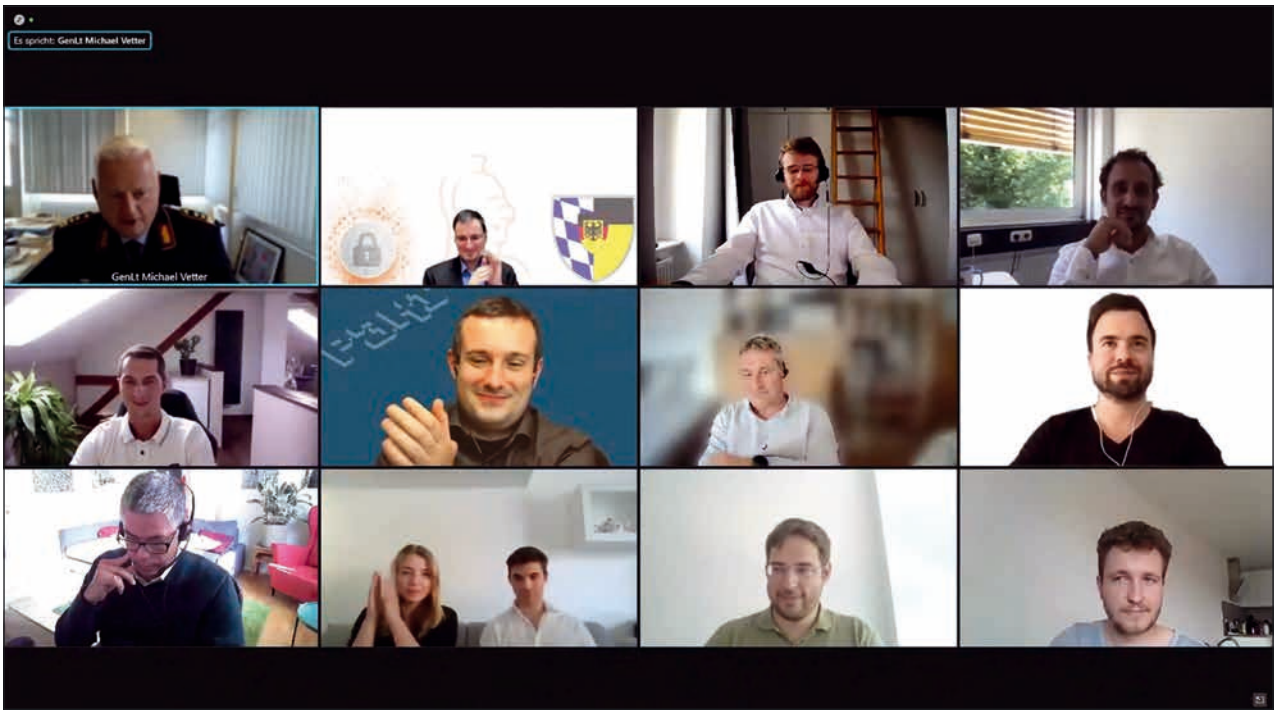
Innovationstagung: Zwölf innovative Ideen, drei Gewinner

Im Anschluss an die Workshop-Session fand am Nachmittag des zweiten Tages die Innovationstagung zum Themengebiet Cyber- und Informationstechnologie statt. Generalleutnant Michael Vetter, Abteilungsleiter des Referats Cyber- und Informationstechnik (CIT) im Bundesverteidigungsministerium, das für Forschung und Technologie sowie Innovationsmanagement Cyber/IT zuständig ist, betonte die Relevanz der Aufgabe, Innovationen zum Nutzen einer größeren digitalen Souveränität stärker zu fördern, und wies auf neue Einrichtungen wie das Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) sowie die Agentur für Innovation in der Cybersicherheit hin: beide konnten trotz der pandemischen Lage etabliert werden. In diesem Zusammenhang sei auch die Innovationstagung als fester Bestandteil zu verorten, um für die Bundeswehr relevante technische Neuerungen aus akademischer und industrieller Forschung und Entwicklung in einem kompetitiven Verfahren zu identifizieren und die Innovatoren sowie Bedarfsträger miteinander zu vernetzen.

Die im Jahr 2021 relevanten Themen für den Call for Proposals zur Innovationstagung waren Cybersicherheit, Kommunikation, Geoinformation sowie Informationsverarbeitung und -management. Aus einer Vielzahl von Einreichungen wählte die Jury zwölf innovative Ideen aus, die im Rahmen von siebenminütigen Kurzvorträgen dem Fachpublikum vorgestellt wurden. Anschließend bestand für die Tagungsgäste die Möglichkeit, mit den Vortragenden über ihre Konzepte zu diskutieren.

Dr. Kim Nguyen konnte sich über den ersten Platz im Wettbewerb freuen. Seine Idee zu Intelligent Composed

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



Die Teilnehmenden der Innovationstagung während der Siegerehrung.

Algorithms entstand mit dem Ziel, bekannte kryptografische Algorithmen zu kombinieren und diese in Anwendungen und Public-Key-Infrastrukturen einführen zu können. Die kombinierten Algorithmen sollen gleichzeitig verhindern, dass Standards wie X.509 oder CMS nur deshalb geändert werden müssen, weil Agilität bei den Algorithmen erreicht werden soll.

Der zweite Platz ging an Prof. Dr. Martin Werner von der Technischen Universität München. Er und sein Team adressierten mit ihrer Idee das effektive Verarbeiten großer Datenmengen aus unterschiedlichen Bereichen und Medien und insbesondere das gezielte Suchen nach bestimmten Informationen.

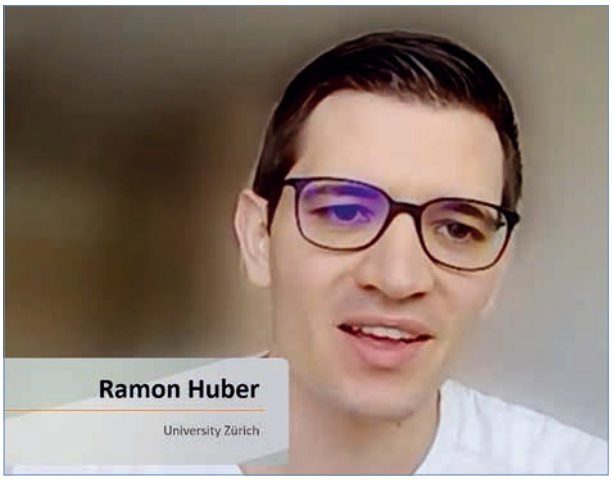
Erik Heiland von der Universität der Bundeswehr München erreichte im Wettbewerb den dritten Platz. Seine Idee zielt darauf ab, den proaktiven Umgang mit Bedrohungslagen zu verbessern und so entsprechende Gegenmaßnahmen früher einzuleiten.

Forum für den wissenschaftlichen Nachwuchs: Science Track

Zum zweiten Mal fand im Jahr 2021 im Rahmen der CODE-Jahrestagung der Science Track statt, der jungen Doktorandinnen und Doktoranden ein Forum zum wissenschaftlichen Austausch und Netzwerken bieten soll. Die Veranstaltung gliederte sich in das „Early Stage PhD Forum“ sowie das „Last Stage PhD Forum“. Der erste Programmpunkt bot angehenden Doktorandinnen und Doktoranden eine Plattform, um Promotionsvorhaben bereits zu einem frühen Zeitpunkt vorstellen und diskutieren zu können, während der zweite Programmpunkt einen Erfahrungsaustausch zwischen weiter fortgeschrittenen Doktorandinnen und Doktoranden mit ihren jüngeren Pendants ermöglichte. Aus den im Vorfeld der Tagung erhaltenen Einreichungen wurden im Rahmen eines wissenschaftlichen Begutachtungsprozesses sechs ausgewählt. Thematisch war das Programm bunt aus dem Bereich der IT-Sicherheit gemischt und reichte von Vorträgen aus dem Bereich der IT-Sicherheit vernetzter Systeme bis hin zu Anwendungen aus der Data Science beziehungsweise dem maschinellen Lernen.

Der erste Teil des wissenschaftlichen Programms wurde von Ramon Huber von der Universität Zürich mit einem Vortrag zu einer effizienten Kommunikation in drahtlosen Sensornetzen (wireless sensor networks, WSN) eröffnet. Das Ziel der Arbeit ist es, das von IPFIX abgeleitete Protokoll TinyIPFIX als rechen- und energieeffizienten Ansatz der push-basierten Kommunikation in Smart-Home-Szenarien umzusetzen.

Mina Schütz vom Austrian Institute of Technology (AIT) eröffnete den zweiten Teil des Doktorandenforums. Schütz stellte ihre Arbeit zur automatisierten Erkennung von Desinformationskampagnen vor. In ihrem Vorhaben legt sie einen besonderen Fokus auf die Erklärbarkeit der Ergebnisse, indem sie Methoden der natürlichen Sprachverarbeitung (natural language processing, NLP) mit Ansätzen aus dem Bereich der „Explainable AI“ (XAI) kombiniert.



Im Science Track hielt Ramon Huber einen Vortrag zu effizienter Kommunikation in drahtlosen Sensornetzen.

Wissenschaftlich wurde die Tagung von Prof. Dr. Barbara Carminati von der Universität Insubria (Italien), Prof. Dr. Burkhard Stiller von der Universität Zürich (Schweiz) sowie Prof. Dr. Florian Alt, Prof. Dr. Harald Baier und Prof. Dr. Wolfgang Hommel vom Forschungsinstitut CODE der Universität der Bundeswehr München begleitet. Die Veranstaltung erfreute sich großer Beliebtheit und konnte auch in rein virtueller Form einen guten Anschlusserfolg an die Premiere im Jahr 2020 erzielen. Der Science Track der CODE-Jahrestagung liefert einen zentralen Baustein zum Aufbau einer Community für den wissenschaftlichen Nachwuchs. ■

Mehr Informationen zur Jahrestagung „CODE 2021“

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

BEIDE ABB.: FI CODE

ABB.: ADOBE STOCK / NMEDIA

Forschung

Porträts
und Projekte

Die Forschung am FI CODE

Am Forschungsinstitut CODE werden derzeit 40 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.

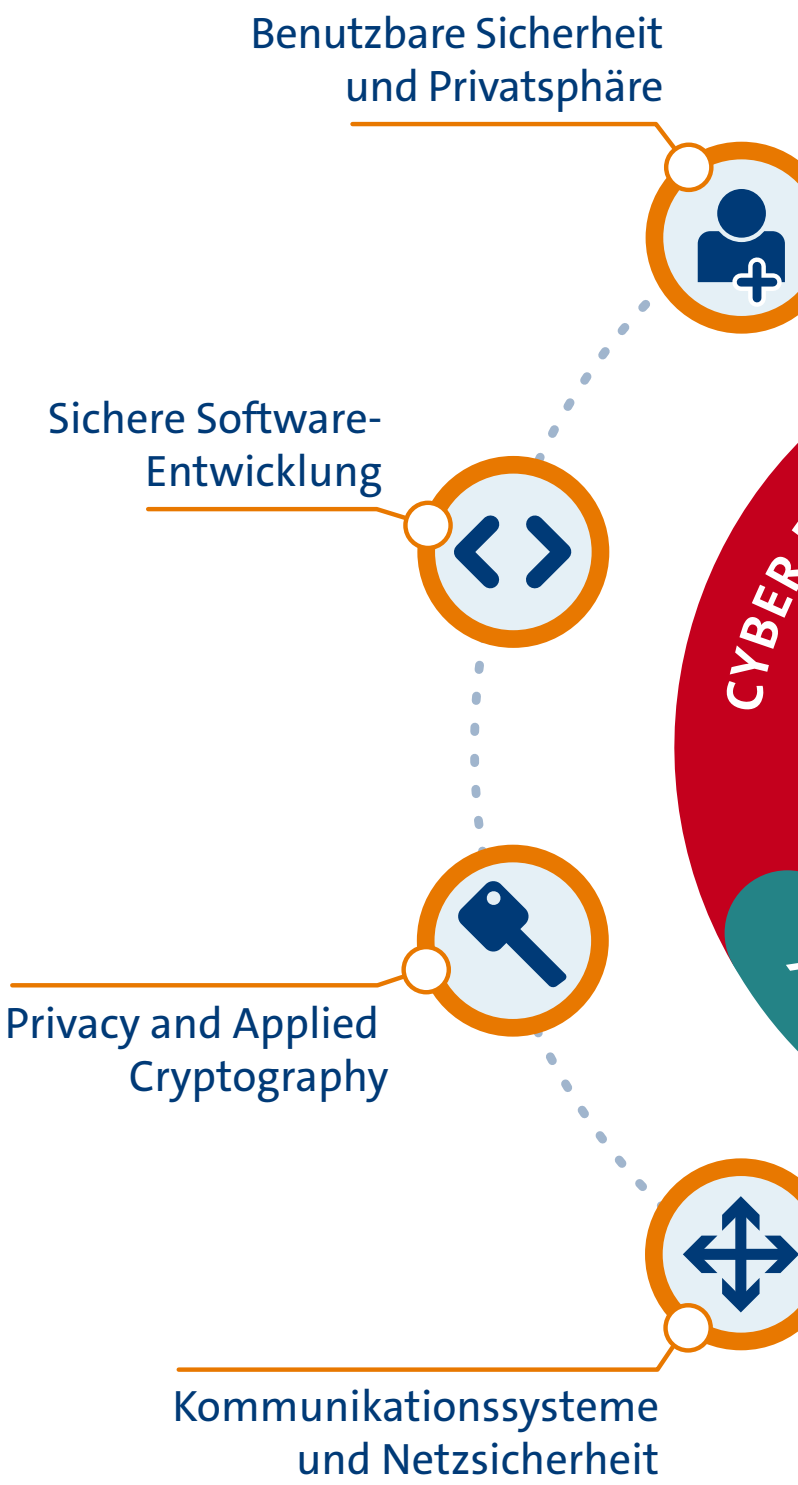
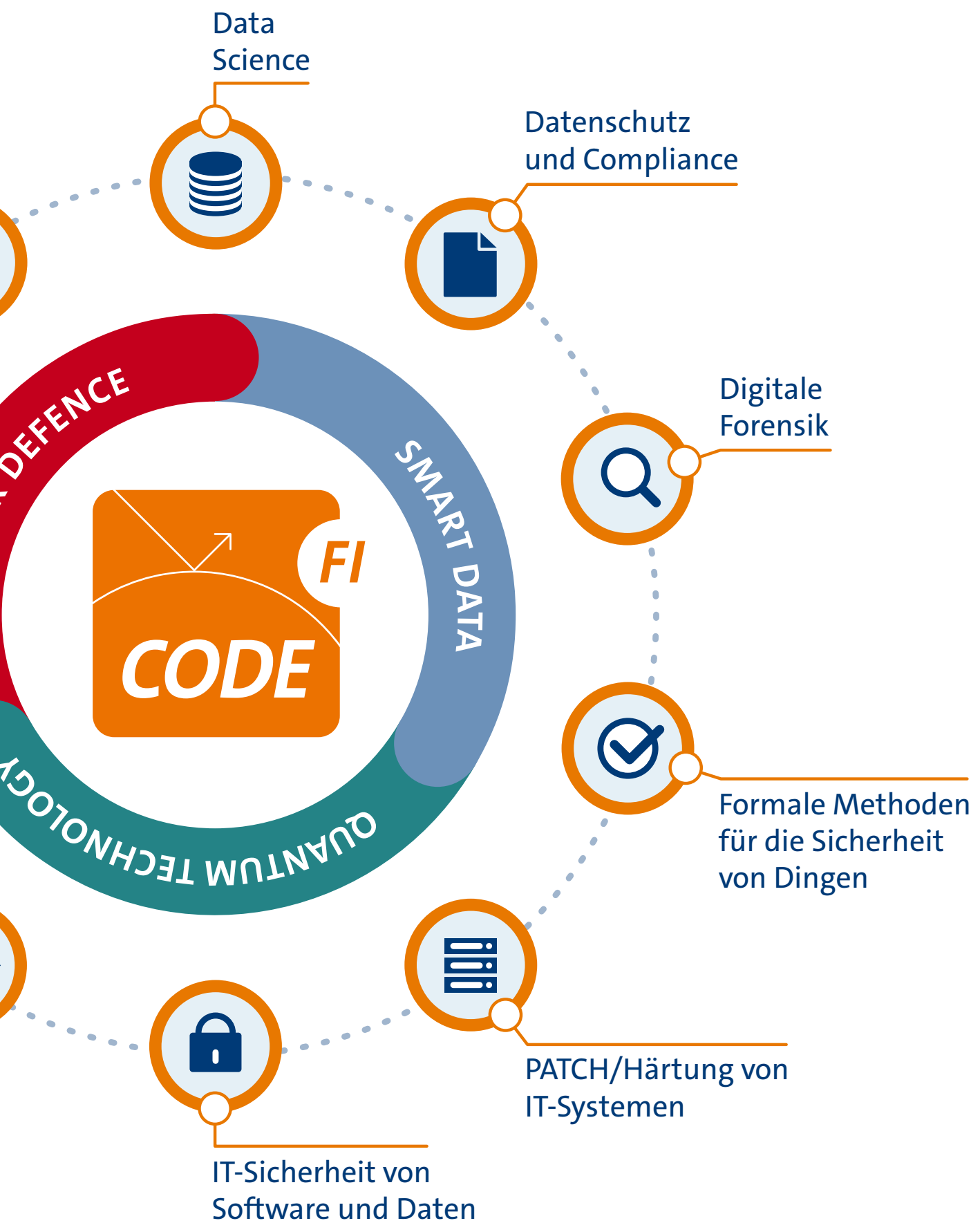


ABB.: TAUSENDBLAUWERK.DE


Data Science
Datenschutz und Compliance
Digitale Forensik
Formale Methoden für die Sicherheit von Dingen
PATCH/Härtung von IT-Systemen
IT-Sicherheit von Software und Daten
DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
FI
CODE

Prof. Dr. Florian Alt

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 die Frage, wie solche Systeme besser an die Interaktion, das Verhalten und den physiologischen Zustand von Menschen angepasst werden können.

