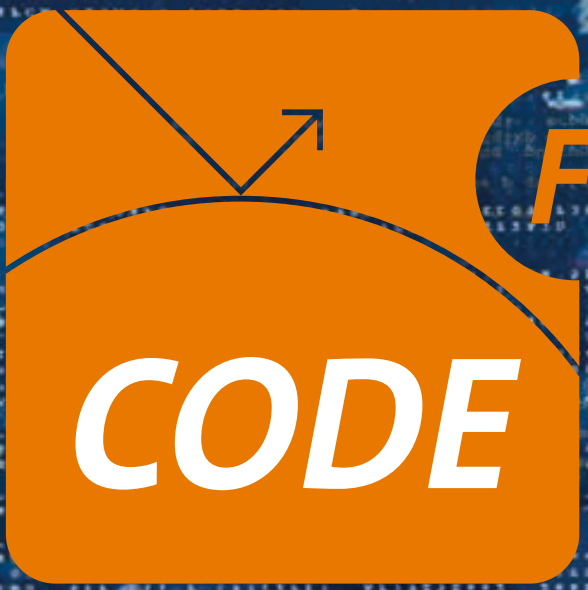
der Bundeswehr
Universität München

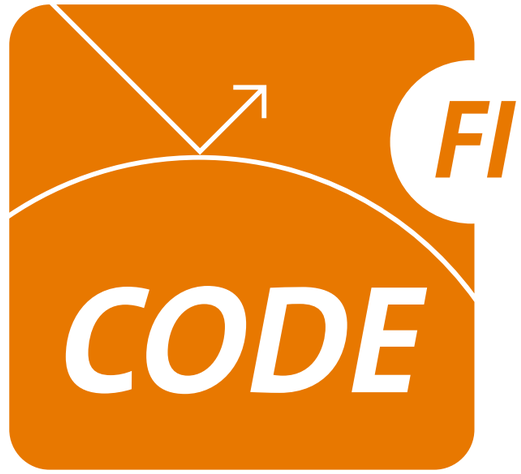


JAHRESBERICHT 2020

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Das Institut in Zahlen ▶▶▶

der Bundeswehr
Universität München



JAHRESBERICHT

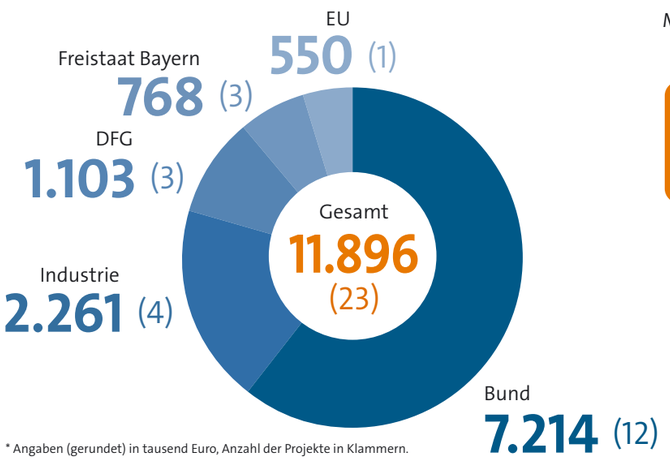
2020

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Projektförderung

2020 wurden insgesamt 23 drittmittelfinanzierte Projekte am FI CODE bearbeitet oder eingeworben. dtec.bw-Projekte erhalten Mittel aus dem Etat des Geschäftsbereichs BMVg.

Drittmittel*



* Angaben (gerundet) in tausend Euro, Anzahl der Projekte in Klammern.

dtec.bw-Projekt**

MuQuaNet – Das Quanten-Internet im Großraum München

MuQuaNet

Beteiligte Professuren

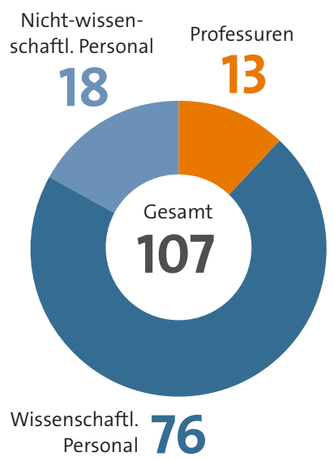
Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Florian Alt

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

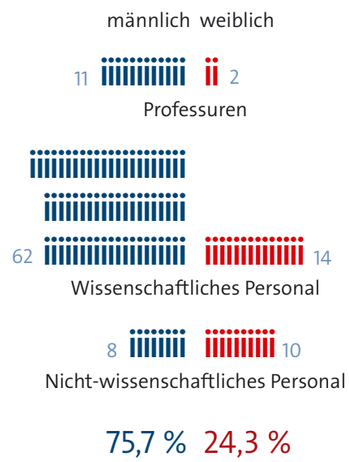
Personalstruktur

Das FI CODE hatte 2020 insgesamt 107 Mitarbeitende. Der Frauenanteil betrug 24,3 %.

Mitarbeitende



Geschlechteranteil



Forschungsarbeit

Übersicht der Promotionen und Publikationen am FI CODE 2020

Promotionen

4

Publikationen

65

Internationalität

Das FI CODE unterhält ein internationales Netzwerk.

Mitarbeitende***

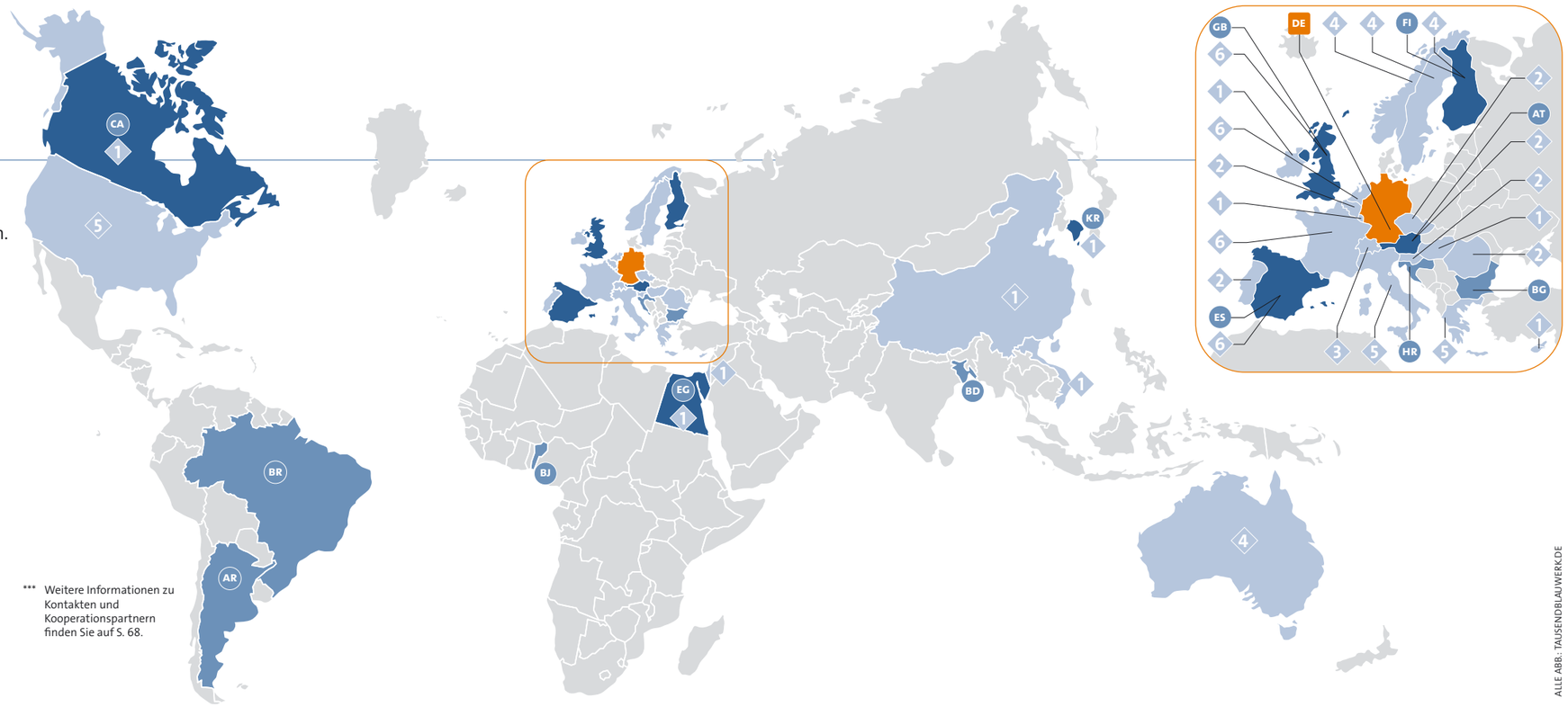
Die Mitarbeitenden stammten 2020 aus 14 Ländern.

Kooperationspartner***

2020 arbeitete das FI CODE mit 79 Partnern in 28 Ländern zusammen.

Legende

- Standort FI CODE
- AT – Herkunftsland von CODE-Mitarbeitenden
- 1 – Anzahl internationaler Kooperationspartner im betreffenden Land
- Länder mit Kooperationspartnern und Mitarbeitenden



*** Weitere Informationen zu Kontakten und Kooperationspartnern finden Sie auf S. 68.

ALLE ABB.: TAUSENDBLAUWERK.DE

Vorwort der Präsidentin

Wir leben in unsicheren Zeiten. Die Bandbreite der Bedrohungsszenarien weitet sich immer mehr aus, wie die Covid-19-Pandemie uns deutlich vor Augen führt. Die Universität der Bundeswehr München konzentriert sich mit ihren Forschungszentren dezidiert auf Themen der Sicherheit in Gesellschaft und Technik. 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 auf eine erfolgreiche Entwicklung in den letzten Jahren zurückblicken. Es wurde 2013 als Forschungszentrum gegründet und 2017 zum Forschungsinstitut des Bundes und der Bundeswehr ausgebaut. CODE ist eines der in Deutschland und Europa führenden Forschungsinstitute, wo sowohl grundlagen- als auch anwendungsorientierte Forschung in den Bereichen Cybersicherheit, Smart Data und Quantentechnologie betrieben wird. Zentrale Aufgabe des FI CODE ist der Aufbau eines europäischen Ökosystems, das die Zusammenarbeit von nationalen und internationalen Stakeholdern aus Forschung, Industrie, öffentlichen Einrichtungen, Start-ups und Risikokapitalgebern ermöglicht und erleichtert.

Es freut mich daher außerordentlich, dass die positive Entwicklung von CODE erstmals in einem umfassenden Jahresbericht abgebildet und dokumentiert werden kann, der Ihnen nun vorliegt. Die wachsende Bedeutung des FI CODE spiegelt sich auch in einer steigenden Zahl von Professuren, Forschungsgruppen sowie Mitarbeiterinnen und Mitarbeitern wider, denen ich weiter viel Erfolg bei ihrer spannenden Arbeit wünsche!

Mit besten Grüßen

Prof. Dr. Merith Niehuss
Präsidentin UniBw München

ABB.: PRIVAT; FI CODE

Liebe Leserinnen und Leser,

dieser erste Jahresbericht ist ein kleiner, aber wichtiger Meilenstein auf dem Wachstumskurs des Forschungsinstituts CODE. Er gibt einen spannenden Einblick in die umfangreichen Forschungsthemen sowie ausgewählte Projekte der am FI CODE beteiligten Professuren und informiert über unsere Highlights aus dem Jahr 2020.

Insbesondere freuen wir uns über unsere Neuzugänge: Prof. Dr. Michaela Geierhos hat seit April 2020 die Professur für Data Science, Prof. Dr. Harald Baier seit September 2020 die Professur für Digitale Forensik inne. Die Exzellenz und Sichtbarkeit des Forschungsinstituts CODE zeigt eine deutlich steigende Zahl an wissenschaftlichen Publikationen, Drittmittelprojekten und Kooperationen, abgeschlossene Promotionen in unseren noch jungen, aber international erfolgreichen Forschungsgruppen und der Aufwuchs unseres dritten großen Forschungsgebiets der Quantentechnologien.

Im Pandemiejahr 2020 fand unsere Jahrestagung unter dem Titel „Europe's Digital Sovereignty – Road to Success?" mit über 500 prominenten Gästen erstmals komplett digital und als Beitrag des BMVg zur deutschen EU-Ratspräsidentschaft statt. Es sprachen unter anderem die Bundesverteidigungsministerin Annegret Kramp-Karrenbauer und die Verteidigungsministerin der Niederlande Ank Bijleveld-Schouten, wofür wir uns herzlich bedanken möchten. Insgesamt waren die Vorbereitung und reibungslose Durchführung der Jahrestagung unter erschwerten Bedingungen ein Kraftakt, der nur dank des Engagements aller Angehörigen der CODE-Geschäftsstelle und der mitwirkenden Kolleginnen und Kollegen gelingen konnte.

Wir nutzen die Gelegenheit auch für einen herzlichen Dank an alle Unterstützer und Kooperationspartner, die allesamt dazu beitragen, dass das Forschungsinstitut CODE sein volles Potenzial entfaltet. Besonderer Dank gilt der Bundesverteidigungsministerin Annegret Kramp-Karrenbauer, dem Abteilungsleiter CIT Generalleutnant Vetter, dem Inspekteur CIR Vizeadmiral Dr. Daum, unseren direkten Ansprechpartnern im BMVg sowie der Leitung der UniBw M, deren Förderung die Grundlage unseres Handelns bildet.

Wir wünschen Ihnen eine unterhaltsame und interessante Lektüre und freuen uns auf die weitere Zusammenarbeit!

Prof. Dr. Gabi Dreo Rodosek *Prof. Dr. Wolfgang Hommel* *Volker Eiseler*
Leitung des Forschungsinstituts CODE

Inhalt

Highlights
Aus dem Institut

Forschung
Porträts und Projekte

Addendum
Publikationen und Aktivitäten

Kooperationen und Partner

Rubriken

ABB.: ISTOCK / ARCH-M3

Highlights

Aus dem Institut

ABB.: FORSCHUNGSZENTRUM JÜLICH / RALF-UWE LIMBACH

Zitat aus dem Programm zur deutschen EU-Ratspräsidentschaft: „Europa muss digital souverän werden, um auch zukünftig aus eigener Kraft handlungsfähig zu bleiben.“

ABB.: ISTOCK / NICOELNINO

Bericht zur Jahrestagung CODE 2020

Europäische digitale Souveränität: Weg zum Erfolg?

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

Die Jahrestagung CODE 2020 vom 10. bis zum 12. November stand im Zeichen der deutschen EU-Ratspräsidentschaft und fand unter dem Motto „Europe’s Digital Sovereignty – Road to Success?“ statt. Vor dem Hintergrund der COVID-19-Pandemie wurde die Tagung erstmals vollständig virtuell abgehalten. Das Forschungsinstitut CODE konnte auf diesem Weg über 540 Gäste begrüßen.

Europa: Digital souverän oder digitale Kolonie?

Alle zukünftigen global marktbeherrschenden Produkte und Dienstleistungen werden in der digitalen Welt, im Cyberspace, angesiedelt sein oder zumindest stark damit interagieren. Beispiele sind Robotik, Industrieautomation, autonomes Fahren, intelligente Stromnetze, Smart City und Smart Home. Die Welt wird „smarter“ und die IT die Basis unserer digitalen Gesellschaft. Digitale Technologien wie Big Data, Künstliche Intelligenz, autonome Systeme und cyberphysische Systeme erzeugen und verarbeiten die dabei anfallenden riesigen Datenmengen.

Europa steht heute für ein hohes Maß an Datensicherheit und Datenschutz. Die EU ist wahrscheinlich die vertrauenswürdigste Region der Welt, wenn es um diese Themen geht. Wirtschaftlich kann dies als ein bedeutender Wettbewerbsvorteil betrachtet werden, der beibehalten und ausgebaut werden muss. Doch wie digital souverän ist Europa? Und was ist der europäische Weg zur digitalen Souveränität? Diese Fragen sind auch im Kontext von Datensicherheit und Datenschutz zu betrachten.