DIE PROFESSUR für Benutzbare Sicherheit und Privatsphäre wurde im Jahr 2018 gegründet und forscht an der Schnittstelle zwischen Mensch-Computer-Interaktion, IT-Sicherheit und Datenschutz. Prof. Dr. Florian Alt untersucht mit seinem Team, wie Wissenschaft, Design und Produktentwicklung dabei unterstützt werden können, Sicherheits- und Datenschutzbedürfnisse bereits im Designprozess zu berücksichtigen. Ziel dabei ist es, Sicherheits- und Datenschutzmechanismen besser in die Art und Weise zu integrieren, wie Menschen 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 dem Blick). Weitere Themen sind die Untersuchung neuartiger Bedrohungen, welche durch ubiquitäre Technologien entstehen, und die Entwicklung entsprechender Schutzmechanismen, sowie das Erforschen von Ansätzen, die das Verständnis und das Verhalten von Personen in sicherheitskritischen Situationen verbessern sollen. Spezifische Anwendungsbereiche sind intelligente Heimumgebungen, Social Engineering, Verhaltensbiometrie und Mixed Reality.

Im Rahmen ihrer Forschung greift die Gruppe auf Methoden 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 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 Benutzerinnen und Benutzern in sicherheitsrelevanten Situationen in der realen Welt untersucht werden können.

Zusammen mit seinem Team hat Prof. Florian Alt über 230 in der Informatik-Bibliografie DBLP gelistete wissenschaftliche Beiträge veröffentlicht und mehr als zehn 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 Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst, die Humboldt-Stiftung, den DAAD, Google und die BMW Group gefördert.

Entwicklung der Forschungsgruppe im Jahr 2021

Die Forschungsgruppe Usable Security and Privacy ist im Jahr 2021 gewachsen und umfasst neben Prof. Florian Alt aktuell 14 Mitarbeitende und vier wissenschaftliche Hilfskräfte. Unter den wissenschaftlichen Mitarbeitenden der Forschungsgruppe befinden sich neun Promovierende und vier Postdoktoranden, die 2021 an über 30 Publikationen mitgewirkt haben.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

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

Die Forschungsgruppe nutzt Technologien wie Augmented oder Virtual Reality, um Privatsphäre- oder IT-Sicherheitsrisiken sichtbar zu machen oder das Verhalten von Personen in simulierten Umgebungen zu erforschen.

ABB.: ISTOCK / PHOTOTECHNO; FLORIAN ALT

Projekt Voice of Wisdom

Sicherere, menschzentrierte Technik

Im Rahmen des Voice of Wisdom-Projekts wird eine Umgebung zur Erforschung menschlichen Verhaltens und physiologischer Reaktionen in sicherheitskritischen Kontexten konzipiert und aufgebaut. Außerdem werden neuartige, sichere Benutzerschnittstellen entwickelt.

Verhalten und Physiologie in risikobehafteten Situationen

Im Voice of Wisdom-Projekt werden neue Ansätze zur Verhinderung menschenbezogener Cyberangriffe erforscht. Ziel ist es, durch eine Analyse menschlichen Verhaltens und physiologischer Reaktionen Anzeichen zu erkennen, dass Menschen einem Risiko ausgesetzt sind, und sie somit beim Umgang mit Technik besser zu schützen. Durch ein besseres Verständnis menschlichen Verhaltens und physiologischer Zustände, sei es bei der Arbeit, in der Kommunikation mit anderen Menschen oder der Interaktion in einer Gruppe, können Anzeichen von und Vorstufen zu einem Verhalten erkannt werden, das ein hohes Risiko impliziert.

Verwendung von alltäglichen Geräten und modernen Technologien

Zu diesem Zweck wird die Tatsache ausgenutzt, dass Sensoren in Geräten des täglichen Gebrauchs – beispielsweise Tastatur, Maus oder Smartwatch – es erlauben, (subtile) Änderungen im Verhalten oder im physiologischen Zustand der Person zu erkennen – auch wenn dieser sich dessen nicht bewusst ist. Moderne Technologien wie Wärmebildkameras, Tiefenkameras und Eyetracker tragen ebenfalls hierzu bei. Mit den gewonnenen Erkenntnissen lassen sich neuartige Sicherheitsmechanismen entwickeln, welche durch Hinweise und Handlungsanweisungen geeignet unterstützen (zum Beispiel Pop-ups, Benachrichtigungen auf einer Smartwatch, Indikatoren für Videokonferenzsoftware) oder automatisiert im Hintergrund ausgeführt werden.

Bestimmte Verhaltensmuster und die physiologischen Reaktionen von Menschen können auf sicherheitskritische Situationen hinweisen.

Ziele des Projekts

Das Voice of Wisdom-Projekt hat zum Ziel, eine Forschungsumgebung zur Beobachtung von menschlichem Verhalten und physiologischen Zuständen in sicherheitskritischen Situationen aufzubauen. Hierdurch wird eine detaillierte Analyse sicherheitskritischer Situationen und deren Einfluss auf Menschen ermöglicht. Darauf basierend werden in einem nächsten Schritt neuartige, menschenbezogene Sicherheitsmechanismen entwickelt und die langfristigen Auswirkungen der entwickelten Technologien sowie der Sicht der Betroffenen untersucht.

Projektfortschritt im Jahr 2021

Im ersten Projektjahr wurden Grundlagen in technischer sowie konzeptioneller Sicht für das Projekt geschaffen. Eine zentrale Fragestellung besteht darin, welche Sensorik bestmöglich geeignet ist, um Änderungen in der Physiologie des Menschen festzustellen. Gleichzeitig muss gewährleistet sein, dass diese Sensorik akzeptiert und auch aktiv genutzt wird. Aufgrund von COVID-19 sind viele Arbeitnehmerinnen und Arbeitnehmer ins Homeoffice gewechselt. In diesem Zusammenhang stellt sich die Frage, ob Sensorik, die die Privatsphäre einschränkt (wie etwa Tiefenkameras) kritischer betrachtet wird, wenn sie in der eigenen Wohnung aufgestellt wird.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

https://go.unibw.de/vow

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Projekt PrEvoke

Benutzerunterstützung beim Widerruf von Datenschutz-Berechtigungen

PrEvoke befasst sich mit den Folgen des Widerrufs von Datenschutz-Entscheidungen, beispielsweise, wenn Apps der Zugriff auf persönliche Daten entzogen wird. Insbesondere ist den Nutzerinnen und Nutzern im Allgemeinen nicht bewusst, wie sich solche Entscheidungen auf die Funktionalität einer App, deren Verhalten oder Inhalt auswirken.

DIE PERSONALISIERUNG digitaler Dienste oder Apps erfordert den Zugang zu sensiblen Daten, wie etwa zum Standort der Person, ihrem Kalender oder den auf dem Gerät gespeicherten Inhalten. Gleichzeitig ist den Betroffenen meist nicht klar, welchen Einfluss die (Nicht-)Gewährung des Zugriffs auf solche Daten hat. Der heute vorherrschende Ansatz ist, dass einmalig bei der Einrichtung oder der ersten Nutzung entschieden wird, ob die angeforderten Berechtigungen gewährt werden oder nicht. Dieser Prozess ist allgemein als „Privacy Calculus" bekannt, das heißt, die Nutzerinnen und Nutzer entscheiden, ob ihnen der erwartete Vorteil des angeforderten Dienstes oder der angeforderten Anwendung die Herausgabe der entsprechenden Daten wert ist. Die Herausforderung besteht nun darin, dass die Menschen in den meisten Fällen diese Entscheidungen nie überdenken und gegebenenfalls widerrufen.

Bedenken und Erwartungen verstehen

Die Bedenken hinsichtlich der Folgen des Widerrufs von Datenschutz-Entscheidungen, das heißt, ob die Kernfunktionalität einer App oder eines Dienstes beeinträchtigt wird oder wie sich die Entscheidung auf die Auswahl des Inhalts und das Verhalten der App auswirkt, sind derzeit noch kaum erforscht. Zu diesem Zweck werden die erwarteten Konsequenzen und Sorgen in Bezug auf den Widerruf von Datenschutz-Berechtigungen untersucht, um festzustellen, ob diese mit der Realität übereinstimmen und wie Konzepte erstellt werden können, um Missverständnissen und Bedenken entgegenzuwirken.

Für die Personalisierung von Apps ist Zugang zu sensiblen Daten wie dem Standort oder dem Kalender nötig.

Verhalten von Diensten und Anwendungen ermitteln

Außerdem wird bewertet, wie der Entzug bestimmter Berechtigungen die Funktionalität von Webdiensten und mobilen Anwendungen tatsächlich beeinflusst. Die Ergebnisse dieser Auswertung werden mit den Erwartungen der Benutzer verglichen. Auf diese Weise ist es möglich, Missverständnissen vorzubeugen und Informationen zu identifizieren, die durch ein entsprechendes Assistenzsystem für Datenschutz-Berechtigungen vermittelt werden müssen.

Anwendungsbereiche: Webdienste und Smartphone-Apps

Das Projekt fokussiert sich auf zwei Anwendungsbereiche: Webdienste und Smartphone-Apps. Dies ermöglicht die Untersuchung eines breiten Spektrums von Datenschutz-Berechtigungen, angefangen bei physiologischen Sensoren über den Zugriff auf Kalender, Anrufprotokolle, Kamera, Kontakte, Dateien und Medien, Standort, Mikrofon und Zahlungsinformationen bis hin zu körperlicher Aktivität und Nachrichten. Es ist davon auszugehen, dass die Ergebnisse über diese Anwendungsbereiche hinaus, insbesondere aber auf Smart-Home- / Internet-of-Things- und Augmented-Reality-Geräte anwendbar sind.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

Gefördert durch: Google München

ABB.: ISTOCK / METAMORWORKS; ISTOCK / IPOPBA

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 das Gerät 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: Die 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/ MICROGEN, NOPPONPAT

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.

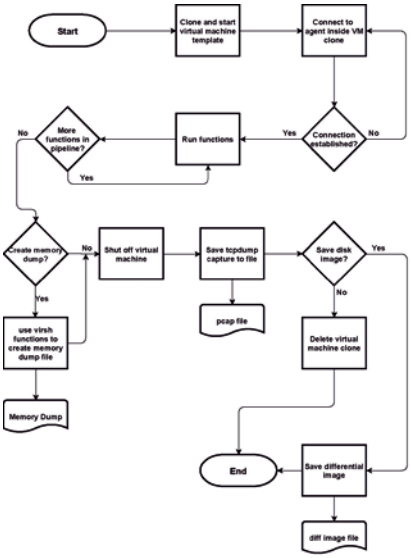
Anforderungen

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.

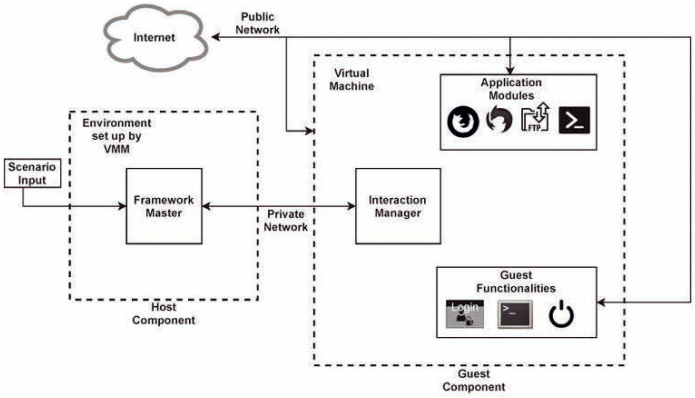
Zudem müssen die Datensätze weitere Anforderungen wie Anpassbarkeit, Verfügbarkeit, Nachvollziehbarkeit und Nachprüfbarkeit erfüllen. Ein weiterer wesentlicher Punkt für die Evaluation der Datensätze ist, dass bekannt sein muss, was die IT-forensische Software später überhaupt finden soll – das heißt,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

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

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

Umgang mit großen Datenmengen

Eine IT-forensische Untersuchung ist mit der Herausforderung der schieren Datenflut konfrontiert. Es sind zahlreiche Datenträger von unterschiedlichen Geräten wie Computer, Smartphones und Tablets sowie Wechseldatenträger wie USB-Sticks, Speicherkarten und DVDs zu sichten. Die Datenmenge erreicht regelmäßig mehrere Terabytes. Hier gilt es, möglichst automatisiert wichtige Spuren von unwichtigen zu trennen, also die berühmte Nadel im Heuhaufen zu finden.

Datenreduktion

Um die Daten nach der IT-forensischen Sicherung möglichst automatisiert im Hinblick auf die juristische Fragestellung zu sichten, hat die Forschungsgruppe unterschiedliche Ansätze der Datenreduktion mitentwickelt, analysiert und bewertet. Ein erster solcher Ansatz sucht nach bekanntermaßen fallirrelevanten Daten (etwa Dateien des Betriebssystems oder installierter Applikationen) und blendet diese für die weitere Untersuchung aus. Untersuchungen der Forschungsgruppe haben aber ergeben, dass für typische Datenträger mit vielen individuellen Dateien die Größenordnung der als irrelevant eingestuften Daten im mittleren einstelligen Prozentbereich liegt.

Approximate Matching

Ein zweiter Ansatz der Datenreduktion verwendet Approximate-Matching-Algorithmen, also veränderungsrobuste Komprimierungsfunktionen („Fuzzy-Hashing-Verfahren"), zur Erkennung bzw. Wiedererkennung fallspezifischer digitaler Artefakte. Beispielsweise können mithilfe von Approximate Matching Fragmente von gelöschten kinderpornographischen Schriften gefunden und dem ursprünglichen Bild zugeordnet werden.

Künstliche Intelligenz

Das Themenfeld der Künstlichen Intelligenz (KI) beziehungsweise des Maschinellen Lernens (ML) soll auch genutzt werden, um fallbezogene Datenstrukturen durch KI-Methoden aufzuspüren. Allerdings befindet sich die Forschung im Vergleich zu anderen Disziplinen der Cybersicherheit hier noch in einem frühen Stadium. Ein wichtiges Problemfeld von KI im Kontext der digitalen Forensik ist, dass viele ML-Verfahren hinreichend gut angelernt, das heißt, mit Daten gefüttert werden müssen. Dazu wird eine kritische Masse an gelabelten Datensätzen benötigt, die leider rar sind. Vor diesem Hintergrund ist es wichtig, dass mit Lösungen wie ForTrace (s. S. 38) auch KI-basierte Verfahren in der digitalen Forensik unterstützt werden.

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

Die hohe Anzahl unterschiedlicher IT-Geräte führt zu großen Datenmengen.

ABB.: ISTOCK / METAMORWORKS; ISTOCK / IPOPBA

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

Die Forschungsgruppe von Prof. Dr. Stefan Brunthaler beschäftigt sich intensiv mit sogenannter sprachbasierter Sicherheit, insbesondere der Absicherung von Software durch sprachbasierte Transformationen, um große Softwaresysteme automatisch, transparent und effizient zu schützen.

DAS MUNICH COMPUTER SYSTEMS Research Laboratory (µCSRL) an der Professur „Sichere Software-Entwicklung“ beschäftigt sich mit der Erforschung und Entwicklung neuester Verteidigungstechniken, um fortgeschrittene, hochkomplexe und brandaktuelle Angriffe zu verhindern. Dabei baut das Team auf seine Expertise im Programmiersprachen-Bereich, insbesondere auf sein Compiler-Know-how, um komplexe und anspruchsvolle Probleme im Querschnitt von Programmiersprachen und Computersicherheit zu lösen.

Rückblickend kann die µCSRL-Forschungsgruppe das Jahr 2021 äußerst positiv bewerten und von wichtigen Fortschritten in den folgenden Bereichen berichten: Erstens konnte das Team seine Verteidigung gegen den mächtigen AOCR-Angriff nicht nur vervollständigen, sondern auch allgemein verbessern. Zweitens konnten die Forscher die Machbarkeit eines komplett neuen Ansatzes zum Dekompilieren von Binärprogrammen erfolgreich demonstrieren. Drittens konnten der Fuzzing-Cluster operativ eingesetzt und schlussendlich auch das Wachstum der Forschungsgruppe vorangetrieben werden.

Neue Forschungsergebnisse

Die Verteidigung gegen den Address-Oblivious Code Reuse (AOCR)-Angriff konnte in vielerlei Hinsicht verbessert werden. Die wichtigste neue Komponente im Ansatz des Teams ist die Erweiterung der Idee von reaktiven „Fallen“, den sogenannten Booby Traps, für Daten und der damit einhergehende vollständige Schutz gegen AOCR. Zweitens konnte das Team seine Verteidigung durch Anwendung von SSE- und AVX-Befehlssätzen weiter optimieren, sodass der vollständige Schutz vor AOCR bei einer durchschnittlichen Geschwindigkeitseinbuße von fünf Prozent erzielt werden kann. Soweit bekannt, existiert derzeit kein bekannter Code-Reuse-Angriff, der nicht durch die entwickelten Software-Diversity-Verteidigungstechniken vollständig automatisch und transparent verhindert werden kann.

Die Bestrebungen der Forscher, den Stand der Technik im Bereich der Dekompilierung von Programmen, mithin der „Rückwärtstransformation“ von Binärcode nach Source Code, voranzutreiben, waren ebenfalls äußerst erfolgreich. Der teameigene Decompiler – µDC, Abkürzung für „Munich Feedback Directed Decompiler“ – verwendet eine Feedback-Schleife, um Binärprogramme auf Quelltext zu projizieren. Die so rekonstruierten Programme können erneut kompiliert und somit als Maß verwendet werden, um festzustellen, ob man sich dem Original-Binärprogramm nähert. Dadurch können dekompilierte Programme beispielsweise auch mit neuen Verteidigungstechniken gegen Angriffe gehärtet werden.

Der Fuzzing-Cluster ist seit Ende des Jahres operativ einsetzbar. Somit können die ambitionierten Forschungspläne mit einer Rechenkapazität von 1.200+ CPUs vorangetrieben werden. Die Forschungsgruppe ist optimistisch, bereits im Jahr 2022 vielversprechende Resultate erzielen zu können, wenngleich das Thema für die unmittelbar folgenden Jahre weiterhin auf der Agenda stehen wird.

µCSRL: Aufwuchs und Neuigkeiten

Schließlich freut es das Team, berichten zu können, dass der Aufwuchs von µCSRL erfolgreich vonstatten geht: Drei neue Doktoranden und ein neuer Masterstudent konnten gewonnen werden. Damit ist das Team optimal aufgestellt, um auch weiterhin ambitionierte und anspruchsvolle Probleme anzupacken.

Prof. Dr. Brunthaler und sein Team haben bisher mehr als 30 Arbeiten im Systems-Bereich publiziert und davon die Hälfte in den jeweils besten internationalen und hochkompetitiven Konferenzen veröffentlicht, etwa im IEEE Symposium on Security and Privacy, dem Networked and Distributed Systems Security Symposium (NDSS), der ACM Conference on Computer and Communications Security (CCS), der ACM SIGPLAN Conference on Object Oriented Programming: Systems, Languages, and Applications (OOPSLA), dem IEEE / ACM International Symposium on Code Generation and Optimization (CGO) und der European Conference on Object-Oriented Programming (ECOOP).

Im Jahr 2021 wurde Prof. Brunthaler als Mitglied in die Arbeitsgruppe 2.4 „Software Implementation Technology“ der IFIP gewählt und hat bisher mehr als 30 eingeladene Vorträge gehalten. Zu guter Letzt wurde seine Forschung zur Optimierung von dynamischen Programmiersprachen von Python angewandt und findet somit täglich bei hunderten Millionen Menschen Anwendung.

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

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

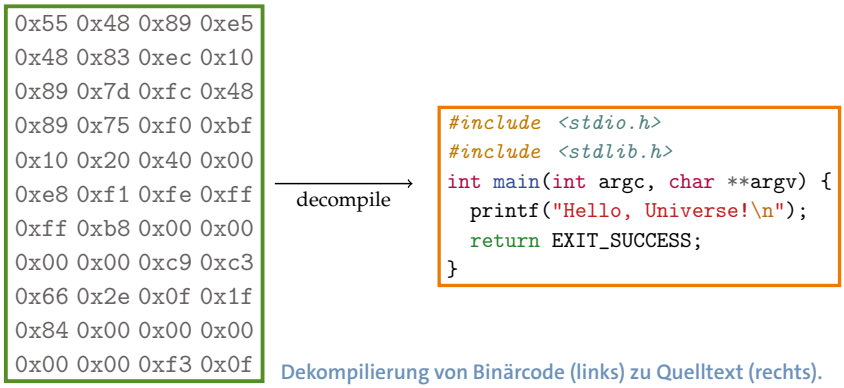
www.unibw.de/ucsrl

ABB.: ISTOCK / DE M10

Projekt µdc

Feedback-gesteuerte Dekompilierung

Compiler übersetzen den Quelltext eines Programms in Binärform, während Decompiler versuchen, diese Übersetzung umzukehren. Da bei der Übersetzung Informationen verworfen werden, ist diese Rückübersetzung nicht immer exakt möglich. Der Munich Decompiler bezieht bei der Rückübersetzung das Feedback eines Compilers ein und kann so deutlich präziseren Quelltext aus der Binärform eines Programms extrahieren.



Dekompilierung von Binärcode (links) zu Quelltext (rechts).

Compiler versus Decompiler

Um ein Programm, das in für Menschen lesbarem Quelltext geschrieben ist, auszuführen, muss der Quelltext zuerst von einem Compiler in Binärform übersetzt werden. Mitunter ist der Quelltext eines bereits kompilierten Programms nicht verfügbar und das Programm liegt ausschließlich in Binärform vor. Der Quelltext ist jedoch für Aufgaben wie Wartung oder Sicherheitsüberprüfungen essenziell. Sogenannte Decompiler versuchen deshalb, die Übersetzung des Compilers umzukehren und den ursprünglichen Quelltext des Programms aus der Binärform zu gewinnen. Diese Rückübersetzung nennt sich Dekompilierung.

Fehlende Informationen bei der Dekompilierung

Nach der Übersetzung von Quelltext in eine Binärform verwirft ein Compiler sämtliche Informationen, die ausschließlich für die Übersetzung, nicht jedoch für die Ausführung des Programms relevant sind. Dieser Informationsverlust erschwert allerdings die Dekompilierung erheblich. Beim Versuch, den ursprünglichen Quelltext aus der Binärform zu extrahieren, muss ein Decompiler Annahmen über diese nicht mehr verfügbare Information treffen, um den ursprünglichen Quelltext bestmöglich anzunähern. Da diese Annahmen jedoch fehlerhaft sein können, entspricht der wiederhergestellte Quelltext oftmals nicht exakt dem ursprünglichen Quelltext.

Der Munich Decompiler

Ein Problem von bestehenden Decompilern ist, dass getroffene Annahmen nicht überprüft werden und Fehlannahmen zu einem unpräzisen wiederhergestellten Quelltext führen. Der Munich Decompiler löst dieses Problem, indem er getroffene Annahmen durch eine erneute Übersetzung mittels eines Compilers validiert. Das so gewonnene Feedback führt zu einer deutlich höheren Präzision des wiederhergestellten Quelltexts.

Bedeutung und gesellschaftliche Relevanz

Der Munich Decompiler stellt eine wesentliche Verbesserung im Problemfeld der Dekompilierung dar und ermöglicht so Fortschritte in etlichen Bereichen, die auf die Dekompilierung von Programmen angewiesen sind. Beispielsweise ist die Dekompilierung bei der Sicherheitsüberprüfung von proprietären Programmen, aber auch bei der Analyse von Schadsoftware von großer Bedeutung.

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

ABB.: S. BRUNTHALER

Projekt Install-Time Diversity

Programmdiversifizierung während der Installation

Schadsoftware befällt oftmals eine Vielzahl von Geräten, da überall das exakt gleiche Abbild eines Programms in Betrieb ist. Software Diversity wirkt dieser Gefahr entgegen, indem jedes Gerät stattdessen eine eigene, diversifizierte Variante desselben Programms erhält. Mit „Install-Time Diversity“ untersucht das Projektteam neuartige Methoden, um Programme bei deren Installation automatisch zu diversifizieren.

Software Diversity

Die wesentliche Idee von Software Diversity ist es, Programme proaktiv zu verändern, um diese resilienter gegenüber Angriffen zu machen. Durch das heutzutage vorherrschende Software-Verteilungsmodell, bei dem auf etlichen Computern identische Kopien eines Programms laufen, ist eine Schwachstelle in sämtlichen Kopien mit einem großflächigen Angriff ausnutzbar. Software Diversity begegnet dieser Gefahr, indem stattdessen auf jedem Computer eine eigens diversifizierte Version des Programms zum Einsatz kommt. Angreifer verlieren so den Skaleneffekt, der es ihnen ermöglicht, mit einem einzigen Angriff eine Vielzahl an Geräten anzugreifen.

Verteilung von diversifizierten Programmen

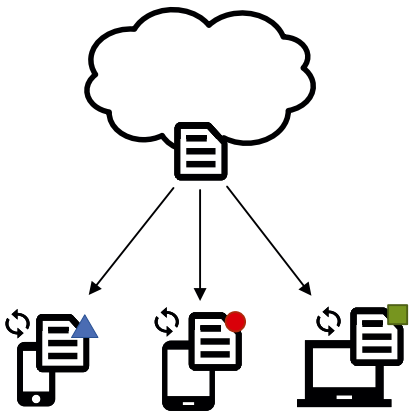
Diversifizierte Varianten eines Programms können an mehreren Punkten im Software-Entwicklungszyklus erstellt werden. Beispielsweise können eigens angepasste Compiler Programme bereits während der Kompilierung diversifizieren. Alternativ können Programme so angepasst werden, dass diese sich bei der Ausführung selbst diversifizieren. Diese beiden Software-Diversity-Varianten eignen sich jedoch schlecht für den Einsatz auf ressourcenschwachen Geräten. Zum einen erschwert der Vertrieb von Programmen über bestehende Verteilungskanäle, wie zum Beispiel App-Stores, die Diversifizierung durch einen Compiler, da das Programm für jeden Download neu diversifiziert werden müsste. Zum anderen führen selbst-diversifizierende Programme auf Geräten mit beschränkten Ressourcen, wie etwa Smartphones, zu Leistungseinbußen.

Software Diversity bei der Installation

Im Projekt „Install-Time Diversity“ beschäftigen sich die Forscher mit Möglichkeiten, um Software Diversity auch im Bereich von Geräten mit Ressourcenbeschränkung praktikabel zu machen. Mit „Install-Time Diversity“ werden die fertig übersetzten Programmteile an das Endgerät ausgeliefert und auf jedem Gerät beim Zusammensetzen individuell verändert. Dadurch kann einerseits bestehende Infrastruktur zur Verteilung von Programmen weiterverwendet werden und andererseits entstehen durch die Diversifizierung zur Installationszeit keine zusätzlichen Laufzeitkosten auf dem Endgerät. Software Diversity wird somit auch auf ressourcenschwachen Endgeräten wie Smartphones oder Routern anwendbar.

Bedeutung und gesellschaftliche Relevanz

Software Diversity ist die Antwort auf die Probleme der Software-Monokultur, die sich unter anderem in der rapiden Verbreitung von Viren und Ransomware widerspiegeln. Das Projekt „Install-Time Diversity“ ermöglicht die effizientere Erstellung von Varianten und ebnet so den Weg für einen breitflächigeren Einsatz von Software Diversity.



Die Diversifizierung der Software erfolgt nach dem Download direkt auf dem Endgerät.

ABB.: S. BRUNTHALER

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 und 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.

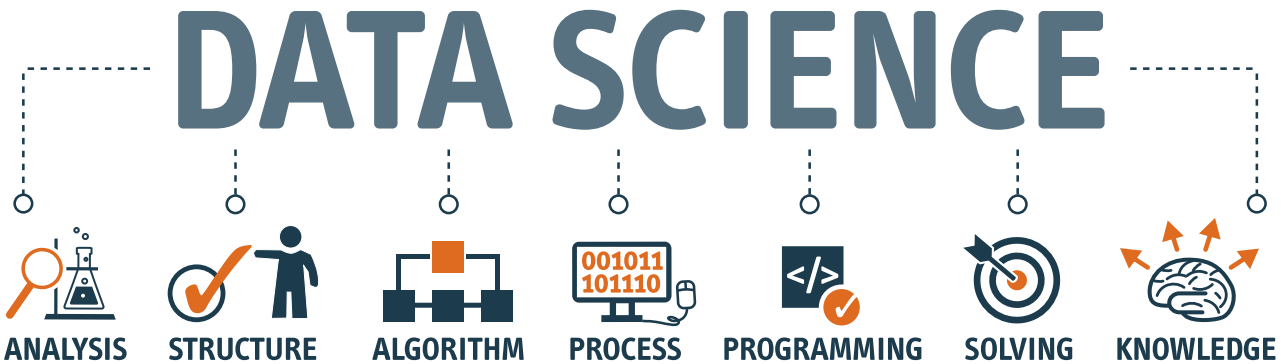
Die jüngsten technologischen Fortschritte und Entwicklungen im Bereich der Künstlichen Intelligenz (KI) haben auch sogenannte Deepfakes hervorgerufen. Hierunter wird eine mittels KI erzeugte audiovisuelle Modifikation eines Videos verstanden, in welcher das Gesicht und/oder die Aussagen der im Video 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; SHUTTERSTOCK / TRUEFFELPIX

Projekt KIMONO

Identifikation und Modellierung von Desinformationskampagnen in Sozialen Medien

Das 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. In diesem Kontext werden die besten Methoden zur Erkennung solcher Kampagnen und Narrative gesammelt, um die Erstellung eines Prototyps für ein Frühwarnsystem anzuregen.

Desinformationskampagnen in Sozialen Medien können viele Formen und Folgen haben.

DESINFORMATIONSKAMPAGNEN können Menschen manipulieren und beeinflussen und so zu einer massiven Schwächung des Vertrauens in die Demokratie, ihre rechtsstaatlichen Prinzipien sowie in die Meinungsfreiheit führen. Zudem besteht die Gefahr, dass staatliche Akteure Beeinflussungskampagnen in Sozialen Medien nutzen, um gegnerische Staaten zu destabilisieren (hybride Kriegsführung). Es gilt daher, diese Kampagnen möglichst frühzeitig zu erkennen und ihre Entwicklung und Verbreitung zu beobachten, um geeignete Gegenmaßnahmen einleiten zu können.

Im Projekt KIMONO wird eine Pipeline implementiert, die entsprechende Daten von verschiedenen Social-Media-Plattformen wie Twitter, Facebook und Instagram abruft und in einer Datenbank speichert. Darüber hinaus konsultiert das Team Fact-Checking-Websites (wie Volksverpetzer.de, Correctiv.org, PolitiFact, TheWhistle), um den Wahrheitsgehalt der gesammelten Daten einzuschätzen. Verschiedene State-of-the-Art-Algorithmen des flachen und tiefen Lernens werden untersucht und auf die Social-Media-Daten angewendet. Für die Analyse und das Training von Klassifikationsmodellen werden die folgenden Merkmale extrahiert:

1. Die **anwenderbezogenen Merkmale** werden anhand der jeweiligen Social-Media-Profile ermittelt. In diesem Zusammenhang werden Informationen, wie lange der Account existiert, wie viele Posts getätigt wurden, wie viele Follower jemand hat und wie vielen Profilen gefolgt wird, als relevant für die vorliegende Fragestellung betrachtet. Diese Merkmale sind auch für die Erkennung von Social Bots nützlich.

2. Bei **beitragsbezogenen Merkmalen** wird davon ausgegangen, dass sich die Sprache von Kampagnen-Beiträgen von der in anderen Beiträgen unterscheidet. Das Team setzt daher auf eine oberflächliche syntaktische und semantische Analyse. Meinungen, Standpunkte, Stimmungen und Themen werden aus den Beiträgen extrahiert und in eine Rangfolge gebracht, um die wertvollsten Informationen zu erhalten. Es ist zu erwarten, dass starke Meinungsäußerungen, reißerische und/oder emotionale Formulierungen sowie die charakteristische Verwendung bestimmter Wörter und Phrasen zu finden sein werden, die von den Initiatoren der Kampagne genutzt werden.

Auch Erklärbarkeit ist in diesem Kontext von immenser Bedeutung. Klassische Deep-Learning-Modelle können als Black-Box-Systeme betrachtet werden und bieten weder genügend Informationen, um die Klassifizierung zu verstehen, noch um schlüssige Maßnahmen zu erkennen. Durch die Kombination leistungsfähiger neuronaler Netze mit traditionellerem Feature-Engineering scheint es jedoch möglich zu sein, Ergebnisse zu erzielen, die transparent und erklärbar sind. Am Ende des Projekts wird eine Liste von Anforderungen vorliegen, um darauf basierend die Entwicklung eines Monitoring- und Frühwarnsystems für Soziale Netzwerke zu initiieren.

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

Gefördert durch:
Bundesministerium der Verteidigung

ABB.: SHUTTERSTOCK / BUFFALOBOY

Projekt SMILE

Ein Skalierbares, Modulares und Interaktives Rahmenwerk zur Lagebildentwicklung

Im Projekt SMILE wird auf Basis unterschiedlicher Daten- und Informationsquellen ein System entwickelt, welches mit künstlicher Intelligenz (KI) ein Lagebild erstellt. Darin sollen beispielsweise themenspezifische Datensätze der letzten 24 Stunden auf einer Karte visualisiert werden, um so einen Überblick zu aktuellen lokalen Ereignissen zu erhalten. Außerdem sollen zur weiteren Analyse Hotspots oder Anomalien klar hervorgehoben werden können.

Ausgangslage im offenen Informationsraum

Plötzlich auftretende, dynamische Ereignisse werden durch eine Vielzahl von Akteuren erfasst und über unterschiedliche Medien und Kanäle verbreitet. Viele dieser Quellen sind öffentlich zugänglich und könnten genutzt werden, um sich umfassend zu politischen, wirtschaftlichen und sozialen Veränderungen, sowohl auf lokaler als auch globaler Ebene, zu informieren. Gleichzeitig offenbart diese gigantische Datenmenge jedoch auch eine Reihe von **Herausforderungen** in Bezug auf die Datenanalyse und -bereitstellung, welche eine effiziente Nutzung der frei verfügbaren Informationen erschweren:

- Datengewinnung aus unterschiedlichen Quellen
- Sicherstellung von Informationsqualität und -validität
- Verarbeitung inhomogener Datensätze
- Effiziente Informationssuche
- Datenaggregation und -korrelation
- Datenvisualisierung
- Dateninteraktion

Für fundierte Entscheidungen und strategische Planungen ist eine zuverlässige Informationsbasis nahezu unabdingbar.