Die Diskussionen und Beiträge der Jahrestagung des Forschungsinstituts CODE (FI CODE) der Universität der Bundeswehr München (UniBw M), CODE 2020, die vom 10. bis 12. November 2020 als digitale Konferenz durchgeführt wurde, beleuchteten unterschiedliche Aspekte dieser Themenstellung.

Der erste Tag der CODE 2020 mit hochrangigen Diskussionsrunden war ein Beitrag des Bundesministeriums der Verteidigung (BMVg) zur deutschen EU-Ratspräsidentschaft. Zitat aus dem Programm der deutschen EU-Ratspräsidentschaft[1]: „Europa muss digital souverän werden, um auch zukünftig aus eigener Kraft handlungsfähig zu bleiben.“ Doch was ist der europäische Weg?

Heutzutage beherrschen fast ausschließlich US-amerikanische sowie zunehmend chinesische, global agierende Unternehmen Daten und digitale Dienste. Wenn die Sicherheitsbehörden in Europa bei ihrer Auftragserfüllung immer stärker von Produkten und Dienstleistungen nichteuropäischer Akteure abhängig werden, bedroht das zukünftig nicht nur in einem Krisenfall die Handlungsfähigkeit des Staates.

In einer zunehmend globalisierten Welt präsentiert sich Europa als Vorreiter ethischer Werte; dies kann jedoch nicht die digitale Souveränität seiner Bürger oder Unternehmen garantieren. Auch aktuelle Herausforderungen im Bereich des Klimaschutzes und der Gesundheit, derzeit besonders im Hinblick auf die COVID-19-Pandemie, können nur mithilfe vertrauenswürdiger IT gelöst werden. Die Digitalisierung ist alternativlos.

Eine strategische Ausrichtung auf den Erhalt und Aufbau essenzieller Fähigkeiten für die Handlungsfähigkeit des Staates und seiner Einrichtungen ist wichtig, um den Schutz und die Sicherheit aller Bürgerinnen und Bürger auch in Zukunft gewährleisten zu können. Das bedeutet nicht zwangsläufig die Notwendigkeit einer Autarkie in allen Bereichen der Gesellschaft. Sie sollte jedoch stärker forciert werden in den Bereichen, die hohe Risiken für den Staat, die Gesellschaft und die Wirtschaft bergen. Gerade dort, wo wir uns auf andere verlassen müssen oder wollen, ist zwingend eigene Kompetenz nötig, um den Einsatz dieser Methoden oder Güter prüfen und regulieren zu können.

1) Auswärtiges Amt (2020): Gemeinsam Europa wieder stark machen – Programm der deutschen EU-Ratspräsidentschaft; 1. Juli bis 31. Dezember 2020; Quelle: www.eu2020.de/blob/2360246/d0e7b758973f0b1f56e74730bfdaf99d/pdf-programm-de-data.pdf

Prof. Dr. Gabi Dreo Rodosek, Leitende Direktorin des FI CODE, und Prof. Dr. Merith Niehuss, Präsidentin der UniBw M.

Schlüsseltechnologien und strategische Perspektiven der Digitalisierung

Generalleutnant Michael Vetter, Leiter der Abteilung Cyber- und Informationstechnik (CIT) und Chief Information Officer im Verteidigungsministerium, eröffnete die Konferenz und betonte die Wichtigkeit eines starken Europas, das seine Bürger schützen kann. Dabei steht die Stärkung der europäischen Resilienz mit dem Fokus auf digitaler Souveränität im Vordergrund. Digitale Souveränität und Cybersicherheit können nur durch die Zusammenarbeit von unterschiedlichen Akteuren, von der Forschung, Industrie und öffentlichen Institutionen bis hin zu Start-ups, erfolgreich umgesetzt werden.

Die Präsidentin der Universität der Bundeswehr München, Prof. Dr. Merith Niehuss, begrüßte über 500 online zugeschaltete Teilnehmende und gab einen kurzen Überblick über die aktuellen Entwicklungen im FI CODE.

Die Bundesministerin der Verteidigung, Frau Annegret Kramp-Karrenbauer, ging in ihrer Keynote auf unterschiedliche Aspekte der europäischen digitalen Souveränität ein. Dabei betonte sie unter anderem die Wichtigkeit der Zusammenarbeit, der Vernetzung und des Aufbaus von digitalen Ökosystemen und nannte hierbei explizit das EU-Projekt CONCORDIA mit derzeit über 55 Partnern, koordiniert durch das FI CODE, als ein wichtiges Programm zum Aufbau eines solchen europäischen digitalen Ökosystems. Die Nutzung vertrauenswürdiger IT, Minimierung der Abhängigkeiten von nichteuropäischer IT, Stärkung der digitalen Resilienz und Etablierung einer europäischen technologischen Führung sind nur einige Aspekte, die die Bundesministerin in ihrer Keynote in den Blick nahm.

Die Ministerin der Verteidigung der Niederlande, Ank Bijleveld-Schouten, betonte die Bedeutung eines starken und unabhängigen Europas. Ferner hob sie die enge Zusammenarbeit der deutsch-niederländischen Streitkräfte in der digitalen Welt hervor.

Prof. Dr. h. c. Wolfgang Ischinger, Vorsitzender der Münchner Sicherheitskonferenz, thematisierte in der Diskussion mit den Ministerinnen Wege zur Stärkung der europäischen digitalen Souveränität und stellte insbesondere die Relevanz von gegenseitigem Vertrauen am Beispiel der Initiative „Charter of Trust“ heraus.

Cybersicherheit als Voraussetzung für digitale Souveränität stand im Fokus des zweiten Panels, moderiert von Prof. Dr. Manfred Broy von der Technischen Universität München. Dabei diskutierten Juhan Lepassaar, Executive Director von ENISA, Vizeadmiral Dr. Thomas Daum, Inspekteur CIR, Ralf Wintergerst, Vorstandsvorsitzender von Giesecke+Devrient, Dr. Annegret Bendiek von der Stiftung Wissenschaft und Politik und Jeremy Jurgens vom World Economic Forum über die Herausforderungen der Cybersicherheit aus unterschiedlichen Perspektiven wie dem Aufbau eines europäischen Datenraums, Privatsphäre, Digitale Identitäten und Datenschutz.

Der erste Tag der CODE 2020 endete mit einer Paneldiskussion über zukünftige Schlüsseltechnologien als Basis der digitalen Souveränität, moderiert von Prof. Dr. Gabi Dreo Rodosek, der Leitenden Direktorin des FI CODE. Benedikt Zimmer, Staatssekretär des Bundesverteidigungsministeriums, betonte, wie wichtig die Verfügbarkeit von vertrauenswürdiger IT für die Handlungsfähigkeit der Streitkräfte ist. Dr. Angelika Niebler, Mitglied des Europäischen Parlaments, und Jiří Šedivý, Chief Executive der European Defence Agency, stellten ihre Perspektive hinsichtlich des Aufbaus und der Förderung europäischer Schlüsseltechnologien dar. Stefan Winners, Berater bei Lakestar, einer europäischen Venture-Capital-Gesellschaft, erläuterte seine Sicht auf Investments in Schlüsseltechnologien und die größten Hindernisse, die dazu führen, dass Europa über keine großen IT-Champions verfügt. Die abschließende Frage an alle Diskutierenden war: „Was ist der Weg, die Roadmap, um ein digital souveränes Europa aufzubauen?“ – „Kooperation, Zusammenarbeit und Vertrauen“, lautete die einvernehmliche Antwort.

Wegbereiter der digitalen Souveränität

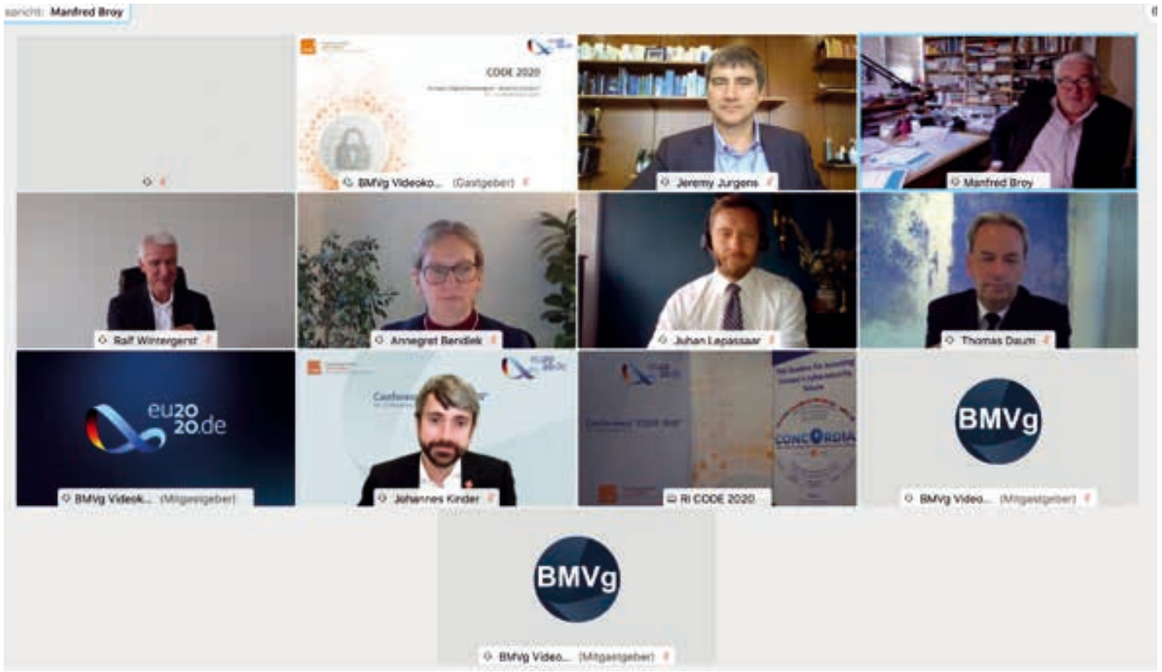
Am zweiten Tag der CODE 2020 fanden parallel sieben Workshops statt, die einen fachlich tiefgehenden, intensiven Austausch zwischen den Experten zu aktuellen Fragestellungen ermöglichten. Die unterschiedlichen Themen, die in den Fachworkshops eingehend vorgestellt und diskutiert wurden, verdeutlichen die zahlreichen Herausforderungen, die es auf dem Weg zu einer europäischen digitalen Souveränität zu bewältigen gilt. An den virtuellen Workshops beteiligten sich insgesamt knapp 300 Teilnehmerinnen und Teilnehmer aus Europa – ein neuer Rekord. Stellvertretend werden nachfolgend die Höhepunkte von zwei der Workshops 2020 zusammengefasst.

Workshop „Cyber Resilience of Critical Infrastructures“

Der Workshop thematisierte die Resilienz kritischer Infrastrukturen in systemischen Verbindungen komplexer

BEIDE ABB.: UNIBW M

Bundesverteidigungsministerin Annegret Kramp-Karrenbauer ging in ihrer Keynote auf unterschiedliche Aspekte der europäischen digitalen Souveränität ein.



Cybersicherheit als Voraussetzung für digitale Souveränität stand im Fokus des zweiten Panels der CODE 2020.

cyberphysischer Systeme. Ein besonderer Fokus lag hierbei auf dem Bereich der Wirtschaft und auf unterschiedlichen Ansätzen von Unternehmen, mit neuartigen Bedrohungsszenarien der Cybersicherheit umzugehen. Inhalt waren auch die Auswirkungen von Angriffen auf für staatliche Sicherheit relevante Einrichtungen, insbesondere die Bundeswehr. Künstliche Intelligenz im Bereich des Internet of Things (IoT) wurde als eine Möglichkeit zur Verbesserung der Cyber-Resilienz genannt, hier insbesondere durch Prädiktion.

Als größte Herausforderungen im Bereich Cyber-Resilienz schätzen die Teilnehmerinnen und Teilnehmer es ein,

a) Best-Practice-Beispiele mit relevanten Stakeholdern zu teilen,
b) den sicheren und schnellen Austausch von Daten zu ermöglichen.

Das Logo der EU-Ratspräsidentschaft 2020.

Workshop „Quantum Technology“

Der Schwerpunkt dieses Workshops lag auf Quanten-Computing und Post-Quanten-Kryptographie (PQC). Einerseits sind Quanten-Computing und dafür verwendete Hardware ein direktes Resultat der Anwendung von quantenmechanischen Effekten. Andererseits ist PQC eine Verbesserung von bisherigen klassischen kryptographischen Methoden, welche nun potenziellen Angriffen durch Quantencomputer standhalten müssen. Die Theorie von Quantenschaltkreisen bildet die Grundlage zum Verständnis für gegenwärtig verfügbare Hardware.

Die Algorithmen von Lov Grover und Peter Shor aus den 1990er Jahren sind noch immer die besten Beispiele für die Effektivität eines Quantenansatzes. Beide Methoden bringen sowohl symmetrische als auch asymmetrische Kryptographie in Gefahr, wobei Letztere in Form von ECC[2] und RSA[3] stärker betroffen ist. Darum läuft ein NIST[4]-Prozess zur Standardisierung von neuen Methoden zur Verbesserung von gegenwärtigen digitalen Signaturen, Schlüsselaustauschprotokollen und Kryptographie mit öffentlichen Schlüsseln.

2) Elliptische-Kurven-Kryptographie
3) Asymmetrischer Verschlüsselungsalgorithmus
4) National Institute of Standards and Technology, USA

IBM legte erst kürzlich einen anspruchsvollen Fahrplan für Geräte mit mehr als 1.000 Qubits bis zum Jahr 2023 vor. Dieser Meilenstein könnte endgültig die Tür zu einer besseren Fehlerbehandlung und -korrektur öffnen. Daher wird man PQC wohl eher früher als später anwenden müssen.

Innovation als Voraussetzung für digitale Souveränität

Der Nachmittag des zweiten Tags der CODE 2020 war der Innovationstagung zum Themengebiet Cyber- und Informationstechnologie gewidmet. Nach ihrer Einführung 2018 fand sie nunmehr zum dritten Mal statt. Bernd Schlömer vom BMVg-Referat CIT I 2, das für Forschung und Technologie sowie Innovationsmanagement Cyber/IT zuständig ist, erläuterte in seiner Rolle als Juryvorsitzender einführend die Zielsetzung, 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.

Aus mehr als 30 Einreichungen zur Innovationstagung wählte das Organisationsteam zwölf zur Präsentation im Rahmen von Pitches, also auf eine Dauer von maximal sieben Minuten begrenzten Kurzvorträgen, aus. Auf Basis der Kurzvorträge und anschließenden Diskussionen wurden die drei besten der zwölf Beiträge, die allesamt ihre Relevanz unter Beweis gestellt haben, bestimmt.

Trotz der Individualität jedes Beitrags war erkennbar, dass 2020 der Einsatz von Machine Learning – unter anderem zur Identifikation von Fake News und zur Entscheidungsunterstützung –, die fein granulierte Segmentierung von Datennetzen zur Platzierung technischer Sicherheitsmaßnahmen und die Auswertung von im Internet frei zugänglichen Daten im Sinne der Open Source Intelligence Schwerpunkte der vorgestellten Innovationen darstellten.

Über den dritten Platz freute sich Tobias Appel vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften, der für seinen Beitrag zur automatisierten Erfolgsprüfung beim Einsatz von Exploits im Rahmen von Penetrationstests der eigenen IT-Infrastruktur ausgezeichnet wurde. Der zweite Platz ging an Michael Grytz von der HENSOLDT Sensors GmbH für die Vorstellung von I-unHYDE, einem KI-basierten Werkzeug zur Aufdeckung und Analyse von Desinformationskampagnen. Den ersten Platz belegten Ingmar Heinrich und Ulf Schröter von der Rheinmetall Electronics GmbH, die einen Ansatz zur Moving Target Defence in mikrosegmentierten Zero-Trust-Netzen vorstellten. Alle Teilnehmer bekamen die Gelegenheit, ihre Innovationen im Nachgang zur Tagung ausgewählten Zielgruppen noch ausführlicher zu präsentieren.