Zielsetzung von SMILE

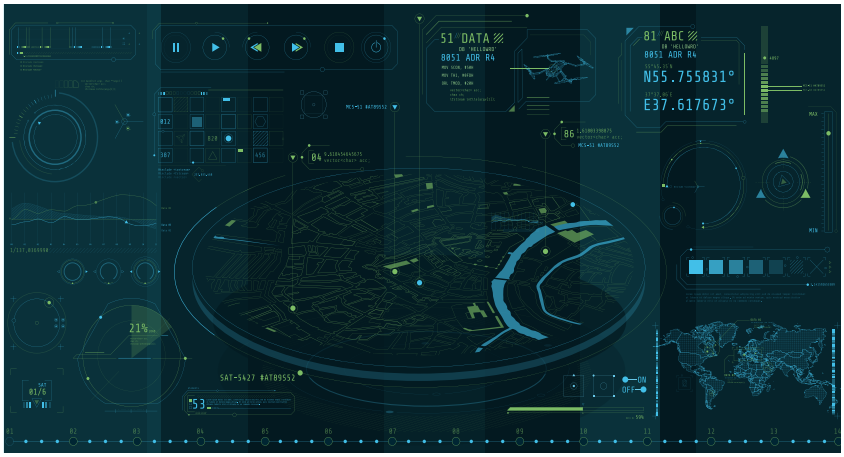
Das Ziel von SMILE ist daher die Entwicklung eines skalierbaren, modularen und interaktiven Rahmenwerks, welches Daten aus unterschiedlichen Quellen extrahiert, verarbeitet und visualisiert. Die Daten sollen dabei letztendlich so aufbereitet werden, dass Hotspots, Anomalien oder ähnliche Abweichungen vom Ausgangszustand klar erkennbar sind. Zur weiteren Analyse soll darüber hinaus zum einen eine räumliche oder zeitliche Eingrenzung erfolgen und zum anderen ein bestimmtes Ereignis unter Hinzunahme ergänzender Datenquellen genauer betrachtet werden können.

Zum Erreichen dieser Ziele werden Methoden des Information Retrieval mit Clustering- und Klassifikationsalgorithmen sowie Methoden der Mensch-Maschine-Interaktion (HCI) kombiniert. Bei der Datengewinnung liegt der Fokus insbesondere auf öffentlich zugänglichen Daten, wie beispielsweise Presseagenturen, Social-Media-Diensten oder strukturierten Ereignis-Datenbanken.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340



Exemplarische Darstellung eines KI-gestützten Lagebilds.

ABB.: SHUTTERSTOCK / CONCEPTCAFE

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

Das Team von Prof. Dr. Wolfgang Hommel forscht unter dem Leitmotiv „Entwicklung und Betrieb sicherer vernetzter Anwendungen“ an technischen und organisatorischen Sicherheitsmaßnahmen für komplexe IT-Infrastrukturen und Umgebungen 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 sowie ökonomische und rechtliche Randbedingungen berücksichtigt.

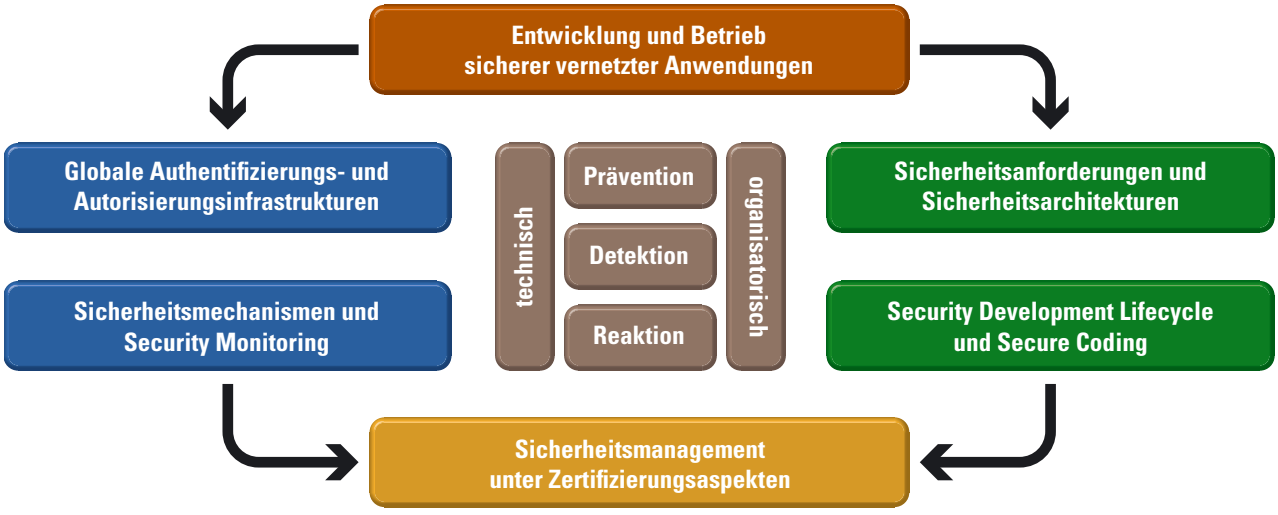
In aktuellen Forschungsvorhaben und Projekten wird beispielsweise an der Umsetzung des Self-Sovereign-Identity-Paradigmas für den Einsatz in globalen Authentifizierungs- und Autorisierungsinfrastrukturen als datenschutzfreundliche technologische Weiterentwicklung des in der Praxis bewährten Federated 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 beim Schutz der Remote-Management-Infrastrukturen moderner 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

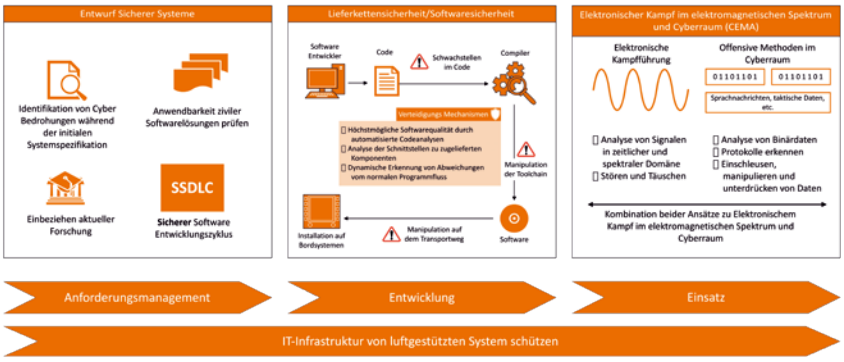
Projekt ACSE

Cybersicherheit für luftgestützte Systeme

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

Cybersicherheit als integraler Bestandteil des Entwicklungsprozesses: Aufzeigen von Bedrohungen aus dem Cyberraum

Das FI CODE und Airbus Defence and Space bündeln Kompetenzen aus den Bereichen IT-Sicherheit und Entwicklung luftgestützter Systeme, um aktuelle Entwicklungsprozesse beständig weiterzuentwickeln und fit für die Zukunft zu machen. Das Team begleitet aktuelle Industrieprojekte und evaluiert Möglichkeiten, den Entwicklungsprozess mit zusätzlichen organisatorischen und technischen Sicherheitsmechanismen zu erweitern. Um allgemein die Sensibilität für Bedrohungen aus dem digitalen Raum für fliegende Systeme zu erhöhen, wurden im Rahmen des Projekts relevante realistische Szenarien entworfen; diese dienen als „Leitplanken" für den weiteren Projektverlauf.



Beiträge von ACSE innerhalb des Entwicklungs- und Lebenszyklus.

Komplexe vernetzte Systeme härten

Moderne luftgestützte Systeme verfügen aufgrund anforderungsbedingter zunehmender Vernetzung über eine Vielzahl an heterogenen Schnittstellen zu internen und externen Netzwerken. Ziel von ACSE ist es, Methodiken und Konzepte zur (teil-)automatisierten Analyse und Interaktion dieser Schnittstellen zu untersuchen und zu implementieren. Dafür wird ein Framework entwickelt, das Protokolle und deren interne Einschränkungen und Abhängigkeiten möglichst generisch abbildet. Darauf basierend können unterschiedliche Funktionen modular realisiert werden. Unter anderem evaluiert das Team Möglichkeiten, die Schnittstellen von Hardwarekomponenten leichtgewichtig mithilfe des Frameworks zu emulieren, um passive sowie aktive Analysen zu ermöglichen. Gewonnene Daten können zu etablierten Netzwerkanalyse-Tools zur Weiterverarbeitung exportiert werden. Zur nahtlosen Integration in die bestehenden Entwicklungszyklen werden existierende Schnittstelledefinitionen den Entwicklern automatisiert durch das Framework zur Verfügung gestellt.

Sichere Software-Entwicklung im gesamten Entwicklungszyklus

Entwicklungs- und Zertifizierungsprozesse stellen hohe Anforderungen an die Software in Avionik-Systemen, insbesondere für Anwendungen mit hoher Kritikalität. Eine besondere Herausforderung ist die Heterogenität von Hardware und Software, die durch lange Projektlaufzeiten entsteht. Das Team nimmt aktuelle Entwicklungsprozesse unter die Lupe und erarbeitet organisatorische und technische Maßnahmen, um eine sichere Software-Entwicklung auch langfristig zu unterstützen. Für einzelne Abschnitte im Entwicklungszyklus werden konkrete technische Lösungen konzipiert. Ein Fokus liegt hierbei auf einer weitgehenden Automatisierung von Prozessschritten wie Code Reviews oder der Erstellung von Dokumenten, um diese direkt in den bestehenden Entwicklungszyklus einzubinden.

ABB.: ALEXANDER FRANK

Alexander Frank

alexander.frank@unibw.de

+49 89 6004 2745

www.unibw.de/software-security/forschung/acse-resources/acse

Gefördert durch:
Airbus Defence and Space

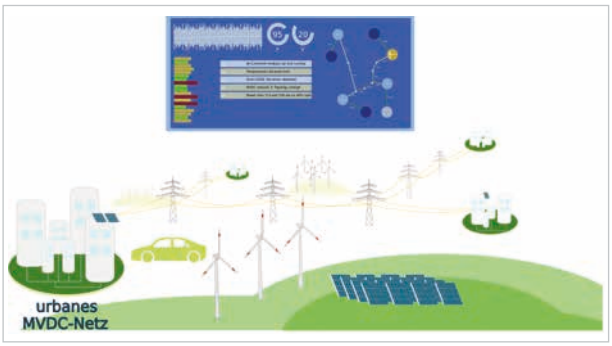
Projekt DEFINE

DC-Netze für eine sichere Energieversorgung

Im dtec.bw-Projekt DEFINE erforscht die Professur für IT-Sicherheit von Software und Daten in Zusammenarbeit mit den Fakultäten für Elektrotechnik und Informationstechnik, für Maschinenbau sowie für Bauingenieurwesen und Umweltwissenschaften der Universität der Bundeswehr München sichere Stromnetzinfrastrukturen der Zukunft.

Stromnetze: Schlagadern moderner Gesellschaften

Elektrischer Strom ist die Grundlage der modernen Informationsgesellschaft. Stromnetze sind historisch gewachsen und haben sich weitestgehend als Wechselstrom (AC) durchgesetzt. In den letzten Dekaden wichtig gewordene Aspekte wie Ressourceneffizienz und Kontrolle im Stromnetz lassen sich jedoch deutlich besser in Gleichstrom-(DC)-Netzen realisieren, die bei gleicher Investition ca. 50 Prozent mehr Energie transportieren können. Im Projektvorhaben wird daher die Realisierung von Mittelspannungsgleichstrom-(MVDC)-Netzen betrachtet.



Zentrales Netzmanagement für MVDC-Netze.

Sicherer Betrieb von MVDC-Netzen

MVDC-Netze erfordern im Betrieb jedoch eine hochdynamische Überwachung und Steuerung in Echtzeit: Darin befindliche Converter-Stationen müssen sich in Aktualisierungszyklen von wenigen hundert Mikrosekunden laufend aufeinander abstimmen. Da es derartige Konzepte für herkömmliche AC-Netze noch nicht gibt, müssen sichere Steuerungsinfrastrukturen, -algorithmen und -protokolle dazu grundlegend erforscht und von Grund auf nach heutigen Standards der IT-Sicherheit gestaltet werden. Wesentliche Herausforderungen betreffen den Umgang mit jeglichen potenziellen Störfaktoren wie dem Ausfall einer Komponente, aber auch mit böswilligen Angriffen auf die Stromnetz- und Steuerungsinfrastruktur. Dadurch, dass der aktiven Steuerung und Konfiguration der Converter-Komponenten in einem MVDC-Netz eine zentrale Rolle zukommt, gewinnt auch die Absicherung der Kommunikations- und Steuerungsinfrastruktur stark an Relevanz. Von Angreifern manipulierte oder alte wiedereingespielte Steuerungsnachrichten (sog. Replay-Angriffe) können zur Betriebsunfähigkeit von MVDC-Netzen führen und müssen verhindert werden. Die hohen Updateraten von wenigen hundert Mikrosekunden beschränken jedoch die verwendbaren „Standardlösungen“ und lassen sich in MVDC-Netzen nicht direkt anwenden, sodass auch hier neue Lösungen notwendig werden.

Mandantenfähige Lösungen für Stromnetze

Ein weiteres Thema, welches in modernen IT-Netzen spätestens seit dem Aufkommen von Cloud-Computing nicht mehr wegzudenken ist, ist eine mandantenfähige Verwaltung. Auch im Stromnetz gibt es unterschiedliche Mandanten – zum Beispiel Stromerzeuger, Stromnetzbetreiber und Endkunden – die anfallende Echtzeitüberwachungsdaten immer besser einsetzen wollen. An der Professur werden auch hierzu neuartige Konzepte und daraus Prototypen entwickelt. Die Abbildung verdeutlicht dabei die Kernvision: Mehrere Teilnetze, verbunden durch herkömmliche Netzinfrastrukturen werden zentral überwacht, ausgewertet und gesteuert, um Fehlerfälle schnell und automatisiert behandeln zu können.

Michael Steinke

michael.steinke@unibw.de

+ 49 89 6004 4825

https://go.unibw.de/inf24define

Gefördert durch:
dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

ABB.: MICHAEL STEINKE

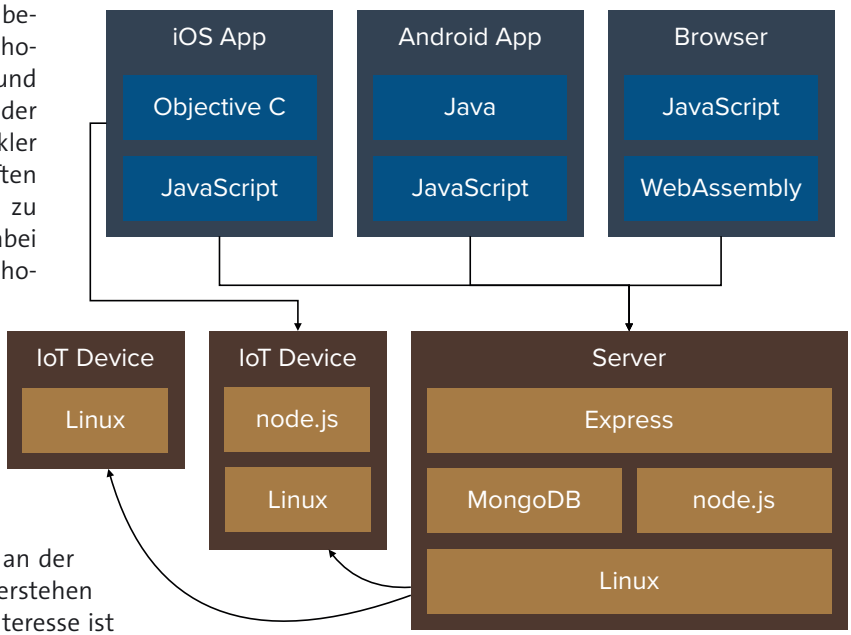
Prof. Dr. Johannes Kinder

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

Die Forschungsgruppe PATCH beschäftigt sich seit ihrer Gründung im Jahr 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 in jüngerer Zeit auch 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.



Moderne IT kombiniert viele verschiedene Programmiersprachen und Systeme.

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 mithilfe 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, 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

ABB.: ISTOCK / MONSITJ; J. KINDER / FI CODE

Projekt DEMISEC – Erkennung von Schadcode-Implantaten

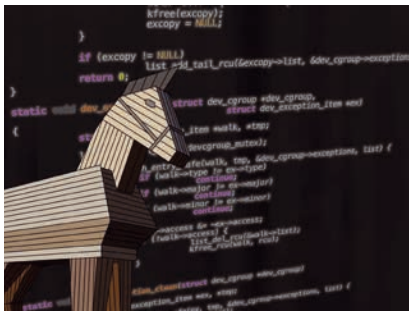
Moderne Software-Lieferketten vor Angriffen von innen wie außen schützen

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.