ABB.: UNIBW M; EU

Digitale Souveränität erfordert digitale Kompetenzen

2020 fand im Rahmen der CODE-Jahrestagung erstmalig der „Science Track“ statt, der jungen Doktorandinnen und Doktoranden ein Forum zum wissenschaftlichen Austausch und Netzwerken bieten soll. Die Veranstaltung gliederte sich in zwei Teile: 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 zu können, während der zweite Programmpunkt einen Erfahrungsaustausch zwischen weiter fortgeschrittenen Doktorandinnen und Doktoranden mit ihren jüngeren Pendants ermöglichte.

Insgesamt wurden sieben Vortragende im Rahmen eines wissenschaftlichen Begutachtungsprozesses ausgewählt. Thematisch bot das Programm verschiedene Inhalte aus dem Bereich der IT-Sicherheit und erstreckte sich von sehr technischen Vorträgen auf der Ebene von Maschinenbefehlen bis hin zu semantischen Analysen sozialer Netzwerke oder Aspekten der Visualisierung im Rahmen der Ausbildung.

Prof. Dr. Aiko Pras von der Universität Twente, Prof. Dr. Gabi Dreo Rodosek und Prof. Dr. Florian Alt vom FI CODE begleiteten die Diskussion wissenschaftlich. Die Veranstaltung erfreute sich auf Anhieb großer Beliebtheit und konnte mit über 80 Zuhörern trotz der rein virtuellen Form einen guten Auftakterfolg erzielen. Der „Science Track“ der CODE-Jahrestagung trägt auch 2021 zum Aufbau der wissenschaftlichen Community bei und unterstützt junge Wissenschaftlerinnen und Wissenschaftler auf ihren Karrierepfaden.

Mehr Informationen zum Thema:

www.unibw.de/code/events/jahrestagungen

www.eu2020.de

www.youtube.com/c/FZcodeDeubw

Quantentechnologien

Get Quantum ready

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

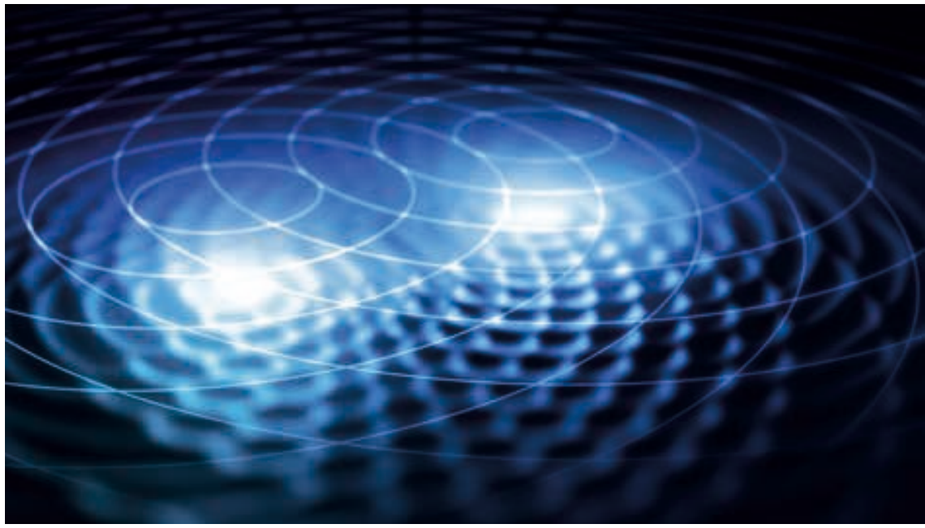
Quantentechnologien bilden die Basis für moderne Technik wie Mikrochips, Breitbandinternet oder Satellitennavigation. Effekte wie Quanteninterferenz und Quantenverschränkung sind erst heute technologisch nutzbar und bieten das Potenzial für völlig neue technische Lösungen wie Quantencomputer, Quantensensoren und -metrologie, Quantenkryptographie und -kommunikation sowie Quantensimulation. Am Forschungsinstitut CODE forschen wir in den Gebieten Quantencomputing und Quantenkommunikation. Aber auch die Post-Quanten-Kryptographie ist Forschungsthema am FI CODE: Diese beschäftigt sich mit der Entwicklung neuer Verfahren zum Schutz von Daten und der Kommunikation vor Bedrohungen durch Quantencomputer.

Quantencomputing

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.

Theoretische Arbeiten haben gezeigt, dass – verglichen mit den besten bekannten klassischen Algorithmen – bestimmte strukturierte Probleme mit Quantenalgorithmen exponentiell schneller berechnet werden können. Die Rechenoperationen werden dabei mit Qubits durchgeführt. Ein Qubit ist die kleinste Informationseinheit eines Quantencomputers – ein quantenmecha-

Diese Seite: Der Ursprung der Quantenbeschleunigung liegt darin, dass Quantencomputer Interferenzen zwischen den Berechnungspfaden zulassen.



Links: IBM Q auf der Consumer Electronics Show 2020. Das IBM Q Network umfasst inzwischen über 100 Organisationen.

ABB.: IBM / ANDREW LINDEMANN; ISTOCK / PETROVICH9

nisches 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.

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 bemerkenswerten jüngsten technologischen Fortschritten besteht nun die Möglichkeit, Quantenalgorithmen und Quantenheuristiken auf kleinen Quantencomputern zu testen.

Obwohl die Quantenhardware ständig verbessert wird, ist sie aktuell noch fehler- und rauschanfällig. Durch Wechselwirkung mit der Umgebung oder Rauschen werden die Superpositionszustände gestört. Dies führt zum Verlust der Interferenzeffekte. Ein wichtiges Ziel ist es, die Zeit, für die der Superpositionszustand aufrechterhalten bleibt, möglichst zu maximieren und so die Fehlerraten zu minimieren. Liegen diese unterhalb eines bestimmten Schwellenwerts, können nicht nur längere Quantenberechnungen ausgeführt werden, sondern mithilfe von Fehlerkorrektur sogar beliebig lange Berechnungen mit beliebig guter Genauigkeit durchführt werden.

Das berühmte Doppelspaltexperiment.

Eine Fehlerkorrektur ist aufgrund der Hardware-Anforderungen derzeit noch schwierig zu implementieren, doch die Minderung von Fehlern zur Verbesserung des Signal-Rausch-Verhältnisses ist möglich. Zentral für die weitere Forschung und Entwicklung sind neben der Hardwareverbesserung deshalb die hardwarebasierte Programmierung mit Fehlerminderungsverfahren, die Entwicklung neuer Heuristiken für Optimierungsanwendungen sowie die Modellierung und Simulation komplexer Systeme auf Quantencomputern.

IBM Q-Hub am FI CODE

Das Forschungsinstitut CODE beschäftigt sich seit mehreren Jahren wissenschaftlich mit Anwendungen, die mit universellen Quantencomputern umsetzbar sind. Zusätzlich werden künftig auch militärische Lagebilder und Szenarioanalysen weitere Anwendungsfälle in der Forschung im Bereich Quantencomputing am FI CODE sein. Gemäß der Planungsweisung 2022 des BMVg sind die Bereiche Quantentechnologie (QT), Digitalisierung und Innovationsfähigkeit Schlüsselaspekte für die Umsetzung eines zukunftsorientierten Personalmanagements. Die militärische Nutzung der Quantentechnologie soll unter anderem vom FI CODE in Verbindung mit der mittelfristigen Beschaffung eines Quantencomputers (QC) sowie der Administration eines QC-Hubs sichergestellt werden.

Seit 2018 betreibt das FI CODE an der Universität der Bundeswehr München (UniBw M) als Mitglied des IBM Quantum Network einen von weltweit nur 16 exklusiven Zugängen zur IBM-Quantencomputer-Infrastruktur als sogenanntes IBM Q-Hub. Die derzeitige Verfügbarkeit von kleinen, mit Rauschen behafteten Quantencomputern (20–65 Qubits) ermöglicht es den Forscherinnen und Forschern am CODE, Quantenalgorithmen und -heuristiken sowie Fehlerminderungsschemata zu testen.

Neben dem maschinellen Lernen sind Vielteilchenphysik und Optimierung mit hybriden Variationsalgorithmen die vielversprechendsten ersten Anwendungen. In Zukunft werden weitere Quantenheuristiken entwickelt und im Rahmen von möglichen Anwendungsfällen getestet. Darüber hinaus arbeiten die Wissenschaftlerinnen und Wissenschaftler an einer Vielzahl von Methoden zur Fehlervermeidung.

Kontaktinformationen zum IBM Q-Hub:

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

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

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

IBM Q Computation Center.

ABB.: ISTOCK; IBM / ANDREW LINDEMANN

Quantenkommunikation

Sichere Kommunikation über das Internet ist eine wesentliche Voraussetzung für eine vertrauensvolle Zusammenarbeit in allen Bereichen unserer Gesellschaft. Anwendungen, Daten, Nachrichten, Telefonate oder E-Mails müssen vor dem Zugriff unbefugter Dritter im Internet geschützt werden. Leistungsfähige, universelle Quantencomputer, die bereits in ersten Testversionen verfügbar sind, würden praktisch alle heute eingesetzten Public-Key-Verschlüsselungs- und Schlüsselaustauschverfahren unsicher machen. Um im Sinne eines angemessenen Risikomanagements vorbereitet zu sein, müssen die Vorbereitungen für die „Post-Quanten-Zeit“ bereits heute beginnen. Betroffen sind dabei Vertraulichkeitsdienste mit einem langfristigen Schutzbedarf, wie zum Beispiel Programme zum Austausch persönlicher Nachrichten, Videokonferenzen oder Onlinebanking, sowie Signaturzertifikate mit langen Laufzeiten. Damit die staatliche Souveränität erhalten bleibt, muss die sensible und zum Teil als geheim eingestufte militärische Kommunikation besonders abgesichert werden.

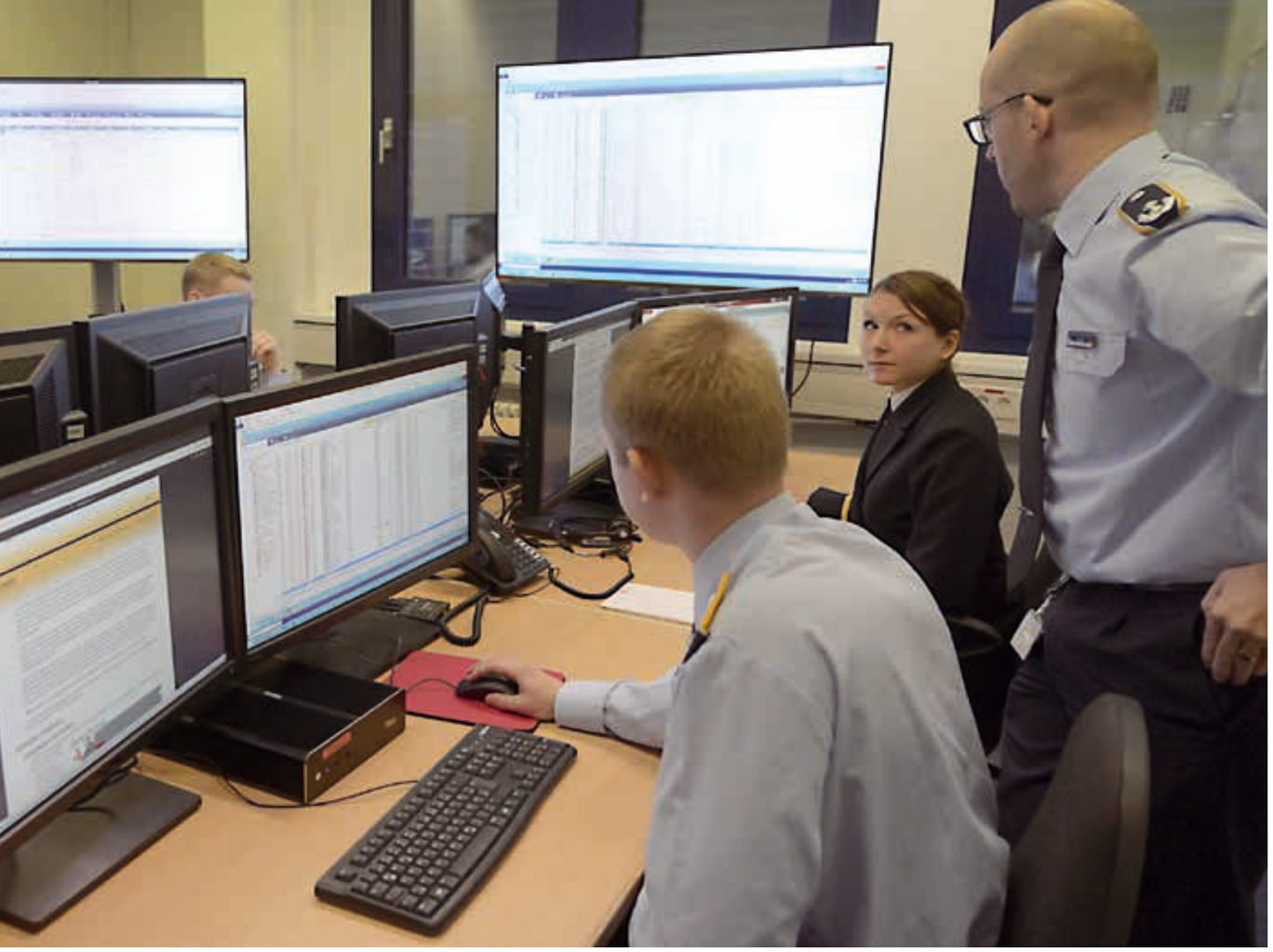
Quantum Key Distribution (QKD, Verteilung von Quantenschlüsseln) ist ein Verfahren, das die physikalischen Eigenschaften der Quantenmechanik nutzt, um zwei oder mehreren Parteien einen gemeinsamen, sicheren Schlüssel für die Kommunikation zur Verfügung zu stellen. Der Vorteil des Quantenschlüsselaustauschs gegenüber klassischen Verfahren zur Schlüsselverteilung besteht darin, dass die damit erreichte Sicherheit auf bekannten physikalischen Gesetzmäßigkeiten beruht und nicht auf Annahmen über die Leistungsfähigkeit von Computern und Algorithmen oder die Verlässlichkeit von Vertrauenspersonen. Die Sicherheit der verschiedenen Verfahren des Quantenschlüsselaustauschs entsteht dadurch, dass ein Angreifer, der die Schlüsselübertragung abhört, bemerkt wird und sogar die Menge der von ihm abgegriffenen Informationen gemessen werden kann.

Zur Erforschung und zum experimentellen Nachweis nutzbarer Quantum Key Distribution wurde das vom Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr dtec.bw geförderte Forschungsprojekt „MuQuaNet“ (Das **Qua**nten-Inter**net** im Großraum **Mü**nchen) mit einer Laufzeit von vier Jahren aufgesetzt. Im Rahmen von MuQuaNet wird im Großraum München eine Quantenkommunikationsinfrastruktur aufgebaut. Die Forscherinnen und Forscher implementieren ausgewählte sicherheitskritische zivile und militärische Anwendungsfälle und testen sie auf ihre Vertraulichkeit, Integrität, Verfügbarkeit und Wirtschaftlichkeit gegen Angriffe von Quantencomputern.

Neben der Entwicklung und Integration optischer QKD-Komponenten für Glasfaser- und Freiluftstrecken steht ein skalierbares Quantum-Key-Distribution-Managementsystem im Zentrum des Projekts. Darüber hinaus sind Sicherheitsanalysen von den Anwendungen über die Middleware bis hin zu den QKD-Endgeräten ein wesentlicher Bestandteil des Forschungsvorhabens. ■

Kontaktinformationen zum dtec.bw-Projekt MuQuaNet:

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



Trainingsraum der ICE&T Cyber Range am Forschungsinstitut CODE mit sechs Arbeitsplätzen.

Die Cyber-Range-Lösung am Forschungsinstitut CODE

ICE&T – IT Competence Education & Training

Die Cyber Range ICE&T (IT Competence Education & Training) ist das zentrale Labor am Forschungsinstitut CODE für realitätsnahe Trainings im Bereich der Cybersicherheit sowie für die Testung und Evaluation neuer Cybersicherheitsprodukte. Sie bietet eine Plattform zum Erlernen, Üben und Vertiefen von Fähigkeiten im Bereich der Cyber Network Operations mit Fokus auf der Verbesserung der Zusammenarbeit als Team.