DIE WIEDERVERWENDUNG von Softwarekomponenten ist gängige Praxis in der Softwareentwicklung. Entwickelnde können heutzutage komplexe Projekte schnell realisieren, indem sie Komponenten und Bibliotheken miteinander kombinieren und dabei aus einem großen Angebot an Open-Source-Code auswählen. Einerseits eliminiert dies Wiederholungen und damit Möglichkeiten, versehentlich (neue) Schwachstellen einzuführen. Andererseits entsteht dadurch eine lange Software-Lieferkette mit Abhängigkeiten, bei der jedes Element vertrauenswürdig sein sollte.

Schutz von Open-Source-Code

Bösartiger Code, der an einem beliebigen Punkt der Lieferkette implantiert wird, kann sich in kritische Systeme hinein ausbreiten. Es gab bereits mehrere Fälle, in denen Anmeldedaten von Open-Source-Entwicklern gestohlen wurden, um bösartigen Code in beliebte Bibliotheken hochzuladen. Da Open-Source-Repositories *de facto* zu einer kritischen Infrastruktur werden, werden zuverlässige Methoden zur Verifizierung und Validierung von Quellcode benötigt. Ziel des Forschungsprojekts „DEMISEC – Detecting Malicious Implants in Source Code“ ist daher die Erforschung und Evaluierung von Methoden und Techniken zum Schutz vor absichtlich implantiertem Schadcode in Drittanbieter- und Open-Source-Software.



Angreifer können Software kompromittieren, indem sie bösartigen Code in ansonsten harmlosen Quellcode einschleusen.

Das Team wird eine Kombination aus statischen und dynamischen Techniken verwenden, um dieses Ziel zu erreichen: Fuzzing oder symbolische Ausführung zum differenziellen Testen von Programmversionen und Modellieren von Code-Implantaten, um gefährliche Muster in Code-Repositories mithilfe statischer Analyse zu erkennen. In Zusammenarbeit mit dem µCSRL-Labor von Prof. Dr. Brunthaler untersucht das Forschungsteam „Quick-Vetting“ für die schnelle Attestierung von vorgeprüften Softwarekomponenten. Schließlich wird die Gruppe groß angelegte Studien zu Open-Source-Code durchführen, um die Projektergebnisse zu bewerten.

Einordnung von Angriffen

Im Rahmen des Projekts konnten bisherige Angriffe in vier große Kategorien eingeteilt werden: Typosquatting, also das Ausnutzen von Tippfehlern im Namen von Bibliotheken; Dependency Confusion, der unbeabsichtigte Import externer Bibliotheken; Malicious Commits, also bösartig eingefügter Code in legitimen Projekten; und Intrusions, also gezielte Angriffe auf die Systeme von Herstellern.

Das Projekt DEMISEC wird im Rahmen einer deutsch-israelischen Forschungskooperation im Auftrag des Bundesministeriums der Verteidigung (BMVg) durchgeführt. Auf israelischer Seite sind das Verteidigungsministerium, die Ben-Gurion-Universität des Negev (BGU) sowie weitere Forschungseinrichtungen beteiligt. Die Kooperation soll die Fähigkeiten beider Partner im Bereich Cyber Defence stärken, ist rein defensiv ausgerichtet und hat einen offenen Forschungscharakter.

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+49 89 6004 7335

www.unibw.de/patch

Gefördert durch: WTD81/BAAInBw

ABB.: FI CODE / 13SMOK@PIXABAY

Modellierung von Spectre-Angriffen

Mit einem axiomatischen Ansatz werden die Risiken spekulativer Ausführung sichtbar

Im Jahr 2018 erschütterten die Spectre-Angriffe die Welt der IT-Sicherheit mit der Nachricht, dass die spekulative Ausführung in den meisten modernen Prozessoren inhärente Schwachstellen verursacht. Das vorgestellte Projekt konzentriert sich auf die Definition neuer Semantiktypen für die spekulative Ausführung und den Aufbau von Tools zur Verifizierung von Software gegen Spectre und verwandte Angriffe.

Semantik von Mikroarchitekturen

Trotz vieler Erfolgsgeschichten bei der Anwendung formaler Sicherheitsmethoden waren spekulative Ausführungsangriffe lange außerhalb der Reichweite von Verifizierungstechniken, da sie die Rolle der Mikroarchitektur schlicht ignorierten. Heutzutage gibt es mehrere Ansätze, um Effekte der Mikroarchitektur in eine formale Semantik zu integrieren. Die meisten stützen sich jedoch auf eine operative Semantik, welche Beschreibungen des Zustands der Mikroarchitektur erfordert, was zu komplexen Modellen führt. Neu entdeckte Angriffe können eine Neugestaltung der gesamten Semantik erfordern, um die relevanten Effekte zu berücksichtigen. Aus diesem Grund haben Überprüfungstechniken Schwierigkeiten, mit dem Tempo Schritt zu halten, in dem neue Angriffe entwickelt und Gegenmaßnahmen vorgeschlagen werden.

Das Team präsentiert einen alternativen, leichtgewichtigen und axiomatischen Ansatz zur Spezifikation spekulativer Semantik, der sich auf Erkenntnisse aus Speichermodellen für Nebenläufigkeit stützt. Es verwendet die CAT-Modellierungssprache, die ursprünglich für Speicherkonsistenz entwickelt wurde (und seit 2017 von ARM für diesen Zweck übernommen wurde), um Ausführungsmodelle zu spezifizieren. Mit seinem modularen Ansatz ist CAT ideal geeignet, um eine Vielzahl von Angriffen zu erfassen, die spekulativen Kontrollfluss, Store-to-Load-Forwarding, Predictive Store Forwarding und Memory Ordering Machine Clears ausnutzen.

Von der Semantik zu Tools

Die Verwendung von CAT ermöglicht auf natürliche Weise die Modellierung verschiedener Arten von spekulativer Semantik unter Verwendung von Bounded Model Checking (BMC). Die Forscher schlagen ein einheitliches Analyse-Framework vor, das von einem in CAT definierten Mikroarchitekturmodell parametrisiert wird. Dieses Framework ist im Prototypen „Kaibyo“ implementiert. Die Experimente zeigen, dass die vorgeschlagenen Modelle präzise genug sind, um mehrere verschiedene Schwachstellen, die unterschiedliche Mikroarchitekturmerkmale ausnutzen, genau zu erkennen und zu beweisen, dass bekannte Gegenmaßnahmen wirksam sind. Gleichzeitig ermöglicht CAT die schnelle Erweiterung von Kaibyo auf neue Angriffe.

Der Ansatz schafft den ersten systematischen und werkzeuggestützten Rahmen, um spekulative Ausführung mit axiomatischer Semantik zu formalisieren. Die Forscher beschreiben das vorgeschlagene Semantik- und Analyse-Framework zusammen mit einer Bewertung seiner Aussagekraft und Genauigkeit in einem Artikel, der auf dem 43. IEEE Symposium on Security and Privacy (S&P), einem führenden Forum für IT-Sicherheit, erscheinen wird.

```
case_13:                        load_value:
        push    [esp+4]                 sub     esp, 16
        call    load_value              mov     eax, A.size
        add     esp, 4                  sub     eax, 1
        mov     edx, eax                and     eax, [esp+20]
        mov     eax, edx                mov     edx, eax
        movzx   eax, al                 mov     eax, edx
        movzx   edx, B[eax]             movzx   eax, A[eax]
        movzx   eax, temp               mov     [esp+15], al
        and     eax, edx                movzx   eax, [esp+15]
        mov     temp, al                add     esp, 16
        ret                             ret
```

Kaibyo kann Schwachstellen erkennen, die (unter anderem) auf die Ausführung von Instruktionen außer der Reihe zurückzuführen sind.

ABB.: MICHAEL STEINKE

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

Prof. Dr. Arno Wacker

Datenschutz und Compliance

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

EINES DER WICHTIGSTEN ZIELE der Professur für Datenschutz und Compliance 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 soll auch der breiten Öffentlichkeit demonstriert werden, dass datenschutzfördernde Technologien in den Alltag integrierbar sind, im privaten wie im geschäftlichen Bereich.

Lehre

Die Lehre in der Professur unterteilt sich in die Vorlesungen Penetrationstesting, Datenschutz, Privacy Enhancing Technologies, Kryptologie und Sichere Netze und Protokolle. Diese Vorlesungen vermitteln den Studierenden unter anderem, was Privacy ist und warum sie sowohl für Einzelne als auch für demokratische Gesellschaften von Bedeutung ist. Penetrationstesting behandelt das Überprüfen einzelner Systeme, komplexerer IT-Dienste und ganzer IT-Infrastrukturen sowie praxisrelevante Angriffsvarianten mit Orientierung an bewährten Good-Practice-Dokumentationen.

Es werden Grundlagen der Kryptographie sowie Wissen über die verschiedenen Methoden zur sicheren Datenübertragung in modernen Kommunikationsnetzen vermittelt.

Forschung

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

- Privatheit-unterstützende Mechanismen haben zum Ziel, die Privatsphäre des Einzelnen sowie die Erforschung von Kommunikationsregeln für das Internetzeitalter zu stärken.

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

Ein besonderer Fokus der Professur liegt auf Privatheit und den Datenschutz unterstützenden Maßnahmen.

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

Wissenstransfer

Ein besonderes Anliegen der Professur ist es, interessierte Bürgerinnen und Bürger fortzubilden, aufzuklären und in Fragen der IT-Sicherheit zu schulen und zu informieren. Diese Aufgabe verfolgt die Forschungsgruppe mithilfe von Vorträgen und Workshops, welche sich zum Beispiel mit Penetrationstesting, sicherem E-Mail-Verkehr im Alltag und dem Aufspüren von Sicherheitslücken befassen. Für Letzteres bietet die Professur beispielsweise einen Heartbleed-Webserver, auf welchem Interessierte versuchen können, in einer isolierten Umgebung genau diesen Bug auszunutzen.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

ABB.: ISTOCK / MATEJMO; ISTOCK/THITICHAYA YAJAMPA

Projekt Redundante Strukturen in verteilten Overlay-Netzen

Netzwerkresilienz durch Redundanz

Dieser Forschungsschwerpunkt beschäftigt sich mit passiven Sicherheitsmaßnahmen in verteilten Overlay-Netzen. Ziele sind die Analyse und Verbesserung der Widerstandsfähigkeit solcher Netze gegen Angriffe und technische Defekte. Dies geschieht, indem Redundanzen bezüglich Datenspeicherung und Konnektivität geschaffen und ausgenutzt sowie einzelne Ausfallpunkte entsprechend vermieden werden.

Overlay-Netze ohne zentralen Knoten.

DIE VERFÜGBARKEIT vieler Dienste im Internet hängt von einem zentralen Knoten und dessen Erreichbarkeit ab. Um eine hohe Verfügbarkeit sicherzustellen, wird der zentrale Knoten häufig in Form mehrerer Server mit Lastenausgleich, einer Vielzahl virtueller Serverinstanzen in einer Cloudinfrastruktur oder sogar ein oder mehrerer dedizierter Rechenzentren implementiert. Auch wenn der Betreiber möglicherweise umfangreiche Maßnahmen ergreift, können ein ausreichend schwerwiegender technischer Fehler, eine Fehlkonfiguration oder ein erfolgreicher Angriff zu einem nicht verfügbaren zentralen Knoten und damit zu einem nicht verfügbaren System führen. Abgesehen davon kann die Partei, die den zentralen Knoten kontrolliert, einfach entscheiden, ihn herunterzufahren, wodurch das System unbrauchbar wird. Probleme in einem zentralisierten Netzwerk können nicht nur in Bezug auf die Verfügbarkeit, sondern auch in Bezug auf Datenschutz und Zensur auftreten.

Ein zentraler Knoten, der an den Interaktionen zwischen anderen Knoten beteiligt ist, kann möglicherweise vertrauliche Informationen sammeln. Dies reicht von Metadaten, zum Beispiel, wer mit wem kommuniziert hat, bis hin zur vollständigen Kenntnis aller im System ausgetauschten Informationen. Darüber hinaus kann der zentrale Knoten als Relais zwischen anderen Knoten Zensur auf jede Kommunikation anwenden.

Eine andere Art der Organisation eines verteilten Netzwerksystems ist der vollständig dezentrale Ansatz, zum Beispiel in Form eines Overlay-Netzwerks im Internet. Hier existiert kein zentraler Knoten und daher kein einzelner Ausfall- oder Kontrollpunkt. Die Knoten des Systems sind in Bezug auf Routing, Kommunikation und andere Dienste oder Ressourcen gleich. Der Vorteil der Vermeidung des einzelnen Ausfall- oder Kontrollpunkts ist mit einem Nachteil in Form eines höheren Aufwands für Routing und Ressourcenlokalisierung verbunden. Während beim zentralisierten Ansatz die Interaktion mit dem zentralen Knoten für die Teilnahme ausreicht, erfordert der vollständig verteilte Ansatz häufig die Interaktion mit mehreren Knoten. Sowohl Identität als auch Anzahl dieser Knoten können von Interaktion zu Interaktion variieren.

Im Rahmen des Projekts werden die Schaffung und Ausnutzung von Redundanzen bei der Datenspeicherung und Netzwerkkonnektivität in verteilten Netzen untersucht. Hierdurch sollen einzelne Ausfall- und Kontrollpunkte vermieden, und die Wahrscheinlichkeit, dass Dienste nicht verfügbar sind oder zensiert werden, verringert werden. Das Ziel der Forschung ist die Verbesserung der Netzwerkresilienz großer, vollständig verteilter Systeme hinsichtlich gezielter Angriffe und technischer Fehler.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

ABB.: ISTOCK / METAMORWORKS

Projekt DECRYPT: Entschlüsselung historischer Manuskripte

Automatische Entschlüsselung von historischen Manuskripten

Ziel des Projekts ist es, ein neues, fachübergreifendes wissenschaftliches Feld der historischen Kryptologie zu etablieren. Indem verschiedene Disziplinen zusammengebracht werden, um Daten für einen schnelleren Fortschritt beim Entschlüsseln zu sammeln und Methoden auszutauschen, können historische Manuskripte entschlüsselt und kontextualisiert werden, welche bislang in Archiven und Bibliotheken verborgen sind.

FÜR UNSER KOLLEKTIVES Gedächtnis spielen handgeschriebene historische Aufzeichnungen eine Schlüsselrolle: Ohne sie wäre das Verständnis stark eingeschränkt. Ein besonderer Typ von handgeschriebenen historischen Aufzeichnungen sind verschlüsselte Manuskripte, sogenannte Chiffrate (Geheimtexte). Nach Schätzungen von Historikern ist ein Prozent des Materials in Archiven und Bibliotheken verschlüsselt oder codiert, und viele dieser Dokumente sind immer noch nicht enträtselt. Folglich bedarf es, während ein bedeutender Teil unseres kollektiven Gedächtnisses noch immer verborgen ist, einer großen Forschungsanstrengung, um sicherzustellen, dass dieses fehlende Wissen ans Licht gebracht und zur Förderung eines tieferen Verständnisses unserer gemeinsamen Geschichte genutzt wird.

Bisher arbeiteten Historiker und Sprachwissenschaftler zumeist individuell und unkoordiniert an der Identifizierung und Entschlüsselung dieser Dokumente. Dies ist ein zeitaufwendiger Prozess, da die Forschenden oft ohne Zugang zu automatischen Methoden arbeiten, die eine Entschlüsselung unterstützen und beschleunigen können. Gleichzeitig entwickeln Forschende aus den Bereichen Informatik, Kryptologie und Computerlinguistik automatische Entschlüsselungsalgorithmen zur Identifizierung und Entschlüsselung verschiedener Chiffrentypen, ohne Zugang zu verschiedenen Arten von echten Geheimtexten zu haben.

Ziel des Projekts ist es, ein neues, interdisziplinäres wissenschaftliches Feld der historischen Kryptologie zu etablieren, und zwar durch das Zusammenbringen des Fachwissens

In Bibliotheken und Archiven finden sich noch viele ungelöste Rätsel.

verschiedener Disziplinen. Durch das Sammeln von Daten und den Austausch von Methoden können schnellere Fortschritte beim Entschlüsseln und Kontextualisieren historischer Manuskripte erzielt werden, welche bisher in den Archiven und Bibliotheken verborgen sind.

Konkret wird das Projekt zu einer öffentlich zugänglichen Datenbank führen, die Tausende verschlüsselte Manuskripte und Verschlüsselungsschlüssel mit Informationen über ihre Herkunft und andere relevante Dokumente enthält. Durch das Zusammenbringen des Fachwissens der verschiedenen Disziplinen werden historische verschlüsselte Quellen digitalisiert, verarbeitet und entschlüsselt sowie Werkzeuge für die (halb-) automatische Entschlüsselung dieser Manuskripte über einen Webservice bereitgestellt.

Eine der hervorzuhebenden Punkte im Berichtsjahr 2021 ist der vorgestellte Angriff auf das Schlüsselgerät 41 von George Lasry. Das Schlüsselgerät 41 war eine Verschlüsselungsmaschine aus dem Zweiten Weltkrieg. Sie konnte damals von den Alliierten (Briten) in Bletchely Park nicht gebrochen werden. Die Maschine gilt als kryptographisch anspruchsvoll, selbst nach heutigen Maßstäben. Dies äußert sich auch darin, dass der von Lasry angewandte Lösungsansatz eine große Rechenleistung benötigt.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

Gefördert durch:
Swedish Research Council (SRC)

ABB.: ISTOCK / PASEVEN

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.

Projekt MuQuaNet

Münchens Quantennetzwerk

Das dtec.bw-Projekt MuQuaNet errichtet mithilfe der Technologien Quantenschlüsselaustausch (QKD) und Post-Quanten-Kryptographie (PQC) das erste quantensichere Netzwerk im Münchner Raum. Dabei analysiert es den Gewinn für die IT-Sicherheit und untersucht die Integration in existierende sichere Netzwerkarchitekturen. Zudem demonstriert das Projekt anhand ziviler und militärischer Anwendungsfälle die Nützlichkeit der Technologien QKD und PQC.

DAS AUFKOMMEN leistungsfähiger Quantencomputer stellt neben allen Fortschritten für die Wissenschaft auch eine ernstzunehmende Bedrohung für die heutigen Verschlüsselungsmethoden dar. Es gibt zwei wesentliche Möglichkeiten, dem entgegenzuwirken: die Post-Quantum Cryptography (PQC) und die Quantenschlüsselverteilung (Quantum Key Distribution, QKD). PQC beruht auf speziellen mathematischen Problemen, die allerdings (bisher) auch durch Quantencomputer nicht effizient lösbar sind. QKD benutzt dagegen einzelne Lichtquanten (Photonen), um gemeinsame Schlüssel an zwei Standorten zu erzeugen. Die Sicherheit gegenüber möglichen Abhörversuchen basiert hier auf den physikalischen Gesetzen der Quantenmechanik.

Infrastruktur des Quantennetzwerks

Das Projekt MuQuaNet errichtet das erste quantensichere Netzwerk im Großraum München und erforscht dieses in Bezug auf den möglichen Sicherheitsgewinn und die Praktikabilität der neuen Technologien QKD und PQC. Die Netzwerkknoten bilden die Partnerorganisationen ZITiS, LMU, Airbus, BWI und DLR sowie mehrere Institute der UniBw M (FI CODE, INF3, ETTI, dtec.bw). Verbunden werden diese über separate Dark-Fiber-Glasfaserverbindungen und QKD-Freistrahlstrecken. Im so entstehenden Netz werden unterschiedliche QKD-Geräte mit unterschiedlichen Protokollen eingesetzt. So soll es gelingen, die diversen Technologien miteinander zu vergleichen und ihre Nützlichkeit für die Zukunft einzuschätzen.

Schlüsselmanagement und Sicherheitsanalysen

IT-Sicherheit ist auch über QKD und PQC hinaus ein wichtiges Thema. Daher gilt es zu erforschen, wie beide in bereits bestehende sichere Netzwerkarchitekturen integriert werden können. Hierzu kommen Verschlüsselungsgeräte sowohl auf Layer 2 als auch Layer 3 des berühmten OSI-Schichtenmodells zum Einsatz. Mit allen damit verbundenen Themen sowie der Frage, wie die QKD-Schlüssel in den weiteren Schichten bis hin zur Anwendungsebene verwendet werden können, beschäftigt sich das Arbeitspaket Schlüsselmanagement.

Im Arbeitspaket Sicherheitsanalysen wird das Netzwerk durch Penetration Testing sowie das Ausloten möglicher Seitenkanalangriffe auf die Belastungsprobe gestellt und etwaige Schwächen des Netzwerks werden ausfindig gemacht. Zudem werden die theoretischen Sicherheitsbeweise der verwendeten Protokolle kritisch untersucht und weiterentwickelt.

Anwendungsfälle

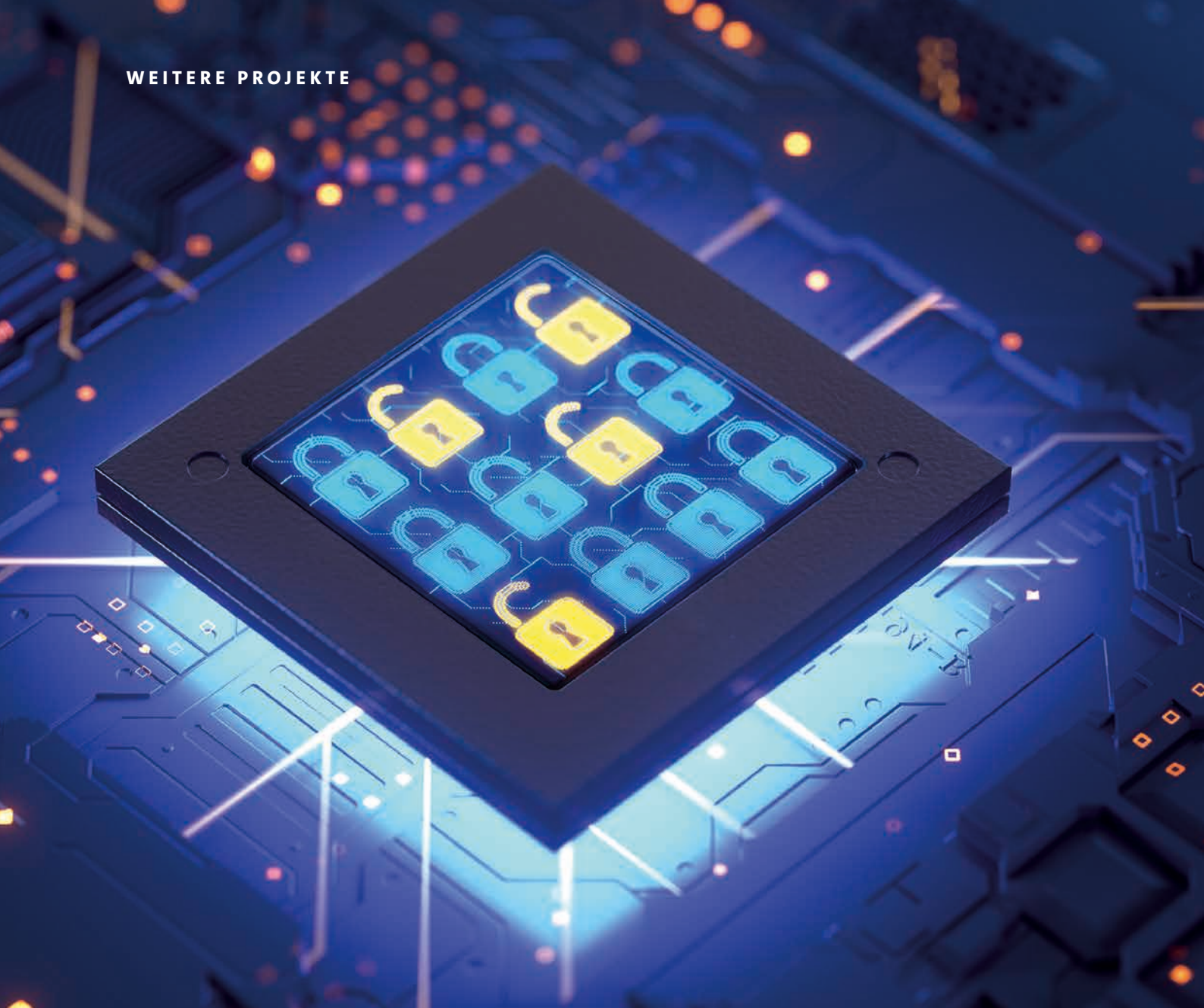
Ein Kernstück des Projekts sind die zivilen und militärischen Anwendungsfälle. Zu diesen gehört die quantensichere Fernwartung kritischer Infrastrukturen, beispielsweise einer Fregatte der Bundeswehr. Diese wird in MuQuaNet durch die Fernsteuerung eines Roboters als Proof of Concept demonstriert. Für die Echtzeitübertragung von Video- und Steuerdaten darf das Netz nur geringe Latenzen aufweisen und muss hohe Durchsatzraten ermöglichen. Noch höher sind die erforderlichen Raten beim zweiten Anwendungsfall, der Applikation ADRIAN, bei der etliche Terabyte schützenswerter, personenbezogener Daten quantensicher übertragen werden müssen. Abgerundet werden die Anwendungsfälle durch die Implementation von Usable Security sowie durch Wissenschaftskommunikation und -erziehung im Zusammenhang mit QKD.

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

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

ABB.: TAUSENDBLAUWERK.DE / MARKUS KRÄMER



Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

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

Projekt SW_GruVe

Mit mathematischen Beweisen zu sicherer Software – Anwendung von formaler Programmverifikation in industrieller Software-Entwicklung

Seit Jahrzehnten wird die Sicherheit von softwarebasierten Systemen durch Programmierfehler beeinträchtigt, trotz aller Methoden zu deren Vermeidung. Formale Programmverifikation verspricht dies zu ändern, erfordert aber einen extremen Aufwand für reale Programme. Im Projekt SW_GruVe erhöht das Team der Forschungsgruppe zusammen mit einem Industriepartner den Automatisierungsgrad von formaler Verifikation, um sie näher zur Praxis zu bringen.

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.

Die Werkzeuge

Formale Verifikation funktioniert am besten, wenn ein Programm von vornherein für dieses Ziel entwickelt wird, möglichst in einer dafür geeigneten höheren Programmiersprache. Im Vorgängerprojekt HoBIT untersuchte das Team die von Data61 und der University of New South Wales entwickelte Sprache Cogent als interessanten Kandidaten. Neben der Übersetzung von abstrakter Hochsprachen-Ebene in ausführbaren Code unterstützt Cogent die Verifikation, indem es automatisch einen „Refinement"-Beweis dafür generiert, dass sich das Ergebnis verhält wie spezifiziert.

Der Zielcode im Projekt ist C-Programmcode für Betriebssystemkomponenten, der durch den Projektpartner HENSOLDT Cyber aus seinem System TRENTOS bereitgestellt wurde. Im HoBIT-Projekt entwickelten die Forscherinnen und Forscher das Werkzeug Gencot für die teilautomatische Übersetzung von C nach Cogent. In SW_GruVe erweitern sie es zu einer vollautomatischen Übersetzung mit der Ausnahme von Sprungbefehlen. Durch die Übersetzung macht Gencot formale Verifikation anwendbar auf existierenden C-Code.

Uniqueness-Typen

Der von Cogent generierte Code verwendet Zeiger in einen gemeinsamen Speicher für effiziente Datenmanipulation. Um automatisch Äquivalenz mit einem funktionalen Programm zu beweisen, bei dem Werte nicht modifizierbar sind, verwendet Cogent ein „Uniqueness"-Typsystem. Wie die Sprache Rust unterstützt es eine statische Prüfung daraufhin, dass in Zeiger übersetzte Werte nie in verschiedenen Programmteilen genutzt werden, sodass keine unerwarteten Seiteneffekte auftreten können.

Gencot kann diese Eigenschaft nicht garantieren, wenn es ein C-Programm übersetzt. Stattdessen kann aber der Cogent-Compiler das Ergebnis statisch prüfen und alle Stellen finden, an denen sie verletzt wird. Nur diese Stellen erfordern manuelle Eingriffe.

Datenabstraktion

Gencot automatisiert den Übergang zwischen funktionalen Spezifikationen und ausführbarem Code, übersetzt aber die Datenstrukturen des C-Programms wie beispielsweise Arrays nicht in abstraktere Datentypen wie Abbildungen. In SW_GruVe ergänzt das Team Gencot durch ein Rahmensystem für die Abstraktion der übersetzten Datenstrukturen in Isabelle. Zusammen ergibt sich eine Methode zur relativ einfachen Überführung von C-Programmen in automatisch verifizierbare abstrakte Spezifikationen.

Als Praxis-Nachweis wurde Gencot erfolgreich auf TRENTOS-Komponenten angewendet. Gencot ist als Open Source auf GitHub verfügbar.

Prof. Dr. Gunnar Teege
gunnar.teege@unibw.de
+49 89 6004 3353
www.unibw.de/fomset

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

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

Kooperationen

Deutschland und die Welt

ABB.: ADOBE STOCK / BAIVECTOR / TAUSENDBLAU.WERK.DE

Nationale Partner

Das FI CODE arbeitet in Deutschland mit 47 Partnern in 34 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 47 Institutionen in 34 Städten und Gemeinden zusammen. Besondere Schwerpunkte liegen dabei auf Bayern bzw. dem Münchner Raum, Nordrhein-Westfalen und Hessen. ■

Institution	Ort
Universität Bayreuth	Bayreuth
govdigital eG	Berlin
Fachhochschule Bielefeld	Bielefeld
Ruhr-Universitat Bochum (RUB)	Bochum
Technische Universität Braunschweig	Braunschweig
Universität Bremen	Bremen
Technische Universität Chemnitz	Chemnitz
Hochschule Darmstadt	Darmstadt
Technische Universität Darmstadt	Darmstadt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE	Darmstadt
Technische Universität Dresden	Dresden
Universität Duisburg-Essen	Duisburg-Essen
secunet Security Networks AG	Essen
Frankfurt University of Applied Sciences	Frankfurt am Main
IDunion, Main Incubator GmbH	Frankfurt am Main
Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften	Garching
Helmut-Schmidt-Universität Hamburg	Hamburg
Technische Universität Ilmenau	Ilmenau

Institution	Ort
SoSafe GmbH	Köln
Universität Leipzig	Leipzig
Airbus Defence & Space	Manching
GESIS – Leibniz-Institut für Sozialwissenschaften	Mannheim
BWI GmbH	Meckenheim
Google München	München
Ludwig-Maximilians-Universität München	München
Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	München
FAST-DETECT GmbH	München
Rohde & Schwarz GmbH & Co. KG	München
Bayerisches Staatsministerium für Digitales (BayStMD)	München
Bayerisches Staatsministerium für Gesundheit und Pflege (BayStMGP)	München
H & D GmbH	München
Technische Universität München	München
Bayerisches Landesamt für Steuern (BayLfSt)	München/Nürnberg/Zwiesel
Friedrich-Alexander-Universität Erlangen-Nürnberg	Nürnberg
Bayerisches Landesamt für Sicherheit in der Informationstechnik (BayLSI)	Nürnberg
IABG Industrieanlagen-Betriebsgesellschaft mbH	Ottobrunn
Universität Paderborn	Paderborn
Weframe AG	Planegg
Max-Planck-Institut für Informatik, Saarland Informatik Campus	Saarbrücken
Fraunhofer Institut für Angewandte Informationstechnik (FIT)	Sankt Augustin
Universität Siegen	Siegen
Universität Stuttgart	Stuttgart
HENSOLDT Cyber GmbH	Taufkirchen
Airbus CyberSecurity	Taufkirchen
Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)	Wachtberg/Bonn-Bad Godesberg
Hessisches Landeskriminalamt	Wiesbaden
Bundeskriminalamt	Wiesbaden/Berlin

ABB.: TAUSENDBLAUWERK.DE


1 Hamburg
1 Bremen
2 Berlin
1 Braunschweig
1 Bielefeld
1 Paderborn
1 Duisburg
Bochum 1
Essen 1
1 Leipzig
1 Dresden
1 Chemnitz
1 Köln
1 Siegen
Sankt Augustin 1
1 Meckenheim
Bonn 1
1 Wachtberg
1 Ilmenau
2 Wiesbaden
Frankfurt/Main 2
Darmstadt 3
1 Bayreuth
3 Nürnberg
1 Mannheim
1 Saarbrücken
1 Zwiesel
1 Manching
1 Stuttgart
Garching 1
10 München
Ottobrunn 1
1 Planegg
Taufkirchen 2
Legende
1 Standort mit einem Partner
2 Standort mit mehreren Partnern
Standorte der Partner

Internationalität

Auch international pflegt CODE ein großes Netzwerk. Im Jahr 2021 stammten die Mitarbeitenden aus 15 Ländern. In 25 Ländern gab es 70 Kooperationspartner.

Mitarbeitende

Nationalität	Anzahl
Ägyptisch	2
Argentinisch	2
Bangladeschisch	1
Bosnisch	1
Brasilianisch/argentinisch	1
Britisch	1
Bulgarisch	1
Deutsch	100
Finnisch	1
Französisch	1
Kroatisch	1
Österreichisch	6
Slowenisch / Deutsch	1
Spanisch	1
Südkoreanisch	1

Internationale Kooperationspartner

Land	Partner
Ägypten	German University in Cairo
Australien	The University of Melbourne
	University of New South Wales
Belgien	EIT Digital
	KU Leuven
Dänemark	Aarhus University
Frankreich	Centre de Recherche de l'École de l'Air (CREA)
	Cyber-Detect
	INRIA/Université de Lorraine
	Université catholique de l'Ouest (UCO)

Land	Partner
Griechenland	Foundation for Research and Technology – Hellas
	ATHENA Research Center
	National Cyber Security Authority of the Ministry of Digital Governance
Großbritannien	Imperial College London
	Lancaster University
	University College London
	University of Glasgow
Israel	Ben-Gurion University of the Negev
Italien	Centro Ricerche Fiat
	Telecom Italia
	University of Insubria
	University of Milan
Kanada	evolutionQ Inc.
	University of Waterloo
Luxemburg	University of Luxembourg
Niederlande	Arthur's Legal B.V.
	SIDN – Stichting Internet Domeinregistratie Nederland
	SURFnet
	University of Twente
	Utrecht University
Norwegen	Norwegian University of Science and Technology
	Oslo Metropolitan University
	Telenor Group
	University of Oslo
Österreich	Österreichisches Bundesheer
	SBA Research
	Software Competence Center Hagenberg
Portugal	Efacec Electric Mobility
	University of Lisbon
Rumänien	Babeș-Bolyai University
	Bitdefender

Land	Partner
Schweden	Chalmers University of Technology
	Ericsson
	RISE – Research Institutes of Sweden
	University of Gothenburg
	Uppsala University
Schweiz	Ecole polytechnique fédérale de Lausanne
	ID Quantique SA
	RUAG
	Université de Lausanne
	University of St. Gallen
	University of Zurich
Slowenien	Jožef Stefan Institute
	University of Maribor
Spanien	Atos Spain S.A.
	CaixaBank
	Telefónica I+D
	Universitat Autònoma de Barcelona
Südkorea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Tschechische Republik	Flowmon Networks
	Masaryk University
Ungarn	Budapesti Műszaki és Gazdaságtudományi Egyetem
	Eötvös Loránd University
USA	Auburn University, Samuel Ginn College of Engineering
	Davidson College
	George C. Marshall European Center for Security Studies
	The University of Arizona, College of Engineering
	The University of North Carolina at Charlotte
Zypern	Cyprus University of Technology

ABB.: ISTOCK / BLUE PLANET STUDIO

Nachwuchs-förderung

Chancen und Angebote

ABB.: ADOBE STOCK / PICKUP

Studienpreis des Forschungsinstituts CODE 2021

Realitätsnahe Datensätze für die IT-Forensik

Mit dem Studienpreis des Forschungsinstituts CODE 2021 wurde der Absolvent des Masterstudiengangs Cyber-Sicherheit Martin Lukner ausgezeichnet. In seiner Arbeit beschäftigte er sich mit der Erzeugung von konfigurierbaren und realitätsnahen Datensätzen für die IT-Forensik.