Überblick

ICE&T ist eine umfassende und flexible Cyber-Range-Lösung. Derzeit sind komplexe Cyber-Incident-and-Response-Management (CIRM)-Szenarien in drei unterschiedlichen Schwierigkeitsgraden sowie in den Bereichen SCADA und Offensive Cyber Security verfügbar. Ein Self-Learning-Modul, sowie mehr als 80 individuelle Übungen aus neun verschiedenen Themengebieten ermöglichen ein zielgerichtetes Selbststudium.

Aufbau der Cyber Range

Durch Virtualisierung werden Szenarien auf vordefinierten virtuellen Netztopologien durchgeführt. Ein Lernmanagementsystem sowie eine Steuerungssoftware zur Kontrolle und Leitung durch die Trainer unterstützen die Trainings. Mittels durchdachter Ausstattung von Trainingsräumen wird speziell die Teamarbeit während der Durchführung der Übungen gefördert. Die flexible und modulare Architektur erlaubt die stetige Entwicklung neuer Szenarien in unterschiedlichen Themengebieten der Cybersicherheit. Neue Netztopologien, Software- und auch Hardwarelösungen können ebenfalls integriert werden und ermöglichen so den Ausbau des Funktionsumfangs und die Testung neuer Sicherheitslösungen in unterschiedlichen Domänen.

Ziele der Trainings

Über unterschiedliche Trainingsinhalte und Umfänge können Ziele je nach Bedarf erreicht werden. In einem Basic Training wird als ein Kernziel die Bearbeitung von Cyber Security Incidents im Team verfolgt. Durch die gemeinsame Analyse betroffener Systeme eines Angriffs werden Vorfälle nachvollzogen, um dadurch das Vorgehen von Angreifern zu verstehen, Maßnahmen zu ergreifen und Awareness zu schaffen.

Ein fortgeschrittenes Training ermöglicht es, die vorhandenen Fähigkeiten in ihrer Effizienz zu steigern. Komplexere Angriffe sollen erkannt und untersucht werden mit speziellem Fokus auf der besseren Koordination im Team und der sauberen Dokumentation der Vorfälle und des Vorgehens.

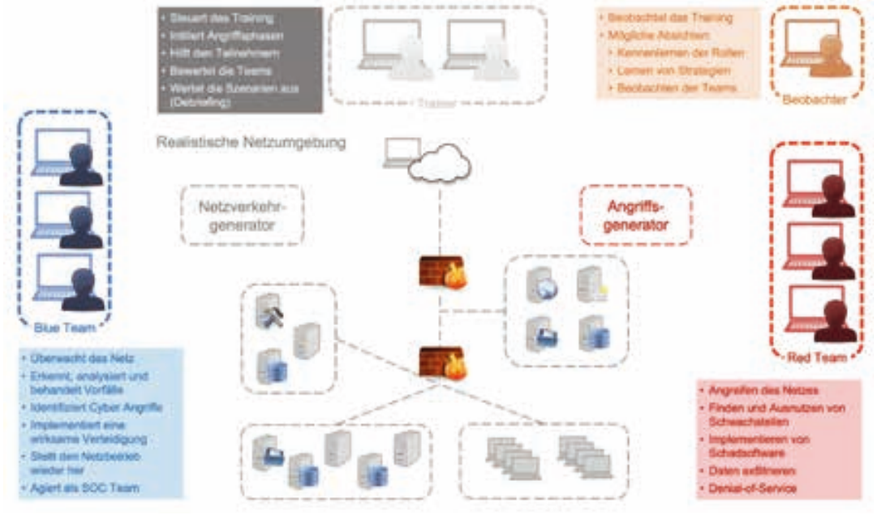
FI CODE *Forschungsinstitut Cyber Defence*
Universität der Bundeswehr München

Aktuelles Logo der ICE&T Cyber Range am FI CODE.

Auch die individuelle Zusammenstellung und Entwicklung von Trainings ist möglich, um noch weitere Ziele abzudecken, wie beispielsweise die Übung in eigenen Netztopologien.

Aktuelle Arbeiten

Zur Beibehaltung einer Trainingserfahrung in möglichst realitätsnahen Umgebungen ist die fortlaufende Anpassung bestehender Szenarien an den aktuellen Stand der Technik und die Entwicklung neuer Szenarien ein wesentlicher Bestandteil der aktuellen Aktivitäten. Auch die Einbindung in Forschungs- und Entwicklungsprojekte ist Teil der derzeitigen Arbeiten. Des Weiteren ist eine Erweiterung in den Bereichen IoT, SCADA und 5G geplant. ■



Rollen und Funktionen der ICE&T Cyber Range am FI CODE.

BEIDE ABB.: FI CODE

Forschung

Porträts und Projekte

ABB.: SHUTTERSTOCK / EFMAN

Prof. Dr. Florian Alt

Benutzbare Sicherheit und Privatsphäre

Der Lehrstuhl für Benutzbare Sicherheit und Privatsphäre unter Leitung von Prof. Dr. Florian Alt erforscht menschliches Verhalten in sicherheitsbezogenen Systemen. Die Gruppe beschäftigt sich insbesondere mit der Rolle von Sicherheit und Privatsphäre in benutzerorientierten Designprozessen und untersucht, wie sichere Systeme besser an die Art und Weise der Interaktion von Benutzern angepasst werden können.

Die Professur „Benutzbare Sicherheit und Privatsphäre“ wurde 2018 gegründet und forscht an der Schnittstelle zwischen Mensch, Computer und Interaktion, IT-Sicherheit und Datenschutz. Prof. Dr. Florian Alt geht mit seinem Team der Frage nach, wie Wissenschaftler und Produktentwickler dabei unterstützt werden können, Sicherheits- und Datenschutzbedürfnisse bereits im Designprozess zu berücksichtigen, mit dem Ziel, Sicherheits- und Datenschutzmechanismen besser in die Art und Weise zu integrieren, wie Nutzer im Alltag mit Technologie interagieren.

Die Forschungsgruppe beschäftigt sich mit einer Vielzahl verschiedener Themen. Darunter sind Sicherheits- und Datenschutzmechanismen basierend auf menschlichem Verhalten, die Nutzung des physiologischen Zustands von Benutzern, um sowohl bestehende Sicherheitsansätze zu verbessern als auch neue Sicherheitskonzepte zu entwickeln, das Verstehen und Untersuchen von Bedrohungen, welche durch ubiquitäre Technologien entstehen, sowie die Erklärbarkeit von Sicherheit und Datenschutz. 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 der Gruppe macht. Um Verhalten zu verstehen und neue Ansätze zu evaluieren, werden sowohl Labor- als auch empirische Studien durchgeführt.

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

Zusammen mit seinem Team veröffentlichte Prof. Dr. Florian Alt über 200 in DBLP gelistete wissenschaftliche Beiträge und erhielt mehr als zehn Auszeichnungen auf führenden Tagungen seines Fachgebiets. Die Forschung der Gruppe wurde durch die Deutsche Forschungsgemeinschaft (DFG), das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst, die Humboldt-Stiftung, den DAAD, Google und die BMW Group gefördert.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

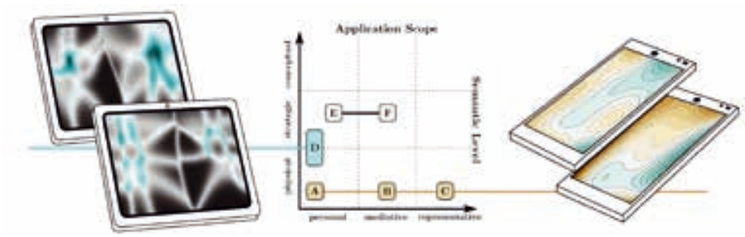
https://go.unibw.de/usec

Das Team des Lehrstuhls für Benutzbare Sicherheit und Privatsphäre.

ABB.: ISTOCK / GREMLIN; FLORIAN ALT

Projekt ubihave

Das Projekt untersucht, wie ubiquitäre Technologien von Verhaltensmodellen profitieren können. Die Forschung ist dadurch motiviert, dass persönliche Geräte und intelligente Umgebungen dank ihrer Sensorik und Rechenleistung reichhaltige benutzerspezifische Daten zur Verfügung stellen können. Dadurch eröffnen sich neue Wege für Anwendungen, welche Verhaltensmodelle verwenden, um sich an individuelle Benutzer und Kontexte anzupassen.



Das Projekt ubihave erforscht, wie Nutzer von der Modellierung ihres Interaktionsverhaltens mit ubiquitären Computern profitieren können.

Sensoren liefern reichhaltige Verhaltensdaten

Computer sind als alltägliche Begleiter (Smartphones, Tablets, Wearables) und eingebettete Sensoren (NFC, (Tiefen-)Kameras, Eye-Tracker) allgegenwärtig. Diese Geräte liefern reichhaltige nutzerspezifische Daten, die neue Wege für Anwendungen basierend auf Verhaltensmodellen eröffnen. Ein Beispiel ist die Möglichkeit, die Vision von intelligenten Benutzeroberflächen, smarten Geräten und reaktiven Umgebungen zu realisieren.

Modellierung von Benutzerverhalten

Viele aktuelle Geräte können auf simple Sensordaten reagieren (z. B. Orientierung eines Smartphone-Displays). Allerdings werden Schnittstellen und Interaktionen nur selten an individuelle Benutzer und Kontexte angepasst, da dies spezielle Methoden zur Verarbeitung unsicherer Daten erfordert. Um solche Informationen für Anwendungen und Benutzer zugänglicher und nützlicher zu machen, zielt dieses Projekt darauf ab, Modelle zu erstellen und anzuwenden, die das Benutzerverhalten basierend auf Daten von mobilen Geräten und allgegenwärtigen Sensoren beschreiben, analysieren und vorhersagen können. Potenzielle Anwendungsbereiche sind Benutzbare Sicherheit und Privatsphäre, Touch-Interaktion, Texteingabe und kontextabhängige adaptive Schnittstellen.

Forschungsfragen

In diesem Projekt beantworten wir eine Reihe von Fragen: In welchen Kontexten profitieren Benutzer von Verhaltensmodellen? Wie können Modelle die Interaktion verbessern? Bemerken Benutzer solche Anpassungen und entsprechen sie ihren Erwartungen? Wie kann Nutzerverhalten erfasst und für Anwendungen nutzbar gemacht werden? Wie können Metriken für Benutzeraktionen mit verhaltensbasierten Schnittstellen entwickelt werden? Welche Interaktionen rufen charakteristisches und konsistentes Verhalten hervor?

Auswirkungen

Dieses Projekt leistet folgende Beiträge: Erstens wird ein ganzheitlicher Gestaltungsraum entwickelt, um das Potenzial der Benutzermodellierung auch jenseits von Desktopumgebungen zu verstehen und zu untersuchen. Dies ermöglicht basierend auf einer gemeinsamen Benutzerrepräsentation eine effiziente Datenverarbeitung über Anwendungen hinweg. Zweitens identifizieren wir Szenarien, in denen verhaltensbiometrische Daten helfen können, Interaktionen zu optimieren, zu personalisieren und zu schützen. Beispiele sind neuartige benutzbare Sicherheitsmechanismen, effiziente und benutzbare mobile Texteingabe, an Nutzeraktivitäten angepasste Anwendungen und neuartige adaptive mobile Dienste. Damit Anwendungen Benutzereigenschaften berücksichtigen können, werden drittens Inferenzwerkzeuge entwickelt, die unsichere Sensordaten im Hinblick auf die angestrebten Benutzerkontexte und -ziele verarbeiten können.

Prof. Dr. Florian Alt
florian.alt@unibw.de
+49 89 6004 7320
go.unibw.de/usec

Gefördert durch:
Deutsche Forschungsgemeinschaft
(DFG)

Projekt Scalable Biometrics

In diesem Projekt untersuchen wir, wie Umgebungen, in welchen Computer und Sensoren allgegenwärtig sind, genutzt werden können, um Nutzer mithilfe verhaltensbiometrischer Systeme zu identifizieren und zu authentifizieren. Ziel ist es, herauszufinden, wie solche verhaltensbiometrischen Ansätze unter Veränderungen der Umgebung, der Anzahl der Personen und ihrer Eigenschaften sowie der verwendeten Technologie skalieren.

Herausforderungen traditioneller Authentifizierungsmechanismen

Wissensbasierte Authentifizierung, wie wir sie heute kennen, stammt aus der Zeit um 1960, als Menschen Großrechner verwendeten und sich nur selten und stets an der gleichen Maschine anmelden mussten. Heute jedoch müssen wir uns wesentlich öfter und in einer Vielzahl von Situationen und an unterschiedlichen Orten authentifizieren. Daraus resultiert ein erheblicher Mehraufwand (Nutzerinnen und Nutzer verwenden im Schnitt etwa 90 Minuten pro Monat für Authentifizierung) und es ergibt sich ein Anreiz, schwächere (und dadurch schneller einzugebende) Geheimnisse zu wählen oder gar ganz auf den Schutz von Daten zu verzichten.

Verhaltensbiometrie als vielversprechende Alternative

Verhaltensbiometrie, also die Identifizierung von Nutzern anhand ihres Verhaltens, hat in den vergangenen Jahren in der Wissenschaft an Popularität gewonnen. Mit diesem Ansatz müssen Nutzer sich kein Geheimnis (z. B. Passwort) merken, sondern können nahtlos und ohne aktive Involvierung über Eigenschaften wie Gang, Tippverhalten oder die Art, wie sie etwas ansehen, im Hintergrund authentifiziert werden. Allerdings wird Verhaltensbiometrie bisher hauptsächlich unter Laborbedingungen erforscht und es ist somit noch unklar, wie solche Ansätze mit Anforderungen außerhalb des Labors skalieren.

Das Projekt Scalable Biometrics untersucht, wie verhaltensbiometrische Konzepte für Pervasive-Computing-Umgebungen umgesetzt werden.

Forschungsfragen

Einige der Fragen, die dieses Forschungsprojekt beantwortet, sind zum Beispiel: Welchen Einfluss haben weitere Personen in der Umgebung, Eigenschaften der Umgebung (öffentlich oder privat) oder neuartige Interaktionsmöglichkeiten auf das Nutzerverhalten? Welchen Einfluss hat dies auf das Design von biometrischen Systemen? Wie können wir Benutzeroberflächen gestalten, um ein bestimmtes Verhalten hervorzubringen, und wie kann man aus dem Kontext geeignete Verhaltensmerkmale für die Identifikation schließen?

Relevanz

Wir sehen die Stärke von Verhaltensbiometrie darin, hohe Benutzbarkeit mit starker Sicherheit zu kombinieren. Darüber hinaus wollen wir mit diesem Projekt aber auch dazu beitragen, Verhaltensbiometrie über Sicherheitsanwendungen hinaus anzuwenden, beispielsweise, um Benutzerschnittstellen an das Verhalten von Nutzern anzupassen.

Prof. Dr. Florian Alt
florian.alt@unibw.de
+49 89 6004 7320
go.unibw.de/scalablebiometrics

Gefördert durch:
Deutsche Forschungsgemeinschaft
(DFG)

ABB.: DANIEL BUSCHEK, STEFAN SCHNEEGASS

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 ein Angriff auf ein IT-System vermutet wird. Stellen Sie sich dazu folgendes exemplarisches Szenario vor: Sie kommen an einem Montagvormittag nach einem entspannten Wochenende ins Büro und finden in Ihrem E-Mail-Postfach eine Reihe von elektronischen Nachrichten vor. Strukturiert, wie Sie sind, widmen Sie sich zunächst den offensichtlich wichtigen E-Mails. Eine Nachricht, die mutmaßlich von Ihrem Chef stammt, fällt Ihnen sofort ins Auge. Er will Ihnen noch einmal in einem angehängten Office-Dokument die aktualisierte Projektplanung für ein wichtiges Projekt erläutern und bittet Sie, sich das genau anzuschauen und zu kommentieren. Sie öffnen also das an die E-Mail angehängte Office-Dokument, allerdings kommt es nur zu einer Fehlermeldung. Eigentlich nichts Aufregendes, der Rechner macht ja oft mal, was er will. Nach ein paar Minuten springt der Lüfter Ihres Rechners an, weil der Prozessor anscheinend viele Befehle verarbeiten muss. Leider verschlüsselt ein Programm gerade alle Ihre gespeicherten Daten und zeigt Ihnen anschließend eine Erpressungsmeldung am Bildschirm: Entweder Sie zahlen ein Erpressungsgeld und können Ihre Daten dann wieder entschlüsseln oder die Daten des Rechners bleiben für immer verschlüsselt.

Eine IT-forensische Untersuchung ist mit zahlreichen Herausforderungen verbunden, mit denen sich die Professur „Digitale Forensik“ beschäftigt. Eine erste wichtige Herausforderung ist die schiere Datenflut im Rahmen einer IT-forensischen Untersuchung. 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.

Eine zweite wichtige Herausforderung ist die Korrektheit von IT-forensischen Tools, das heißt, sie sollen so arbeiten 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.

Eine dritte wichtige Herausforderung 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. Und schließlich versteckt sich Schadsoftware so gut, dass sie nur im „lebenden“ System – also dem Hauptspeicher bzw. dessen Abbild – gefunden und analysiert werden kann. Hierzu sind passende Methoden der Datenträgerforensik auf die Hauptspeicherforensik zu übertragen.

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

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

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

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

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

ABB.: ISTOCK / DEM10; HARALD BAIER

Schwerpunkte der Professur „Digitale Forensik“ sind der Umgang mit großen Datenmengen, die Erzeugung von synthetischen Testdaten, Anti-Forensik sowie fortgeschrittene Methoden der RAM-Analyse.

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

Die Forschungsgruppe von 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.

ABB.: ISTOCK / DEM10

Das Munich Computer Systems Research Laboratory (µCSRL) an der Professur „Sichere Softwareentwicklung“ beschäftigt sich mit der Erforschung und Entwicklung neuester Verteidigungstechniken, um fortgeschrittene, hochkomplexe und brandaktuelle Angriffe zu verhindern. Dazu gehören beispielsweise die sogenannten Transient Execution Attacks (Spectre und Meltdown), Rowhammer, Seitenkanäle, Code-Injektions- und Code-Reuse-Angriffe (z. B. Return-oriented Programming). Aus strategischer Sicht sind diese taktischen Angriffsvektoren auch von zentraler Bedeutung: Die aktuelle Bedrohungslage ist aus offensiver Perspektive durch mehrstufige Angriffskomponenten charakterisiert. Diese Angriffsstrategie begünstigt insbesondere Supply-Chain-Angriffe als Brückenkopf für Advanced Persistent Threats (APTs).

Der derzeitige Hauptfokus der Grundlagenforschung von µCSRL beschäftigt sich mit neuen Methoden und Techniken im Bereich „Software Diversity“. Hier haben wir im Jahr 2020 zwei große Meilensteine erzielt. Zum einen ist es uns gelungen, eine der neuesten Angriffstechniken – Speculative Probing – durch die neue Verteidigungstechnik „Speculation-aware Booby Traps“ zu verhindern. Dies wird in Kombination mit einer anderen Verteidigungstechnik, „Decoy Return Addresses“, verwendet, um sogenannte Address-oblivious-Code-Reuse-Angriffe vollautomatisch und transparent durch einen neuen Übersetzungsvorgang der relevanten Programme zu verteidigen. Zum anderen haben wir neue Resultate im Bereich formal verifizierter Systemsoftware erarbeitet, welche insbesondere für Anwendungen im Hochsicherheits- und Hochverfügbarkeitskontext unabdingbar sind. Diese essenziellen Vorarbeiten verifizieren die Korrektheit von Transformationen im Bereich „Software Diversity“ mechanisch, das heißt, sie können für jede Übersetzung eines Programms einen Beweis der Korrektheit der angewandten Transformation erstellen.

Parallel zum Aufwachsen des µCSRL streben wir eine Erweiterung unserer Forschungsgebiete und der damit einhergehenden Forschungsagenda an. Diese enthält folgende Schwerpunkte:

1. automatische Schwachstellenanalyse mittels Fuzzing,
2. energieeffiziente und platzsparende Datacenter-Architekturen und
3. Systemsoftware im 21. Jahrhundert.

Der erste Schwerpunkt, Fuzzing, wird durch einen eigenen Cluster unterstützt und zusammen mit Herrn Prof. Dr. Kinder erforscht. Hier wird durch gezielte Kooperationen in Europa eine Vorreiterrolle angestrebt, die auch innerhalb der Bundeswehr zur Systemabnahme verwendet werden soll, um Supply-Chain-Angriffe möglichst früh erkennen und bekämpfen zu können. Der zweite Schwerpunkt, Datacenter-Architektur, soll es Deutschland ermöglichen, gezielt und effizient Datacenter aufzubauen, um zu den führenden Hyperscalern aus den USA und China aufzuschließen. Ohne diese Fähigkeit ist es für Deutschland nicht möglich, diesen Supermächten militärisch und industriell die Stirn zu bieten, mit erheblichen Nachteilen für den deutschen Staat und dessen Industrie. Der dritte Schwerpunkt, Systemsoftware im 21. Jahrhundert, widmet sich der notwendigen Grundlagenforschung, um Deutschland und seinen europäischen Partnern essenzielle Systemsoftware, mithin Compiler und Browser, zur Verfügung zu stellen.

Alle drei Schwerpunkte haben ein gemeinsames Ziel, nämlich die digitale Souveränität Deutschlands und Europas zu gewährleisten. Durch die ambitionierte Aufgabenstellung und die angestrebten kompetitiven Resultate hoffen wir, das Forschungsinstitut CODE als international erste Adresse in diesen Forschungsbereichen zu etablieren.

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

Projekt µRAD

Return Address Decoys

Software Diversity ist eine potente Verteidigung gegen fortgeschrittene Angriffe wie z. B. Code-Reuse-Angriffe. Ihre stärkste Ausprägung – Leakage-resilient Software Diversity – kann durch zwei Angriffe ausgehebelt werden: Address-oblivious Code Reuse und BlindSide. µRAD kontert beide Angriffe und ist daher von essenzieller Bedeutung, um die Potenz und Vielseitigkeit von Software-Diversity-Techniken zu belegen.

Software Diversity

Die grundlegende Idee von Software Diversity ist es, den Effekt von Biodiversität im Softwarebereich zu replizieren. Heutzutage wird das Software-Ökosystem als Monokultur organisiert, in der identische Programme auf unzähligen Computern laufen. Diese Monokultur gibt den Angreifern einen fundamentalen Vorteil, indem ein einzelner Angriff alle Computer, auf denen die Zielsoftware läuft, gleichzeitig und in identischer Weise angreifbar macht (also Skaleneffekte zugunsten der Angreifer darstellt). Software Diversity verändert Programme proaktiv, um diesen Vorteil zu nivellieren.

Address-oblivious Code Reuse

Im Jahr 2017 beschrieben Forscher einen neuen Code-Reuse-Angriff namens Address-oblivious Code Reuse (AOCR). Der AOCR-Angriff stellt dabei die Sicherheit modernster Leakage-resilient-Software-Diversity-Techniken, wie z. B. Readactor (u. a. durch die Mitarbeit von Prof. Dr. Brunthaler), in Frage. Die Schlussfolgerung der Arbeit ist, dass der AOCR-Angriff die fundamentalen Grenzen von Software Diversity aufzeigt und sich daher zukünftige Forschung auf Schutzmaßnahmen im Bereich der Integritätssicherung konzentrieren sollte.

BlindSide

Im Jahr 2020 wurde durch Forscher der führenden Forschungsgruppe im Bereich Systemsicherheit – VUSec von der VU Amsterdam – ein weiterer Angriff publiziert, BlindSide. Dieser neue Angriff baut auf einer Vorarbeit aus Stanford, dem sogenannten Blind-ROP-Angriff, auf. Die grundlegende Idee beider Angriffe ist es, durch einen Seitenkanal einen Brute-Force-Angriff zu optimieren. Die wesentliche Neuerung von BlindSide ist die Verwendung der spekulativen Ausführung, um den Angriff zu verbergen. BlindSide kann daher die Speicheradressen von Funktionen identifizieren, welche in einem darauffolgenden Angriff verwendet werden können. Durch dieses Vorgehen kann BlindSide eine Grundsäule moderner Diversity-Verteidigungen unterminieren, den sogenannten Execute-Only-Speicher.

Return Address Decoys

µRAD diversifiziert Rücksprungadressen von Funktionen, sodass ein Angreifer keine vorhersagbaren Inferenzen über die Speichergeometrie von Programmen machen kann. Diese Technik generalisiert auf andere Angriffstechniken und leistet daher Pionierarbeit im Bereich Software Diversity.

Speculation-aware Booby Trap

Um BlindSide-artige Angriffe zu verhindern, nimmt µRAD eine Vorreiterrolle durch die Erforschung sogenannter Speculation-aware Booby Traps ein. Diese Fallen werden zur Übersetzungszeit in ein Programm integriert und ermöglichen aktive Reaktionen auf Angriffe. Bisherige Booby Traps konnten gegen diesen Angriff nicht angewandt werden, da diese normale und spekulative Ausführung nicht unterscheiden konnten. µRAD verwendet neue Booby Traps, die CPU-Spekulation erkennen und den Angreifer damit in die Irre führen können. Sollte der Angreifer danach eine µRAD Booby Trap ansteuern, kann das Programm reaktive Abwehrmaßnahmen einleiten.

Bedeutung und gesellschaftliche Relevanz

µRAD ist die erste bekannte Verteidigung gegen den BlindSide-Angriff und daher immanent relevant, um das FI CODE auf internationaler Ebene zu etablieren. Darüber hinaus widerlegt µRAD die Einschätzung vorheriger Arbeiten, die die Grenzen von Software Diversity vorzeitig ausriefen, und belegt erneut deren vielfältige Anwendbarkeit.

Prof. Dr. Stefan Brunthaler

stefan.brunthaler@unibw.de

+49 89 6004 7330

Gefördert durch:
Bundesministerium der Verteidigung (BMVg)

Projekt µFoCUS

Verifizierte und sichere Ausführung von dynamischen Programmiersprachen

µFoCUS formalisiert und verifiziert die optimierte Ausführung von dynamischen Programmiersprachen. Da verbreitete Just-in-Time-Übersetzer oft viele und schwerwiegende Bugs enthalten, stellt µFoCUS eine hervorragende Alternative mit formalen Garantien dar.

Die Verbreitung von dynamischen Programmiersprachen

Dynamische Programmiersprachen, wie z. B. Python oder JavaScript, sind aus der Welt nicht mehr wegzudenken. Programme wie Dropbox verwenden Python, wohingegen JavaScript die dominante Programmiersprache im Internet ist, welche von allen Browsern verstanden und ausgeführt wird. Die weite Verbreitung dynamischer Programmiersprachen ist wohl deren behaupteter höherer Produktivität geschuldet. Andererseits sind die in diesen Sprachen geschriebenen Programme oft von einer niedrigen Geschwindigkeit betroffen.

Gefahren durch die Ausführung dynamischer Programmiersprachen

Um die Langsamkeit der dynamischen Programmiersprachen auszuhebeln, werden oft sogenannte Just-in-Time-Compiler verwendet, also Programme, die parallel zum eigentlichen Programm laufen und dieses in optimierten Maschinencode übersetzen. Die Erfahrung zeigt aber, dass die Implementierung eines solchen JIT-Compilers für komplizierte Sprachen wie z. B. JavaScript ebenfalls kompliziert ist und daher oftmals dazu führt, dass JIT-Compiler oft viele Fehler enthalten. Dies wird beispielsweise eindrucksvoll von einer dreiteiligen Serie zum Thema „Angriffe auf JIT-Compiler“ von Googles Project Zero Security Team belegt. Das fundamentale Problem dieser JIT-Compiler ist, dass Maschinencode zuerst generiert und dann vom Programm selbst ausgeführt wird. Interpreter umgehen dieses fundamentale Problem dadurch, dass kein Maschinencode generiert wird, weisen aber oft selbst Geschwindigkeitsprobleme auf.

µFoCUS

Das Projekt Verifikation und Sichere Ausführung von dynamischen Sprachen baut auf Vorarbeiten von Prof. Dr. Brunthaler zur Optimierung von Interpretern auf. Dabei widmete er sich spezifisch dem Problem, Interpreter in ähnlicher Weise zu einem JIT-Compiler zu optimieren, wodurch er bis zu sechsfache Geschwindigkeitsverbesserungen erzielen konnte. Da diese Interpreter konstruktionsbedingt keinen Maschinencode generieren, sind Schwachstellen und darauf aufbauende Angriffe von vornherein ausgeschlossen. Im Rahmen dieses Projekts haben wir die Essenz einer dynamischen Sprache in Isabelle formalisiert und mechanisch verifiziert, dass die von uns angewandten aggressiven Optimierungen semantikerhaltend sind. Die Resultate dieser Arbeit wurden kürzlich bei der Internationalen Konferenz zu zertifizierten Programmen und Beweisen (CPP 2021) präsentiert.

Bedeutung und gesellschaftliche Relevanz

Unser Projekt vereint hohe Geschwindigkeit mit einer garantierten, formal bewiesenen Korrektheit, welche wiederum ganze Klassen an Implementierungsfehlern ausschließt. Damit ist es für die Gesellschaft zum ersten Mal möglich, eine garantiert korrekte Alternative zu verwenden, welche die zunehmend sicherheitsrelevante Ausführung von dynamischen Sprachen ermöglicht.

Prof. Dr. Stefan Brunthaler

stefan.brunthaler@unibw.de

+49 89 6004 7330

Gefördert durch:
Bundesministerium der Verteidigung (BMVg)

Prof. Dr. Gabi Dreo Rodosek

Kommunikationssysteme und Netzsicherheit

Der Lehrstuhl befasst sich mit der Detektion und Mitigation von sogenannten Advanced Persistent Threats, der Entwicklung neuartiger netzbasierter Moving-Target-Defence-Ansätze, dem Einsatz von KI/ML, unter anderem im Bereich Lagebildentwicklung und Social Media Analytics, sowie Software Defined Networking, 5G/6G, Internet of Things und Quantenkommunikation.

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

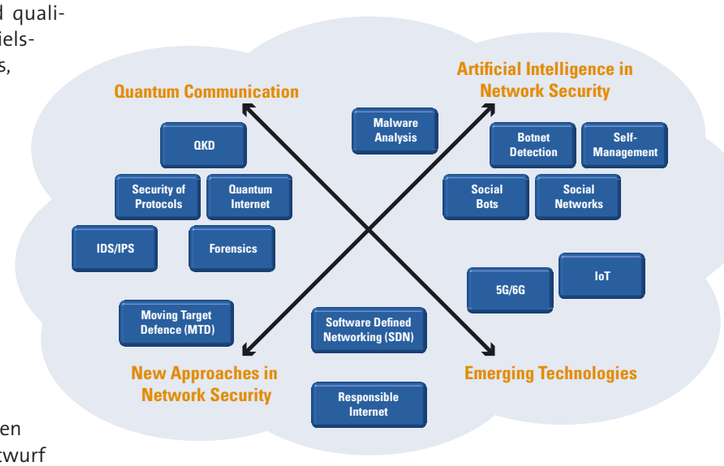
Alle zukünftigen globalen marktbeherrschenden Produkte und Dienstleistungen werden in der digitalen Welt angesiedelt sein oder zumindest stark damit interagieren. Beispiele sind Robotik, Industrieautomation, autonomes Fahren, intelligente Stromnetze, Smart City und Smart Home. Die digitale Transformation und zunehmende Vernetzung verschiedenster Systeme und Objekte verändern bereits heute unser soziales, gesellschaftliches und berufliches Leben. Die Komplexität der IT-Systeme und insbesondere ihre Vernetzung bedingen auch eine hohe Cyberbedrohungslage.