MALWARE, also schädliche Software, spielt bei heutigen IT-Sicherheitsvorfällen eine zentrale Rolle. Zur Aufarbeitung dieser Vorfälle werden zuverlässige Tools und aktuelles Expertenwissen benötigt. Damit die Tools auf einer soliden Grundlage bewertet und Expertinnen und Experten für IT-Forensik realitätsnah geschult werden können, ist man auf fallspezifische Datensätze angewiesen. In diesem Bedarfsfeld bewegt sich Martin Lukners Arbeit mit dem Titel „Synthesis and evaluation of malware traces on Windows systems".

Individuelle Gestaltung von Malware-Spuren

Meist sind vorhandene Datensätze zu klein, veraltet oder können nur in bestimmten Fällen verwendet werden. Deswegen wurden in den letzten Jahren sogenannte „synthesis frameworks" entwickelt, um die benötigten Malware-Spuren automatisch zu erzeugen. In keinem dieser Frameworks ist es allerdings möglich, die Spuren nach bestimmten Vorgaben zu konfigurieren. Martin Lukner entwarf in seiner Arbeit daher eine Erweiterung für ein bereits an der Professur für Digitale Forensik von Prof. Dr. Harald Baier existierendes Framework, welches genau das erlaubt: Die neue Komponente für Malware ermöglicht es, Spuren nach individuellen Wünschen zu gestalten und trägt so zur Entwicklung vielfältiger Szenarien in verschiedenen Schwierigkeitsgraden bei. Erreicht wird dies, indem verschiedene Netzwerkprotokolle und Verschlüsselungsarten zum Einsatz kommen. Dabei werden sowohl Spuren im Netzwerk als auch auf Festplatten und im Arbeitsspeicher berücksichtigt.

Publikation auf einschlägiger Konferenz

Mit seiner Arbeit, die an der CODE-Professur für Digitale Forensik betreut wurde, leistet Martin Lukner einen wichtigen Beitrag dazu, konfigurierbare, fallspezifische, realitätsnahe Datensätze für die IT-Forensik zu erzeugen. Konzept, Implementierung und Evaluation seiner Arbeit sind ausgezeichnet. Sie wurde im Januar 2022 erfolgreich auf einer einschlägigen Konferenz für Digitale Forensik (Eighteenth IFIP WG 11.9 International Conference on Digital Forensics) unter dem Titel „On Realistic and Configurable Synthesis of Malware Traces on Windows Systems" als Publikation vorgestellt. ■

„Die Arbeit hat mir die Möglichkeit eröffnet, an einem wissenschaftlichen Projekt mitzuwirken, das nicht nur hochaktuell ist, sondern auch mehrere meiner Interessensgebiete kombiniert."

Preisträger Martin Lukner

Zur Aufarbeitung von IT-Sicherheitsvorfällen durch Malware werden zuverlässige Tools benötigt.

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

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

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 vermittelt, etwa zur Identifizierung und Beseitigung von sicherheitsrelevanten Schwachstellen, zur Entwicklung und Implementierung von Sicherheitskonzepten und zur Erkennung und Abwehr von Angriffen auf IT-Systeme. 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 Universität der Bundeswehr München. Voraussetzungen für die Förderung sind ein Studium (Bachelor oder FH) im MINT-Bereich sowie die erfolgreiche Teilnahme an einem Auswahlverfahren des Assessmentcenters 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

PROMOTIONEN 2021

Tanja Hanauer

„Visualization-based Enhancement of IT Security Management and Operations“

DIE ARBEIT „Visualization-based Enhancement of IT Security Management and Operations“ führt ein Prozessframework für die Visualisierung von Sicherheit ein. Sie unterstützt die Erstellung einer Übersicht, die Handhabbarkeit der IT einer Organisation, ihrer Prozesse, ausgewählter sicherheitsspezifischer Tasks und der Daten, auf denen diese basieren. Zusätzlich trägt die Arbeit zur organisationsweiten Erzeugung von Wissen durch einen Wissenstransfer zwischen Stakeholdern und zur Transformation von individuellem zu organisationsweitem Wissen bei. Es ist zu erwarten, dass die Anwendung des entwickelten Frameworks die Sicherheit verbessert.

Tanja Hanauer wurde im Februar 2021 bei Prof. Dr. Wolfgang Hommel promoviert. Während ihrer Promotion war sie am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften tätig. Derzeit arbeitet sie als Consultant für Informationssicherheit. ■

BEIDE ABB.: PRIVAT

Lorenz Liebler

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

DAS FELD der Speicherforensik ist ein wichtiger Zweig der digitalen Forensik. Verschiedene Konzepte ermöglichen es Praktikern, detaillierte Analysen von potenziell kompromittierten Systemen durchzuführen, indem sie den flüchtigen Speicher eines Ziels auswerten. Die Dissertation von Lorenz Liebler behandelt die (Wieder-)Erkennung digitaler Artefakte in einem gesicherten Hauptspeicherabbild. Liebler untersucht und entwickelt dabei den Ansatz des „Memory Carving“ weiter, das heißt, der Klassifikation digitaler Artefakte ohne Interpretation von Strukturdaten des Hauptspeichers (also ohne Verwendung von Informationen des Betriebssystems, beispielsweise über Prozesse, Handles, Sockets). Zentrales Thema der Arbeit ist die Konzeptionierung, Implementierung und Evaluation der Übertragbarkeit von Approximate-Matching-Funktionen auf den Bereich der Speicherforensik.

Lorenz Liebler verteidigte seine Dissertation am 7. Dezember 2021. Die Arbeit wurde von Prof. Dr. Harald Baier betreut. Liebler schloss im Oktober 2016 sein Masterstudium am Fachbereich Informatik der Hochschule Darmstadt ab, war dort anschließend Wissenschaftlicher Mitarbeiter und ist seit Ende 2020 bei einem privaten Cybersicherheits-Dienstleister tätig. ■

Hacking-Wettbewerb mit Spaß und Spannung

„Game of Trons“: Capture the Flag 2021

Im Herbst 2021 fand auf dem Campus der Universität der Bundeswehr München sowie online der 7. „Capture the Flag“-Hacking-Wettbewerb (CTF) des Forschungsinstituts CODE mit Unterstützung von ITIS e.V. und Team localos statt.

ENDE NOVEMBER kamen – selbstverständlich unter Einhaltung der geltenden Corona-Schutzmaßnahmen – 14 Teams, die das Online-Qualifying als Beste von 60 absolviert hatten, auf dem Campus in Neubiberg zusammen, um sich in verschiedenen Bereichen der Cybersicherheit zu messen. Weitere 15 Gruppen kämpften mit leicht verändertem Aufgabenspektrum um den Sieg im Onlinewettbewerb. 18 Stunden lang lösten die Teilnehmenden, darunter mehrere Studierendenteams, anspruchsvolle Challenges.

Von Forensik bis Virtual Reality: vielfältige Aufgaben

Wie üblich stand das CTF des FI CODE unter einem Motto, das Storyline und Gestaltung der Challenges bestimmte: Gemäß dem Veranstaltungstitel „Game of Trons" – eine Anspielung auf die erfolgreiche Fantasy-Serie „Game of Thrones" und das SciFi-Epos „Tron" – lautete die Zielvorgabe, Kontinente zu besiedeln und Herrschaft über diese zu erlangen.

Die insgesamt 49 Aufgaben kamen in diesem Jahr aus den Kategorien Krypto, Web, Forensik, Misc und Reversing/Pwning. Neben klassischen Herausforderungen, die meist auf echten Sicherheitslücken basierten, warteten auch außergewöhnliche Challenges auf die Teams: So wurden die Teilnehmenden durch eine Hardware-Challenge mit einem Oszilloskop oder eine Virtual-Reality-Challenge von Team localos herausgefordert. Insgesamt wurden 36 der gestellten Aufgaben erfolgreich gelöst.

And the winner is ...

Bis zum Schluss blieb es spannend, doch schließlich stand fest: Die vier glücklichen Gewinner gehörten dem Team „Nemesis" an. Platz 2 erreichte „Team T5", der dritte Platz ging an „Sabobatage". Den Online-Track konnten die „Careless Eagles" vor „0x90" und „Ignorital" für sich entscheiden. Zum Ende des Events gab es dann noch eine große Überraschung: Für das Siegerteam des On-Site-Tracks stiftete das SANS Institute EMEA, ein renommierter Anbieter von Cybersecurity-Trainings und -Zertifizierungen, insgesamt vier Gutscheine für einen On-Demand-Kurs. Das Forschungsinstitut CODE bedankt sich für den großzügigen Preis sowie für die Unterstützung diverser weiterer Partner aus der Industrie, die das Event in dieser Form erst möglich machte. ■

ABB.: FI CODE

In der Virtual-Reality-Challenge musste eine korrekte Befehlssequenz eingegeben werden, um Drachen abzuwehren und eine bedrohte Burg zu retten.

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 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 nicht nur Studierende ihr theoretisches Wissen anhand verschiedener praktischer Herausforderungen testen.

CODE-Geschäftsführer Volker Eiseler (l.) mit dem Siegerteam „Nemesis", das sich auf der sogenannten „Flag of Fame" verewigen durfte.

Mehr Informationen:

www.unibw.de/code/events/ctf

www.unibw.de/code/news/ctf-2021-game-of-trons

ctf@unibw.de

Addendum

Publikationen
Aktivitäten und
Organigramm

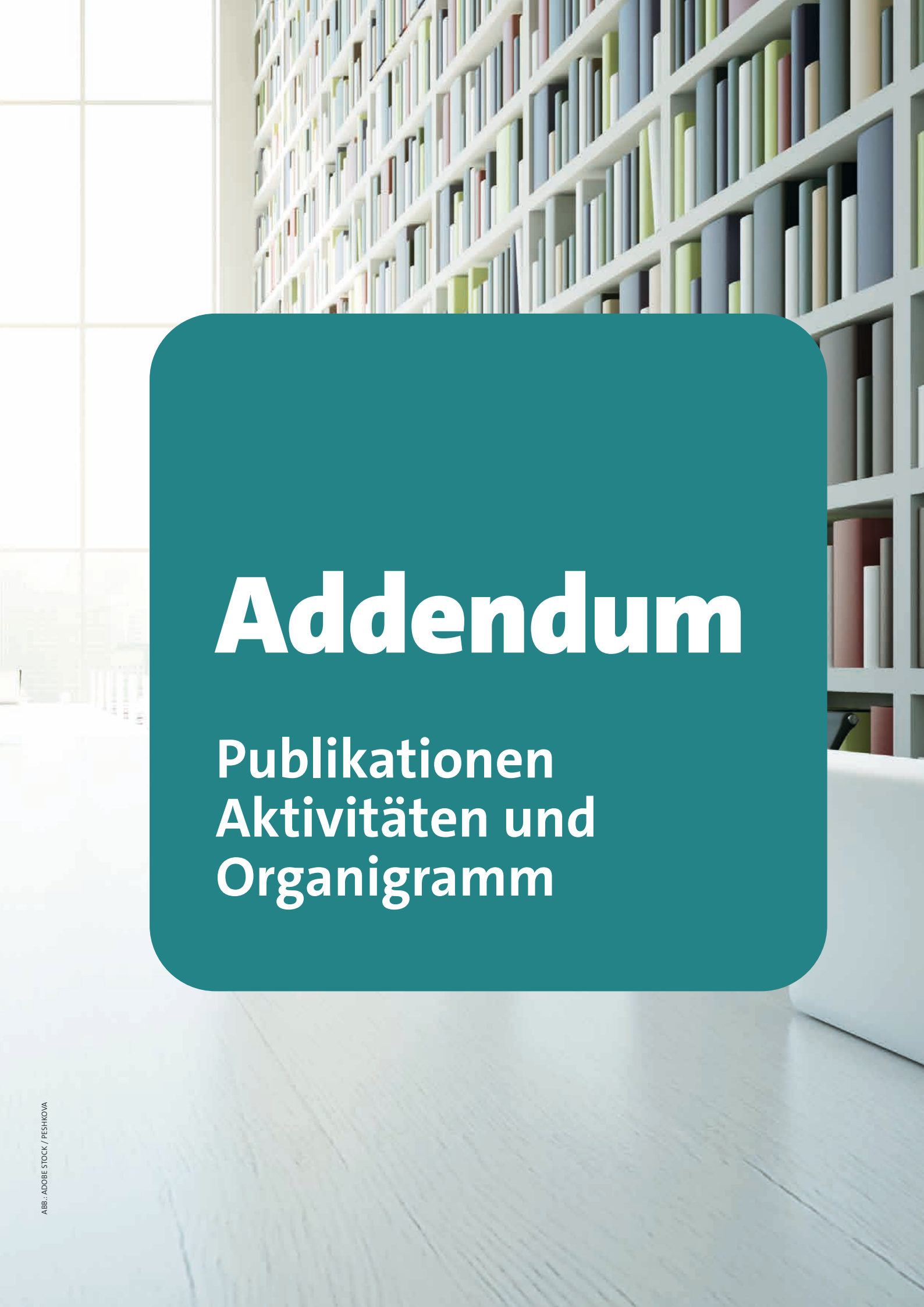


ABB.: ADOBE STOCK / PESHKOVA

Prof. Dr.
Florian Alt

Benutzbare Sicherheit und Privatsphäre

PUBLIKATIONEN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FORSCHUNGSPROJEKTE

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: 1/2019–7/2021

Scalable Biometrics

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

Gefördert durch: DFG
Laufzeit: 4/2020–3/2023

LEHRE

3665-V1 **Sichere Mensch-Maschine-Schnittstellen**

36651 **Benutzbare Sicherheit**

36653 **Praktikum Design sicherer und benutzbarer Systeme**

MESSEN, TAGUNGEN, SEMINARE

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

PREISE UND AUSZEICHNUNGEN

- Google Faculty Research Award 2021
- Designing Interactive Systems (DIS 2021) – Honorable Mention Award für den Beitrag: FROEHLICH, M., KOBIELLA, C., SCHMIDT, A., AND ALT F.: Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences.
- Mobile and Ubiquitous Multimedia (MUM'21) – Honorable Mention Award für den Beitrag: MARKY, K., PRANGE, S., MÜHLHÄUSER, M., AND ALT, F.: Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents.

WEITERE FUNKTIONEN

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

Prof. Dr. Harald Baier

Digitale Forensik

PUBLIKATIONEN

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

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

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

LEHRE

1162 **Digitale Forensik (WT)**

3824 **Digitale Forensik (HT)**

5501/1009 **Seminar Digitale Forensik (FT + WT)**

5501/1009 **Seminar Forensische Methoden der Informatik (HT)**

5505 **IT-Forensik (FT)**

MESSEN, TAGUNGEN, SEMINARE

- Vorbereitung und Moderation des CAST-Workshops Forensik/Internetkriminalität am 16.12.2021, URL: https://cast-forum.de/workshops/infos/302

WEITERE FUNKTIONEN

- Gutachter für „Journal of Digital Investigation" und „Computers & Security"
- Mitgliedschaft in Programmkomitees: Digital Forensics Research Workshop (DFRWS) EU 2021, CAST Förderpreis 2021, CAST-GI Promotionspreis 2021
- Unterstützung des Programmdirektors bei der Einrichtung des Studiengangs „IT Security" an der Vietnamese German University in Ho-Chi-Minh-Stadt, Vietnam

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

PUBLIKATIONEN

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

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

FORSCHUNGSPROJEKTE

ACSE (Airborne Cyber Security 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, Manching
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 Pilot (Dependable Production Systems Pilot Project)

Im Projekt „DEPS Pilot“ wurden wichtige Vorarbeiten für das Projekt DEPS durchgeführt, insbesondere eine Machbarkeitsstudie zur Erforschung, wie Software und Hardware gebunden werden kann.