Es ist nichts Neues, dass sowohl der Angreifer als auch der Verteidiger sich gegenseitig herausfordern, jedoch heutzutage auf einem deutlich höheren und qualifizierteren Level als vor einigen Jahren. Beispielsweise stellte die Cyberattacke auf SolarWinds, die über 250 Behörden, tausende Firmen und über 18.000 Netze betraf, eine neue Dimension der Bedrohung dar, die insbesondere auf das IT-Management von Rechnernetzen abzielte. Daher kommt vor allem der Frage der Cybersicherheit von IT-Infrastrukturen eine Schlüsselrolle zu. Eine vertrauenswürdige IT-Infrastruktur, basierend auf vertrauenswürdigen, sicheren Kommunikationssystemen, ist die Grundvoraussetzung für das Funktionieren in unserer digitalen Gesellschaft.

Der Lehrstuhl verfolgt daher das Ziel, im Rahmen von Forschungsvorhaben Lösungen für den Entwurf und sicheren Betrieb moderner, komplexer Kommunikationsinfrastrukturen zu erarbeiten und prototypisch umzusetzen. Dabei werden unterschiedliche Forschungsbereiche betrachtet.

In einem aktuellen Forschungsvorhaben wird beispielsweise mit Moving-Target-Defence(MTD)-Methoden an einem Paradigmenwechsel in der Netzverteidigung geforscht. Der statische Ansatz, IT-Systeme und Rechnernetze zu sichern, ist aus den Anfängen der Cybersicherheit erwachsen, in der die Systemkomplexität und auch die Anzahl gefundener bzw. möglicher Schwachstellen deutlich geringer als heute war. Um die konventionellen Cyberverteidigungskonzepte aufzubrechen und insbesondere die Asymmetrie des Angriffs zugunsten des Verteidigers zu ändern, werden Fähigkeiten benötigt, die es ermöglichen, die Angriffsoberfläche eines IT-Systems bzw. Netzes dynamisch zu ändern. Durch diese permanente dynamische Änderung der Angriffsfläche wird die Komplexität und damit der Aufwand sowie die Kosten für Angreifer erhöht und das Risiko von Sicherheitslücken und Angriffsmöglichkeiten begrenzt.

Ein weiteres Forschungsfeld ist der Einsatz von KI/ML für die Entwicklung innovativer Cyberverteidigungsansätze auf Ebene der Netzsicherheit. Die Anwendungsfelder sind vielfältig und reichen von der Anomalieerkennung im Bereich IDS/IPS bis hin zur Botnetzerkennung und Detektion von Cyberangriffen wie DDoS in verschiedenen Netzinfrastrukturen (unter anderem Software-defined Networks, 5G/6G und IoT-Netze). Ferner wird die Verwendung von KI/ML auf der Grundlage beliebiger Datenquellen (z. B. soziale Netzwerke) erforscht, um Cyberlagebilder zu erstellen, die Daten zu visualisieren und mithilfe von Mixed-Reality-Technologien mit ihnen zu interagieren.



Forschungslandkarte der Professur „Kommunikationssysteme und Netzsicherheit“.

Ein weiteres Forschungsgebiet beschäftigt sich mit dem Einsatz von Quantenkommunikation und dem Aufbau eines Quanteninternets, in dem Quantenrechner mittels Quantenkommunikationsstrecken verbunden sind. Hierbei werden insbesondere Fragestellungen im Bereich der Post-Quanten-Kryptographie sowie Quantum Key Distribution betrachtet.

Prof. Dr. Gabi Dreo Rodosek

gabi.dreo@unibw.de

+49 89 6004 7300

www.unibw.de/network-security

CONCORDIA

Ein europäisches Ökosystem mit führenden Kompetenzen aus Forschung, Industrie, KMUs und öffentlichen Organisationen

Ziel von CONCORDIA ist der Aufbau des europäischen Secure, Resilient and Trusted Ecosystem zur Entwicklung von Cybersicherheitslösungen der nächsten Generation durch einen ganzheitlichen datengetriebenen End-to-End-Ansatz. Weitere Ziele sind der Aufbau eines europäischen Ökosystems für Aus- und Weiterbildung, die Identifizierung marktfähiger Lösungen, das Wachstum bahnbrechender Technologien und der Aufbau von Inkubatoren.

Die Verbreitung von IKT-Technologien schreitet immer schneller voran, gepaart mit komplexen, miteinander verbundenen Systemen und Netzen von Milliarden von Internet-of-Things(IoT)-Geräten, Diensten und Nutzern. Zukünftige IKT-Umgebungen, meist cloudgestützt und IoT-basiert, bestehen somit aus komplexen miteinander vernetzten Systemen, die sehr heterogen und allgegenwärtig sind. Die zunehmende Heterogenität, Komplexität und Vielfalt von Geräten, Computersystemen, Technologien, Software und Diensten sowie die sich ändernden Benutzerinteraktionen mit Technologien und die technischen Kenntnisse der Benutzer stellen vor allem die Cybersicherheit vor eine Herausforderung.

Die Bedrohungslandschaft entwickelt sich mit enormer Geschwindigkeit. Wir stehen vor einer äußerst schnell wachsenden Angriffsoberfläche mit einer Vielzahl von Angriffsmethoden, einer deutlichen Asymmetrie zwischen Angreifern und Verteidigern, Milliarden vernetzter IoT-Geräte, meist nur reaktiven Ansätzen zur Angriffserkennung und Schadensbegrenzung und schließlich vor Big-Data-Herausforderungen. Die klare Asymmetrie der Angriffe (das heißt, Angreifer müssen nur eine Schwachstelle finden, während die Verteidiger das komplette System schützen müssen) und die enormen Datenmengen sind zusätzliche Gründe, die es erforderlich machen, Ansätze für Cybersicherheit im Hinblick auf die Minimierung der Angriffsoberfläche neu zu überdenken, die Angriffsfläche dynamisch zu verändern, um die Erkennung, Risikobewertung und -minderung zu automatisieren und die Vorhersage und Abwehr von Angriffen mithilfe von künstlicher Intelligenz und maschinellem Lernen zu untersuchen.

Das Konsortium von CONCORDIA mit derzeit 53 Partnern wächst weiter.

Aufbau eines starken europäischen digitalen Ökosystems

CONCORDIA ist eines der vier geförderten Pilotprojekte des Cybersecurity-Calls „Horizont 2020“ aus dem Jahr 2018: „Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap“ (vgl. Abb.).

Da Cybersicherheit für die digitale Souveränität Europas von entscheidender Bedeutung ist, hat das Forschungsinstitut CODE, unter Leitung von Prof. Dreo, als Koordinator in Zusammenarbeit mit 42 Partnern einen Projektantrag für einen Horizont 2020 (H2020)-Call eingereicht, der als bestbewerteter Antrag angenommen wurde. CONCORDIA (www.concordia-h2020.eu) startete im Januar 2019 mit einer Finanzierung von 16 Millionen Euro aus der EU und umfasst mittlerweile 53 offizielle Partner, mit einer zusätzlichen Finanzierung von ca. 7 Millionen Euro aus der Industrie und den Mitgliedstaaten. Die europäische IT-Sicherheitslandschaft leidet nicht unter einem Mangel an Ideen, sondern unter ihrer Fragmentierung über nationale Grenzen hinweg, was ein Schlüsselproblem darstellt. Manchmal ist es nur das fehlende Verständnis industrieller Zwänge und Vorgaben bzw. die Tatsache, dass wichtige Entwicklungen bei sicheren Hard- und Softwaresystemen außerhalb des Einflussbereichs der Europäischen Union liegen, was Anlass zu diesen Sorgen gibt. CONCORDIA geht dieses Problem an, indem es ein europäisches Ökosystem für Cybersicherheit aufbaut und verschiedene Interessengruppen (Industrie, Forschung, KMU, Start-ups, öffentliche Einrichtungen) bei der Entwicklung europäischer IT-Dienstleistungen und IT-Produkte zusammenführt.

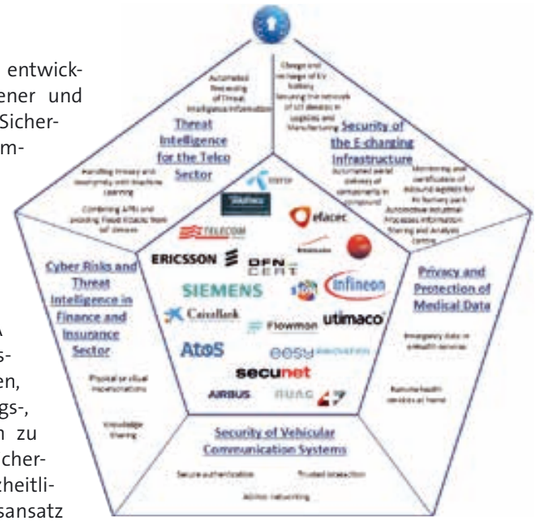
Dienstkatalog von CONCORDIA

CONCORDIA bietet verschiedene Dienste für die Community. So hat der Dienst „Assists“ das Ziel, angehende Forscher und Investoren bei der Etablierung eines Start-ups zu unterstützen. Gleichzeitig unterstützt CONCORDIA mit „Women in Cyber“ Frauen bei ihrer Karriere im Bereich der Cybersicherheit. Da der Mensch immer noch die höchste Gefahrenquelle im System darstellt, setzt CONCORDIA auf die Aufklärung über Gefahren (unter anderem in Blogs, Videos und durch Infographen) kombiniert mit gleichzeitigen Trainings auf verschiedensten Ebenen (u. a. Professionals, Schule, Hochschule, Fachbereich) mit dem Dienst „Educates“. Forschung und Entwicklung hängen eng zusammen und bedingen sich gegenseitig, so dass CONCORDIA hier die Zusammenarbeit und Diversität fördert. Ein weiteres Ziel ist die Vernetzung von unterschiedlichen Stakeholdern.

CONCORDIA-Dienstkatalog.

CONCORDIA erforscht

Ein breit angelegter und entwicklungsfähiger datengetriebener und kognitiver End-to-End(E2E)-Sicherheitsansatz für die hochkomplexen und vernetzten Zusammensetzungen des entstehenden Cloud-, IoT- und Edge-gestützten IT-Ökosystems ist ein Muss in der Forschungsbetrachtung. CONCORDIA adressiert fünf Forschungs- und Technologieebenen, von benutzer-, anwendungs-, system- und netz- bis hin zu gerätezentrierter Cybersicherheit. Dabei wird ein ganzheitlicher End-to-End-Sicherheitsansatz verfolgt, insbesondere, da sich alle Cloud-, IoT- und Edge-Systeme in komplexer, vernetzter Weise weiterentwickeln, um mehrere Systeme und Dienste zu verbinden.

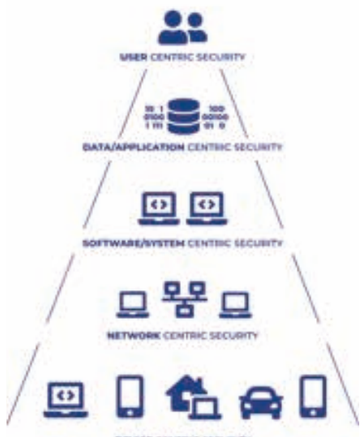


Sieben industrielle Pilotprojekte, um Plattformen, IT-Produkte und IT-Dienstleistungen zu entwickeln.

CONCORDIA entwickelt

Die Entwicklung von IT-Produkten und -Dienstleistungen wird in sieben industriellen Pilotprojekten innerhalb von CONCORDIA durchgeführt. Davon sind fünf sektorspezifische und zwei sektorübergreifende Piloten. Die beiden sektorspezifischen Piloten, nämlich der Telekommunikations- und Finanzsektor, entwickeln eine Threat-Intelligence-Plattform für ihre Anwendungsdomänen.

CONCORDIA entwickelt auch eine Threat-Intelligence-Plattform für Europa (eines der sektorübergreifenden Pilotprojekte). Darüber hinaus liegt ein Schwerpunkt auf E-Health, E-Mobility, der Sicherheit von unbemannten Luftfahrzeugen (UAV) und der Entwicklung eines DDoS-Clearinghouses für Europa.



Forschungsebenen: Komplexes, dynamisches, schnell wachsendes, stark vernetztes „Internet der Dinge“ vom IoT zur Cloud.

Prof. Dr. Gabi Dreo Rodosek
gabi.dreo@unibw.de
+49 89 6004 7300
www.unibw.de/network-security

Gefördert durch: Europäische Kommission

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

Prof. Dr. Michaela Geierhos

Data Science

Das interdisziplinäre Team der Professur „Data Science“ vereinigt Kompetenzen aus den Bereichen Informatik, Computerlinguistik und Wirtschaftswissenschaften, um aktuellen und zukunftsorientierten Forschungsfragen auf den Gebieten des Semantic Information Processing sowie des Knowledge & Data Engineering auf den Grund zu gehen.

ABB.: ISTOCK / METAMORWORKS; SHUTTERSTOCK / TRUEFFELPIX

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 konzentrieren wir uns auf wissensbasierte und computerlinguistische Ansätze. Dazu zählt unter anderem die Entwicklung von Algorithmen zur (semantischen) Textanalyse und das Ermöglichen von Kommunikation zwischen Mensch und Maschine durch die Interaktion über Informationssysteme (z. B. Freitextsuche, Frage-Antwort-Systeme). Praktische Anwendungen sind unter anderem Suchmaschinen, Social-Media-Mining-Systeme, Stimmungsanalyse und wissensbasierte Frage-Antwort-Systeme.

Praxisorientierte Lehre

In unseren Lehrveranstaltungen legen wir besonderen Wert auf ein Konzept, das Theorie und 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. Wir leisten damit 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, pflegen wir 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 erscheint, wusste der Informatiker und Computerpionier Alan Kay schon 1970: „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 Deep Fakes bis hin zur lagebildbasierten Krisenfrüherkennung.

Ziel unserer 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 kurz- und langfristigen 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 Deep Fakes 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 wollen wir aufdecken.

Prof. Dr. Michaela Geierhos
michaela.geierhos@unibw.de
+49 89 6004 7340
www.unibw.de/datascience

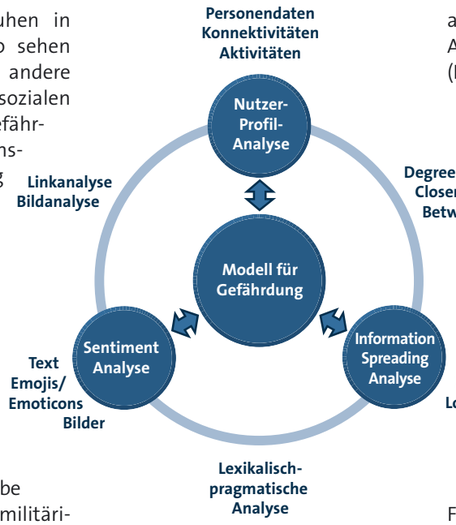
Aufgabenspektrum der Professur „Data Science“.

Projekt ADRIAN

Authority-Dependent Risk Identification and Analysis in Online Networks

Ziel ist es, ausgewählte (Lauf-)Apps automatisiert zu überwachen und deren gesammelte Daten zu analysieren, mit Social-Media-Profilen zu korrelieren und Personencluster zu bilden, um potenzielle Ziele zu identifizieren und ihr Gefährdungspotenzial abzuschätzen. Werden diese Informationen noch mit weiteren eingestuften Materialien korreliert, lässt sich eine Gefährdungsplausibilität für entsprechende Personen(gruppen) oder Standorte ermitteln.

Nicht erst seit den Unruhen in den USA im Sommer 2020 sehen sich Ordnungshüter und andere Personengruppen in den sozialen Medien einem erhöhten Gefährdungspotenzial gegenüber. Insbesondere die Verknüpfung von Social-Media-Accounts und -Posts (bspw. Twitter oder Instagram) mit den Bewegungsprofilen und Standortdaten aus beliebten Lauf-Apps macht die Nutzerinnen und Nutzer sowie ihre Angehörigen identifizierbar, aufspürbar und damit zu einer potenziellen Zielscheibe von Attacken im Netz. Dass militärische Standorte mithilfe der geteilten Geodaten von Laufstrecken lokalisiert werden können, ist in diesem Zusammenhang ein weiterer sicherheitsrelevanter Aspekt.



Zusammenspiel der Verfahren zur Gefährdungsanalyse.

Im Rahmen des Projekts ADRIAN werden zunächst ausgewählte Lauf-Apps überwacht und die dabei gesammelten Geodaten anschließend analysiert. In einem zweiten Schritt werden die Nutzerprofile von Lauf-Apps und Social-Media-Plattformen korreliert, um so ein Personencluster bilden zu können und die Identifikation potenzieller Ziele zu ermöglichen. Da sich auf diese Weise im Rahmen der Datenanalyse und Wissensgewinnung ein sogenannter „Digitaler (Lauf-)Zwilling“ rekonstruieren lässt, werden hochsensible Daten generiert. Können diese Daten noch mit weiteren vertraulichen Daten (unter anderem von Sicherheitsbehörden oder militärischen Dienststellen) korreliert werden, lässt sich eine Abschätzung der Gefährdungsplausibilität für entsprechende Personen(gruppen) oder Standorte vornehmen.

Zur Erreichung dieser Ziele müssen bei der technischen Umsetzung des Vorhabens unter anderem Methoden des Information Retrievals mit Ansätzen aus der forensischen Linguistik kombiniert werden. Ferner werden Verfahren zur Netzwerkanalyse und Clusterbildung eingesetzt, um neuartige Bewertungsfunktionen für die Abschätzung von gefährdeten Zielen (Personen, Orten etc.) auf Basis der preisgegebenen Informationen im Web 2.0 zu entwickeln. Für die spätere Übermittlung der dabei gewonnenen Erkenntnisse an andere Dienste ist zudem der Einsatz einer hochsicheren Quantenverschlüsselung vorgesehen.

Gefördert wird das Teilprojekt „ADRIAN – **A**uthority-**D**ependent **R**isk **I**dentification and **A**nalysis in Online **N**etworks“ im Kontext des Forschungsvorhabens „MuQuaNet“, dessen Ziel der Aufbau, Test und Forschungsbetrieb eines quantensicheren Kommunikationsnetzes im Großraum München ist. Dieses Netz soll zunächst der Universität der Bundeswehr, später jedoch auch weiteren Forschungseinrichtungen, Behörden und militärischen Dienststellen zur Verfügung gestellt werden.

Prof. Dr. Michaela Geierhos
michaela.geierhos@unibw.de
+49 89 6004 7340

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

Projekt TextBroom

Erkennung und Sichtbarmachung potenzieller Privatsphäreverstöße in Fließtexten

Das moderne Web basiert auf Interaktion, Diskussion und dem Austausch von Informationen. Immer wieder werden persönliche Informationen gegen die Urheber selbst eingesetzt. Mit „TextBroom“ wurde ein Konzept entwickelt, das sich der Erkennung von Informationspreisgaben durch eine vielschichtige Verarbeitungskette annimmt, um kritische Textbestandteile zu identifizieren und mit einer Erläuterung möglicher Risiken zu versehen.

Vernetzte Welt: Open Source Intelligence

Durch die fortschreitende semantische Vernetzung im Web („Semantic Web“) entsteht eine riesige, frei zugängliche Informationsquelle für datengesteuerte Anwendungen. Dies stellt unter Umständen ein persönliches Risiko für Einzelne dar. Da im Web die nutzergenerierten Daten („User-generated Content“) immer effektiver mit externen Ressourcen (sog. Wissensquellen) automatisiert verknüpft werden, können selbst ungewollt (implizit) offenbarte Einzelinformationen schädliche Folgen für Individuen haben. Obwohl Serviceprovider im Web mittlerweile die Pflicht haben, die Sicherheit und Privatsphäre von Benutzerdaten zu gewährleisten, gibt es Fälle, in denen Benutzerdaten missbraucht und kompromittiert oder öffentlich verfügbare Informationen gegen den ursprünglichen Verfasser verwendet werden. Es ist somit auch im Interesse der Kommunizierenden, nur diejenigen Informationen in Textbeiträgen zu platzieren, die einen gewissen selbstbestimmten Grad an Anonymität wahren.

TextBroom bei der Arbeit: Hervorhebung von privaten Patienteninformationen in Arztbewertungen.

Digitaler Fußabdruck verleitet zum Datenmissbrauch

Informationen, die tagtäglich, stückweise und über Jahre veröffentlicht wurden, sind für die Verfasser nicht mehr überschaubar, nicht mehr editierbar und damit nicht mehr kontrollierbar. Sie haben das Potenzial, zur Erzeugung eines digitalen Abbilds genutzt zu werden. Ein sehr greifbares Beispiel sind in diesem Zusammenhang Gesundheitsforen, in denen Benutzer unter einem Pseudonym Hilfe zu gesundheitlichen Themen suchen. In ihren einzelnen Beiträgen achten die Verfasser im Idealfall darauf, nicht zu viele Informationen preiszugeben. Sie vergessen dabei allerdings, dass die Summe der Beiträge über die gesamte Existenz ihres Benutzerkontos zur Erzeugung eines digitalen Zwillings herangezogen werden kann. Im Projekt „TextBroom“ konnte gemeinsam mit Dr. Frederik Bäumer von der Fachhochschule Bielefeld aufgezeigt werden, dass sich bei vielen Benutzerkonten über mehrere Beiträge und mehrere Jahre ein aufschlussreiches „Informationspuzzle“ ergab.

Es konnte ferner gezeigt werden, dass durch die schrittweise Analyse der nutzergenerierten und domänenspezifischen Wissensressourcen eine automatische Erkennung von isolierten, privatsphäregefährdenden Aussagen möglich ist. Jedoch wird dieses Verfahren noch nicht der Herausforderung in Gänze gerecht, da das Zusammenwirken einzelner Informationen bislang unberücksichtigt bleibt.

Prof. Dr. Michaela Geierhos
michaela.geierhos@unibw.de
+49 89 6004 7340

ABB.: MICHAELA GEIERHOS

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

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

Das Team der Professur „IT-Sicherheit von Software und Daten“ verfolgt das Ziel, Lösungen für praxisrelevante 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 werden. Dieser Ansatz ermöglicht unter anderem die explorative Anwendung offensiver Testverfahren und somit die qualitative und quantitative Analyse von Schwachstellen in komplexen mehrstufigen Angriffsszenarien. Daraus können systematisch Sicherheitsanforderungen abgeleitet werden, die als Grundlage für die nachfolgenden konstruktiven Tätigkeiten und eine spätere praktische Evaluation erzielter Resultate dienen.

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

In 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. 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 2495

www.unibw.de/software-security

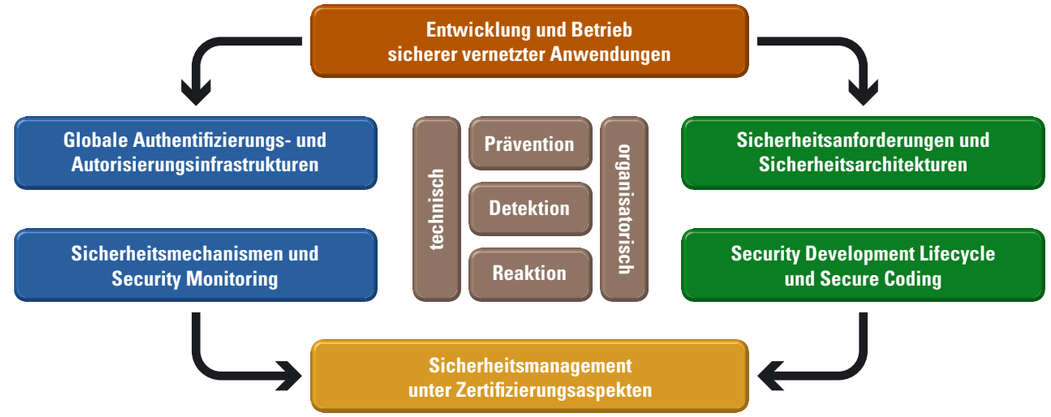


ABB.: ISTOCK / VERTIGO3D; TAUSENDBLAUWERK; QUELLE: W. HOMMEL

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

Projekt DISKURS

Digitale Identitäten für Servicekonten: Umsetzungsstrategien, Richtlinien und Sicherheitsaspekte

Das Projekt DISKURS begleitet den Aufbau und Betrieb der bundesweiten Identitätsföderation FINK wissenschaftlich und unterstützt dabei sowohl in technischen als auch organisatorischen Aspekten. Der Bedarf für eine solche Föderation ergibt sich aus der Umsetzung des Online-Zugangsgesetzes (OZG). Zusätzlich werden auch Zukunftstechnologien wie das Self-Sovereign Identity Management (SSI) untersucht und demonstriert.

Screenshot des Prototyps für SSI-basierte Online-Verwaltungsleistungen.

Das Projekt DISKURS wird vom Bayerischen Staatsministerium für Digitales gefördert. Mit der Umsetzung des OZG soll der Zugang zu Online-Verwaltungsleistungen für Bürgerinnen und Bürger vereinfacht werden. Verwaltungsgänge sollen online durchgeführt werden können. Die dazu notwendige Infrastruktur zur sicheren Authentifizierung wird mit der Föderation FINK geschaffen. Diese beruht auf der seit vielen Jahren bewährten Technologie der Security Assertion Markup Language (SAML).

Verwendung bewährter Ansätze

Durch die einschlägige Erfahrung mit dieser Technologie im universitären Umfeld kann zu Themen wie der eingesetzten Softwarearchitektur inklusive verschiedener Datenmodelle und Profile, den technischen Vertrauensniveaus und der föderationsweiten IT-Sicherheit ein wichtiger Beitrag geleistet werden.

Neben den technischen Aspekten wird auch die organisatorische Seite des Föderationsbetriebs betrachtet. Dabei werden föderationsspezifische Prozesse optimiert. Dazu zählt zum Beispiel der Austausch von Metadaten zwischen den Föderationsteilnehmern, aber auch allgemein der Bereich IT-Service-Management.

Erforschung neuer Technologien

Über die Betrachtung des Status quo der aktuellen Föderationsarchitektur hinaus wird im Projekt auch die Möglichkeit vorgestellt, Self-Sovereign-Identity-Management-Lösungen in den Bereich eGovernment aufzunehmen. Dazu werden anhand eines Demonstrators das Potenzial der SSI-Technologie gezeigt und die Umsetzbarkeit und Vorteile der Lösung präsentiert. Der Fokus liegt dabei darauf, kein komplett neues System vorzustellen, sondern Gemeinsamkeiten zwischen SSI-Ansatz und Föderation zu finden. So können bestehende Investitionen geschützt und langfristige Migrationspfade aufgezeigt werden.

Ausblick

Die Relevanz des Themas SSI und des damit verbundenen Bring-your-own-Identity-Paradigmas zeigt sich auch durch eine Vielzahl ähnlicher Projekte zu diesem Thema sowohl in Deutschland als auch der EU und weltweit. DISKURS kann dabei durch die enge Vernetzung mit den Bayerischen Föderationsprovidern und deren Führungsrolle in der Föderation FINK profitieren und die Untersuchungen auf echte Anwendungsfälle im eGovernment fokussieren.

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

Gefördert durch:
Bayerisches Staatsministerium für Digitales

Projekt Smart Hospitals

Sichere Digitalisierung Bayerischer Krankenhäuser

Smart Hospitals erforscht die Absicherung bayerischer Krankenhäuser angesichts der zunehmenden Digitalisierung. Im Krankenhaus sind heute praktisch alle Aktivitäten IT-gestützt. Hackerangriffe, Malware oder Systemausfälle sind daher eine reale Gefahr für Patienten und den Krankenhausbetrieb. Das Projekt erarbeitet in Abstimmung mit dem Landesamt für Sicherheit in der Informationstechnik Lösungen für eine sichere Digitalisierung.

Die Digitalisierung im Krankenhaus hat viele Facetten: Politik, Krankenhauspersonal, Patientinnen und Patienten fordern das digitale Krankenhaus. Krankenhäuser müssen dem nachkommen, auch um im Wettbewerb zu bestehen, wodurch mehr Handlungsdruck entsteht. Erschwert wird die Situation durch Personalmangel in der IT, teils unvollständige Expertise im Bereich IT-Sicherheit sowie unpraktische und unkonkrete Leitfäden zu dem Thema. Hinzu kommen die wachsende organisatorische Belastung und die Vielfalt der IT-Systeme. In der Summe dieser Herausforderungen schleichen sich organisatorische und technische Schwachstellen ein. Ihre Ausnutzung, z. B. durch Malware, kann nicht nur zu Datenverlust, sondern sogar zur Gefahr für die Patientengesundheit werden.

Unterstützung durch das FI CODE

Die Situation wird durch das FI CODE, gefördert durch das Bayerische Staatsministerium für Gesundheit und Pflege (StMGP), strukturiert analysiert und für die Krankenhäuser in Bayern verbessert. Dafür wurde zunächst eine mehrstufige Situationsanalyse durchgeführt: Knapp 40 % der rund 400 Krankenhäuser in Bayern nahmen an einer Umfrage zur Situation der IT-Sicherheit und Digitalisierung teil. Zusätzlich wurde bei einer zweistelligen Anzahl an Krankenhäusern eine Vor-Ort-Analyse inklusive detaillierter Gespräche mit der IT-Leitung, der Geschäftsführung sowie dem medizinischen Personal durchgeführt, wodurch wertvolle bestehende Lösungen zur Absicherung sowie offene Lücken identifiziert werden konnten.

Ein Maßnahmenkatalog für Krankenhäuser

Auf Basis der Situationsanalyse hat das FI CODE einen Maßnahmenkatalog zur Verbesserung der IT-Sicherheit von Krankenhäusern in einer ersten Ausgabe erstellt und herausgegeben. 33 Maßnahmen zu den ermittelten wichtigsten Themen berücksichtigen nicht nur die technische Perspektive, sondern auch wichtige organisatorische Aspekte und Maßnahmen zur Steigerung des Sicherheitsbewusstseins beim Krankenhauspersonal. Die Maßnahmen wurden mit dem Landesamt für Sicherheit in der Informationstechnik (LSI) in Nürnberg und mit dessen neu entwickelter Orientierungshilfe zur IT-Sicherheit in Krankenhäusern abgestimmt. Der Maßnahmenkatalog ist öffentlich auf der Website des FI CODE zugänglich.

Das Deckblatt des Maßnahmenkatalogs.

ABB.: MICHAEL GRABATIN; SIEGFRIED BRUNNER

Weitere Verbesserung

Der aktuelle Maßnahmenkatalog ist ein Zwischenergebnis. Er wurde an alle bayerischen Krankenhäuser versandt und auf Veranstaltungen mit Vertretern der Krankenhäuser diskutiert. Ihre Rückmeldung zum Maßnahmenkatalog ist eine wesentliche Grundlage für eine neue, erweiterte und aktualisierte Ausgabe im Herbst 2021.

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

Gefördert durch: Bayerisches Staatsministerium für Gesundheit und Pflege (StMGP)

Prof. Dr. Johannes Kinder

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

Die Arbeitsgruppe PATCH beschäftigt sich seit ihrer Gründung 2019 durch Prof. Dr. Johannes Kinder mit der Absicherung von Software. In unserer Gruppe entwickeln wir Systeme zur Programmanalyse, um Software automatisch verstehen und härten zu können. Besonderen Wert legen wir dabei auf den Transfer von theoretisch fundierten Konzepten in die Praxis.

Eröffnung der ACM CCS 2019 in London durch Prof. Dr. Kinder und Prof. Dr. Cavallaro.

PATCH STEHT FÜR „Program Analysis, Transformation, Comprehension, and Hardening“, und entsprechend arbeitet die Forschungsgruppe unter der Leitung von Prof. Dr. Kinder an der Analyse, der Transformation, dem Verstehen und der Härtung von Software.

Programmanalyse und Fehlererkennung

Automatische Methoden, wie z. B. statische Analyse oder Fuzzing, können heutzutage viele klassische Softwarefehler wie Überläufe in C-Programmen finden. Nach wie vor sind aber Softwarefehler eine Hauptursache für IT-Sicherheitsprobleme. Wir beschäftigen uns in der Forschung mit den Problemen, die in der Praxis durch komplexe Laufzeitumgebungen entstehen, z. B. in JavaScript-Ökosystemen wie Node.js oder durch neuartige Plattformen wie WebAssembly.