Gefördert durch: Landesregierung Oberösterreich, Software Competence Center Hagenberg
Laufzeit: 2020–2021

DEPS (Dependable Production Systems)

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: 2021–2025

LEHRE

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

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

1010 **Maschinennahe Programmierung (WT)**

3647 **Compilerbau (WT + HT)**

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

MESSEN, TAGUNGEN, SEMINARE

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

PREISE UND AUSZEICHNUNGEN

Gewähltes Mitglied der Working Group 2.4 „Software Implementation Technology“ der IFIP

WEITERE FUNKTIONEN

- PC Member of IEEE Security & Privacy, 2022
- PC Member of AvioSE'22

Prof. Dr. Michaela Geierhos

Data Science

PUBLIKATIONEN

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

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

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

HÖLLIG, J., DUFTER, P., GEIERHOS, M., ZIEGLER, W., SCHÜTZE, H. (2021). Semantic Text Segment Classification of Structured Technical Content. In: Métais, E.; Meziane, F.; Horacek, H.; Kapetanios, E. (Hgg.): Natural

Language Processing and Information Systems (NLDB), Saarbrücken, 23.–25. Juni 2021. Cham: Springer. S. 165–177. LNCS 12801.

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

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

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

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

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

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

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

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

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

FORSCHUNGSPROJEKTE

SFB 901 „On-the-Fly Computing"

Teilprojekt „Parametrisierte Servicespezifikation"

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

Gefördert durch: Deutsche Forschungsgemeinschaft (DFG)
Laufzeit: 7/2019–6/2023

Quanten-Internet im Großraum München (MuQuaNet)

Teilprojekt „Authority-Dependent Risk Identification and Analysis in online Networks"

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

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr
Laufzeit: 10/2020–12/2024

KI-basierter Sprachsignal-Decoder

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

Laufzeit: 9/2021–12/2024

News-Artikel und Wissen (NAWI)

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

Laufzeit: 12/2021–11/2024

LEHRE

1009 **Wissensmanagement**

1144 **Knowledge Discovery in Big Data**

3850 **Natural Language Processing**

3851 **Information Retrieval**

3852 **Anwendungsgebiete der Data Science**

3853 **Analyse unstrukturierter Daten**

PREISE UND AUSZEICHNUNGEN

AI4HMO Best Paper Award

F. S. Bäumer und S. Denisov stellten einen Ansatz zur Überwachung und Analyse von Fitness-Apps vor, um Ziele von Cyberattacken zu identifizieren und deren Gefährdungsrisiko abzuschätzen.

WEITERE FUNKTIONEN

- Mitglied im Beirat „Deutsche Biographie" der Historischen Kommission bei der BAdW
- Gutachterin für die Alexander von Humboldt-Stiftung

Mitglied des Programmkomitees

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

Hon.-Prof. Dr. Udo Helmbrecht

Quanten-kommunikation

PUBLIKATIONEN

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

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

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

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

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

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

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

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

VERANSTALTUNGEN

Eingeladener Vortrag „MuQuaNet – The quantum network in the Munich area", Dr. Matthias Lienert, European Quantum Leadership Session 2: Quantum Communication, Aufzeichnung siehe www.youtube.com/watch?v=oLSxPuqt6-o, Quantum Business Network, Februar 2021.

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

PUBLIKATIONEN

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

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

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

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

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

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

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

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

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

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

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

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

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

FORSCHUNGSPROJEKTE

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

In diesem Projekt wird die in DISKURS begonnene wissenschaftliche Begleitung des Aufbaus und Betriebs der nationalen Identitätsföderation FINK fortgesetzt.

Zudem wird die technologische Weiterentwicklung von eID-Lösungen mittels Self-Sovereign Identity (SSI) Management analysiert. Dabei wird ein sicherer Umgang mit hochsensiblen personenbezogenen Daten sowie ein klarer Migrationspfad konzipiert.

Gefördert durch: Bayerisches Staatsministerium für Digitales (StMD)
Laufzeit: 4/2021–12/2022

Ledger Innovation and Operation Network for Sovereignty (LIONS)

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
Laufzeit: 1/2021–12/2023

Smart Hospitals – sichere Digitalisierung bayerischer Krankenhäuser

Rund 400 Krankenhäuser bilden in Bayern eine tragende Säule der Gesundheitsversorgung. Im Projekt wurde der Status quo ihrer technischen und organisatorischen IT-Sicherheitsmaßnahmen, insbesondere im Kontext aktueller Digitalisierungsvorhaben, erfasst. Die Erkenntnisse flossen in einen Maßnahmenkatalog zur weiteren Erhöhung des Sicherheitsniveaus ein, der aktuell in Ausgabe 2021/22 vorliegt.

Gefördert durch: Bayerisches Staatsministerium für Gesundheit und Pflege (StMGP)
Laufzeit: 10/2018–11/2021

ROLORAN – Resilient Operation of LoRa Networks

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

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr
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 Informationssicherheit im Gesundheitswesen (WT, HT)**

5501 **Seminar Sicherheitsaspekte von Wide Area Networks über LoRa (HT)**

5507 **Sichere vernetzte Anwendungen (FT)**

5508 **Sicherheitsmanagement (FT)**

MESSEN, TAGUNGEN, SEMINARE

Digitales Ich: Selbstbestimmte Identitäten im Netz. Veranstaltung des Blockchain Bayern e.V. und des Bayerischen Staatsministeriums für Digitales am 27.4.2021.

WEITERE FUNKTIONEN

- Studiendekan der Fakultät für Informatik (bis inkl. Januar 2021)
- Mitglied im Fakultätsrat INF
- Prüfungsausschuss Master of Intelligence & Security Studies
- Mitglied im Betriebsausschuss des Deutschen Forschungsnetzes
- Gutachter im österreichischen Forschungsprogramm Sparkling Science 2.0
- Mitglied im Programmkomitee:
  - IEEE Integrated Management (IM 2021)
  - IEEE International Conference on Communications (ICC 2021)
  - DFN-Konferenz Sicherheit in vernetzten Systemen 2021

Prof. Dr. Johannes Kinder

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

PUBLIKATIONEN

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

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

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

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

LEHRE

38191 **Reverse Engineering (FT)**

38192 **Praktikum Reverse Engineering (FT)**

55011 **Seminar Softwarehärtung (HT)**

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

55102 **Statische Programmanalyse (WT)**

55103 **Praktikum Fuzzing (WT)**

38491 **Dynamische Programmanalyse (HT)**

38492 **Praktikum Fuzzing (HT)**

PROGRAMMKOMITEES

- ACM Conference on Computer and Communications Security (CCS)
- IEEE Symposium on Security & Privacy
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
- GI Sicherheit
- Workshop on Offensive and Defensive Techniques in the Context of Man At The End attacks (CheckMATE)
- Workshop on Principles of Secure Compilation (PriSC)

WEITERE FUNKTIONEN

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

Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

FORSCHUNGSPROJEKTE

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

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

Gefördert durch: Airbus CyberSecurity
Laufzeit: 1/2021–12/2023

LEHRE

1016 **Einführung in Betriebssysteme**

5505 **Betriebssystemsicherheit**

Prof. Dr. Arno Wacker

Datenschutz und Compliance

PUBLIKATIONEN

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

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)**

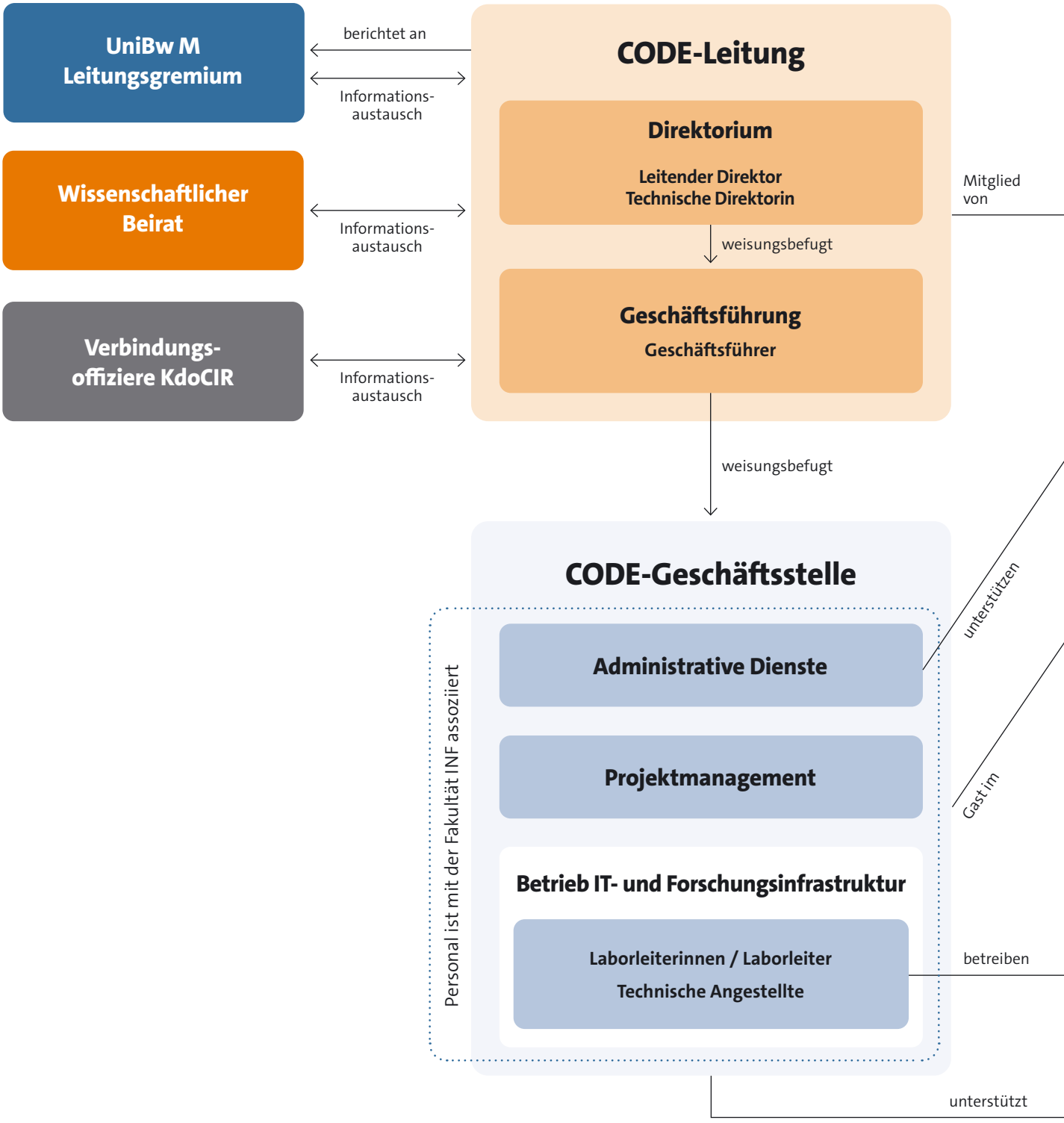
55091 **Penetration Testing (HT)**

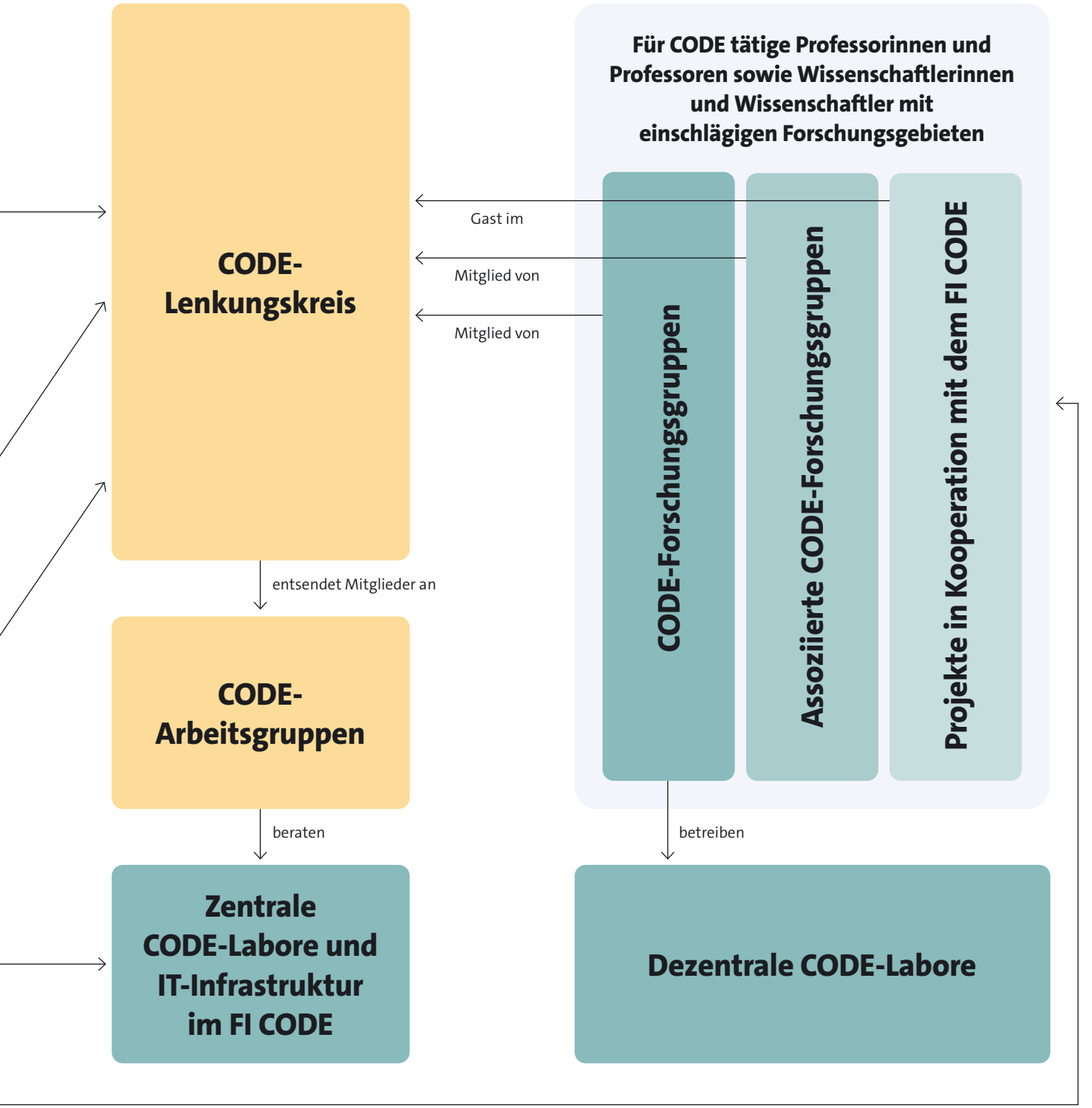
55093 **Praktikum Penetration Testing (WT + FT)**

WEITERE VERANSTALTUNGEN

- eingeladener (Online-)Vortrag am Gymnasium Ulricianum Aurich, 23.11.2021
  - Titel: „Einblicke in Kryptologie und IT-Sicherheit“
- eingeladener (Online-)Vortrag im Rahmen des Projekts „Schule & Zeitung“, 23.11.2021
  - Titel: „You‘re Being Watched – Tricks und Tools der Hacker“ Das Projekt Schule & Zeitung hat zum Ziel, durch die Beschäftigung mit dem Medium Tageszeitung die Medien- und Lesekompetenz der Schülerinnen und Schüler zu fördern. Die Jugendlichen sollen lernen, sich kritisch mit Medieninhalten auseinanderzusetzen.
- eingeladener Vortrag am Immobilientag IVD Mitte, Frankfurt/M, 30.9.2021
  - Titel: „You‘re Being Watched – Tricks und Tools der Hacker“
- ARD-alpha: „Wahlen im Visier von Hackern“, TV-Sendung, 22.6.2021
  - Prof. Dr. Arno Wacker zu Gast bei alpha-demokratie

Organigramm 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 (seit 11/2021);
Technischer Direktor (2/2021–10/2021);
Kommissarischer Leitender Direktor (10/2021)

Prof. Dr. Gabi Dreo Rodosek,
Leitende Direktorin (bis 9/2021)

Prof. Dr. Michaela Geierhos,
Technische Direktorin (seit 11/2021)

Prof. Dr. Udo Helmbrecht,
Technischer Direktor (bis 1/2021)

Dipl.-Inf. Volker Eiseler,
Geschäftsführer (bis 12/2021)

Marcus Knüpfer M. Sc.,
Kommissarischer Geschäftsführer (seit 1/2022)

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. Helmut Mayer,
Professor für Visual Computing

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 2021)

Aus der Fakultät für Informatik der
Universität der Bundeswehr München

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

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Wolfgang Hommel

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

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

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Weitere Mitglieder

Prof. Dr. Aiko Pras,
Universität Twente (NL)

Wolfgang Sachs,
Referatsleiter CIT I 2, Bundesministerium der Verteidigung

Dr. Norbert Gaus,
Executive Vice President der Siemens AG

Ralf Wintergerst,
Vorsitzender der Geschäftsführung der
Giesecke+Devrient GmbH

REDAKTION

Lisa Scherbaum M.A.,
Referentin für Öffentlichkeitsarbeit

ART DIRECTION

Tausendblauwerk, Agentur für Gestaltung
Michael Berwanger
www.tausendblauwerk.de

LEKTORAT

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

DRUCK

Holzer Druck und Medien
www.druckerei-holzer.de

REGULARIEN

Redaktionsschluss: März 2022

Titelabbildung: Adobe Stock / Digital art

ISBN: 978-3-943207-61-3 | ISSN: 2748-8780

Auch erschienen als elektronische Publikation
(ISBN: 978-3-943207-62-0 | ISSN: 2748-8799)
sowie in englischer Sprache
(ISBN: 978-3-943207-63-7 | ISSN: 2748-9485).


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