Programmverstehen und Reverse Engineering

Um Software vor dem Einsatz auf ihre Eignung und Sicherheit zu überprüfen, entwickeln wir automatische Verfahren zum Kategorisieren und Verstehen von Programmbestandteilen. So können z. B. Hintertüren entdeckt oder Schadsoftware erkannt werden. Wir entwickeln hierfür sowohl klassische Ansätze mit formalen Methoden als auch Modelle mit neuronalen Netzen und statistischem maschinellem Lernen. Die Bandbreite der Anwendungen reicht dabei von Desktopanwendungen, Dienstprogrammen und Gerätetreibern zu mobilen Apps.

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.

Internationale Vernetzung

Wir legen besonderen Wert auf Vernetzung mit der internationalen Forschungsgemeinschaft im Bereich der IT-Sicherheit. Einhergehend mit einem Fokus auf Veröffentlichungen mit höchster internationaler Sichtbarkeit nehmen wir regelmäßig an den führenden akademischen Konferenzen teil. Im Jahr 2020 bedeutete dies vor allem Videoübertragungen zu – in Europa – später Stunde. Dabei gab es im November 2019 noch einen Höhepunkt mit der Organisation der ACM Conference on Computer and Communications Security (CCS) in London durch Prof. Dr. Kinder, gemeinsam mit Prof. Dr. Cavallaro vom King’s College London. Auf dieser international führenden Konferenz kamen über 1.200 Wissenschaftlerinnen und Wissenschaftler zusammen, um die neuesten Forschungsergebnisse vorzustellen und zu diskutieren.

Prof. Dr. Johannes Kinder
johannes.kinder@unibw.de
+49 89 6004 7335
www.unibw.de/patch

ABB.: ISTOCK / MF3D; MIA ROBERTSON

Sicherheitstests für dynamische Sprachen

Das ExpoSE-System generiert automatisch Tausende von Tests für komplexe JavaScript-Programme

Dynamische Programmiersprachen bilden die Grundlage des World Wide Web und werden sowohl in Webbrowsern als auch auf Servern ausgeführt. So können schnell Funktionen, Websites und Systeme aufgesetzt werden, aber auch leicht Fehler entstehen. Im EASTEND-Projekt (Efficient Automatic Security TEstiNg for Dynamic Languages) entwickeln wir neue Methoden, um Fehler in JavaScript-Programmen automatisch zu finden.

Das Projekt zeigt, dass eine dynamische Verifikation am besten zu einer inhärent dynamischen Sprache passt. Wir verwenden dynamische symbolische Ausführung (DSE), um systematisch Testfälle zu erzeugen, die Sicherheitseigenschaften entlang einzelner Programmpfade überprüfen. DSE liefert dabei zwar keine Beweise, aber alle Tests und Fehler sind garantiert im Programmkontext erreichbar. Die beiden Teilbereiche des Projekts waren die Verbesserung von DSE für JavaScript und die Entwicklung einer flexiblen Spezifikationsmethode für Sicherheitseigenschaften.

Symbolische Ausführung von JavaScript

ExpoSE, unsere Open-Source-DSE-Engine für JavaScript, die wir im Rahmen des Projekts entwickelt haben, kann für die meisten Node.js-Programme vollautomatisch Testfälle generieren. Die Herausforderung für JavaScript ist vor allem seine komplexe Semantik und umfangreiche Standardbibliothek. Insbesondere verarbeiten die meisten JavaScript-Programme Strings und reguläre Ausdrücke, die viele Arten von automatisierter Analyse verhindern.

In diesem Projekt haben wir die erste vollständige Strategie zur Verarbeitung von regulären Ausdrücken in symbolischer Ausführung vorgestellt. Die entsprechende Semantik konnten wir mithilfe von Bedingungen über Strings und klassische reguläre Ausdrücke codieren. Ein automatisches Schema zur Verfeinerung der Bedingungen löst dabei das Problem der Auswertungsreihenfolge und der Greediness: Reguläre Ausdrücke lesen so viele Eingabezeichen wie möglich von links nach rechts. Diese Einschränkung wurde bisher in verwandten Arbeiten und vorhandenen Codierungen für reguläre Ausdrücke ignoriert.

Reguläre Ausdrücke in NPM

Unsere Studie von über 400.000 JavaScript-Paketen aus dem NPM-Software-Repository zeigt, dass ein Fünftel komplexe reguläre Ausdrücke verwendet, die unsere Technik benötigen. Wir haben unser Codierungs- und Verfeinerungsschema in ExpoSE implementiert und es auf 1.131-Node.js-Paketen evaluiert. Wir konnten zeigen, dass die Codierung effektiv ist und die Testabdeckung um bis zu 30 % erhöhen kann. Dies bedeutet, dass unsere Codierung erlaubt, zusätzliche Testfälle zu generieren, die Fehler und Schwachstellen in bisher unerreichbaren Teilen des Programms finden könnten.

Die Codierung, Verfeinerung und Bewertung beschreiben wir in einem Artikel, der auf der ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI) veröffentlicht wurde, einer der beiden führenden internationalen Konferenzen auf diesem Gebiet.

Einige sicherheitsrelevante Eigenschaften wie die Herkunft oder Integrität von Daten können nicht als Asserts in JavaScript selbst geschrieben werden. Wir haben daher einen Ansatz entwickelt, um einer Sprache zusätzliche Sicherheitsannotationen hinzuzufügen. Diese einfache Metatheorie von Sicherheitsannotationen ermöglicht es, in Tests Eigenschaften zu überprüfen, die nicht im Programmzustand enthalten sind. Wir haben die Konsistenz unseres Systems in einem statisch typisierten Lambda-Kalkül (veröffentlicht auf PEPM 2018) demonstriert und anschließend eine vollständig dynamische Referenzimplementierung für JavaScript entwickelt. Einen Teil der WebCrypto-API konnten wir mit Sicherheitsannotationen ausstatten und zeigen, wie Sicherheitslücken erkannt werden können. Diese Arbeit wurde auf dem 2019 European Symposium on Research in Computer Security (ESORICS) veröffentlicht, der führenden europäischen Konferenz auf diesem Gebiet.

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+49 89 6004 7335

www.unibw.de/patch

Gefördert durch: UK Government & Engineering and Physical Sciences Research Council (EPSRC)

Reverse Engineering trifft Deep Learning

KI imitiert menschliche Softwareentwickler bei der Benennung von Funktionen im Binärcode

Computerprogramme werden in Quelltext geschrieben und zur Ausführung in eine Binärform übersetzt, die nur noch der Computer versteht. Da Quelltext in vielen Situationen nicht verfügbar ist, können Menschen nur schwer einschätzen, welches mögliche Verhalten in einem binären Programm steckt. Unser maschinelles Lernsystem ist darauf trainiert, Komponenten in Binärdateien mit Namen zu versehen, die dem ursprünglichen Quelltext ähneln.

Funktionsnamen, Kommentare und andere Informationen im Quelltext helfen, die Funktionsweise eines Computerprogramms zu verstehen. Solche Informationen sind normalerweise nicht in den an Endbenutzer verteilten ausführbaren Binärdateien enthalten, und selbst ein Disassembler kann diese Daten nicht rekonstruieren. Dies hilft zwar beim Schutz von geistigem Eigentum, erschwert jedoch die Erkennung von Schadcode und Sicherheitslücken erheblich.

Unsere Arbeit zielt darauf ab, das Verstehen von Programmcode zu automatisieren und so menschenlesbare Informationen zu erzeugen. Wir entwickeln hierfür ein Deep-Learning-Modell, das Strukturen in Programmen Namen und Informationen zuordnen kann. Mit unserer Technik können wir schnell relevante Teile eines Programms zur weiteren Untersuchung identifizieren. Die Idee besteht darin, eine numerische Darstellung des Maschinencodes zu lernen. Um unser Modell zu trainieren, verwenden wir große Mengen an Open-Source-Software, da wir hier Quelltextinformationen eindeutig dem entsprechenden Binärcode zuordnen können.

Funktionsnamen für Binärdateien

Es ist schwierig vorherzusagen, welche Namen von Menschen für bestimmte Objekte vergeben werden. Beispielsweise könnte ein Bild einer Orange als Frucht, Farbe oder Lebensmittel gekennzeichnet sein. Alle diese Beschriftungen sind zwar korrekt, aber nicht eindeutig. Ebenso können ähnliche Funktionen in Maschinencode sehr unterschiedlich benannt werden.

Ohne Debugging-Informationen können Disassembler nur generische Namen vergeben.

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

Wir beginnen mit der Analyse kompilierter Programme, die Debugging-Informationen enthalten, um den Namen und die Position von sogenannten Symbolen zu bestimmen. Ein Symbol beschreibt den Speicherort, den Typ und den Namen einer Struktur in einer Binärdatei. Unser Tool analysiert dann, wie dieses Symbol mit anderen Symbolen interagiert. So können wir ein Diagramm aller Symbole aus einem Programm erstellen, in dem die Verbindungen unterschiedliche Beziehungen darstellen. Nachdem wir die Symbole einer Binärdatei und die Merkmale jedes Symbols extrahiert haben, repräsentieren wir jedes Objekt durch einen Vektor. Dieser Vektor codiert Beziehungen zwischen Symbolen, die wir wiederum einer Menge an natürlichsprachlichen Tags zuordnen, Fragmenten von Funktionsnamen. Für eine gegebene Menge solcher Tags können wir so auch einen Namen für Binärcode vorhersagen, den wir so noch nie gesehen haben. Mit Hilfe dieser Tags lassen sich dann auch Funktionsnamen konstruieren, die in Schadsoftware oder auch kommerzieller Software entfernt wurden.

Eine erste Version und Implementierung unseres Ansatzes beschreiben wir in einem Beitrag, der auf der 2020 Annual Computer Security Applications Conference (ACSAC) veröffentlicht wurde.

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+ 49 89 6004 7335

www.unibw.de/patch

Gefördert durch: Engineering and Physical Sciences Research Council (EPSRC) & Forschungsinstitut CODE

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 HoBIT

Hochsichere Betriebssysteme für Embedded IT

Das Projekt HoBIT entwickelte Methoden, mit denen sich formale Programmverifikation mit dem Ziel der IT-Sicherheit in der Praxis auf Betriebssysteme und Betriebssystemkomponenten anwenden lässt. Dabei wird insbesondere die Verifikation von existierenden und neu entwickelten Programmen in der Sprache C unterstützt, die im Bereich der Betriebssysteme nach wie vor dominant ist.

Systeme und Geräte mit eingebetteten IT-Funktionen sind höchstens so sicher wie das Betriebssystem (BS), das als zentrale Basis aufbauend auf der Hardware verwendet wird. Der BS-Kern läuft im freizügigsten Modus der Hardware. Wenn er kompromittiert wird, kann das Verhalten aller Hard- und Softwarekomponenten im System modifiziert werden. Programmierfehler können direkt zu unerwünschtem Verhalten führen oder bilden ein Einfallstor für Angriffe. Die wirksamste Maßnahme gegen Fehler ist ein formaler Beweis der Fehlerfreiheit. Allerdings sind solche Beweise bisher nur für Programme durchführbar, die deutlich kleiner als praktisch verwendete BS-Kerne sind.

Mikrokernels

Die Antwort darauf sind Mikrokernels mit stark reduziertem Funktionsumfang, die klein genug für formale Verifikation sind. Die wichtigste verbleibende Funktionalität ist die strikte Separierung der übrigen Softwarekomponenten untereinander, vom Mikrokernel und von der Hardware. Mit solchen weiteren Komponenten können dann die übrigen BS-Funktionen implementiert werden. Zusammen mit dem Mikrokernel ergeben sie ein vollständiges Betriebssystem.

Der seL4-Mikrokernel wurde bereits erfolgreich formal verifiziert. Seine Architektur erlaubt die Entwicklung von Betriebssystemen, die ähnlich performant sind wie die existierenden monolithischen BS-Kernels. Das durch Hensoldt Cyber entwickelte BS TRENTOS ist in dieser Weise aufgebaut. Das Ziel des HoBIT-Projekts waren Methoden und Werkzeuge, mit denen sich mittels formaler Verifikation ähnliche Sicherheitseigenschaften für das Betriebssystem erreichen lassen wie für den Mikrokernel selbst.

Die strikte Trennung der übrigen Komponenten hat zur Folge, dass sich die Kompromittierung einer Komponente nicht auf andere Teile des Systems auswirken kann. Eine kompromittierte Komponente kann aber immer noch ein hohes Sicherheitsrisiko für Systeme in einer kritischen Umgebung darstellen. Ein kompromittierter Netzwerktreiber kann beispielsweise wichtige Kommunikationskanäle blockieren oder vertrauliche Daten in andere Kanäle umleiten. Daher ist es notwendig, formale Verifikation zumindest auf einen Teil der weiteren BS-Komponenten anzuwenden.

Verifikation von BS-Komponenten für die Praxis

Formale Verifikation funktioniert am besten, wenn ein Programm von vornherein für dieses Ziel entwickelt wird, möglichst in einer dafür geeigneten höheren Programmiersprache. Im HoBIT-Projekt untersuchten wir die von Data61 (CSIRO, UNSW Sydney) entwickelte funktionale Programmiersprache Cogent. Neben der Übersetzung von abstrakter Hochsprachenebene in ausführbaren Code wird hier ein „Refinement“-Beweis dafür generiert, dass sich das Ergebnis wie erwartet verhält.

In der Praxis werden BS-Komponenten aber meist in C programmiert, einer maschinennahen Programmiersprache, die ein Alptraum für formale Verifikation ist. Dies betrifft auch noch neu entwickelte Komponenten, da den hochspezialisierten Entwicklern C meist am vertrautesten ist. Unser Ansatz in HoBIT war es daher, für die formale Verifikation von C-Code das Unterstützungswerkzeug Gencot zu entwickeln, das halbautomatisch C nach Cogent übersetzt. Sein Ziel ist die Unterstützung von C-Programmierern bei der Überführung von C-Programmen nach Cogent, um so eine formale Verifikation zu ermöglichen. Als Demonstration wurde es erfolgreich verwendet, um für in C implementierte TRENTOS-Komponenten alternative Cogent-Implementierungen zu erzeugen. 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

Prof. Dr. Arno Wacker

Datenschutz und Compliance

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

Eines unserer wichtigsten Ziele ist es, den Datenschutz und die IT-Sicherheit nicht nur zu erforschen und zu lehren, sondern auch im Alltag zu leben. Nur so lassen sich diese Themenkomplexe den Studierenden überzeugend und authentisch vermitteln. Darüber hinaus möchten wir auch der breiten Öffentlichkeit demonstrieren, dass datenschutzfördernde Technologien in den Alltag integrierbar sind, im privaten wie im geschäftlichen Bereich.

Lehre

Die Lehre in der Professur unterteilt sich in Penetrationstesting, Datenschutz, Privacy Enhancing Technologies, Kryptologie und Sichere Netze und Protokolle. Diese vermittelt den Studenten 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 als Ziel, die Privatheit des Einzelnen zu stärken, sowie die Erforschung von Kommunikationsregeln für das Internetzeitalter.
- Die Erhöhung des IT-Sicherheitsbewusstseins (Awareness) befasst sich unter anderem mit dem Bereich „Selbstdatenschutz“. Dazu entwickelt und erforscht die Professur unter anderem Verfahren und Werkzeuge zur Steigerung des Sicherheitsbewusstseins bei der Entwicklung von Softwarewerkzeugen bzw. im Umgang mit diesen.
- 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 unserer Professur ist es, interessierte Bürger fortzubilden, aufzuklären und in Fragen der IT-Sicherheit zu schulen und zu informieren. Diese Aufgabe verfolgen wir mithilfe von Vorträgen und Workshops, welche sich z. B. mit Penetrationstesting, sicherem E-Mail-Verkehr im Alltag und Aufspüren von Sicherheitslücken befassen. Für Letzteres bietet die Professur z. B. 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

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

ABB.: ISTOCK / MATEJMO; ISTOCK / BAKS

Projekt „Redundante Strukturen in verteilten Overlay-Netzen“

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 durch die Schaffung und Ausnutzung von Redundanzen bezüglich Datenspeicherung und Konnektivität und entsprechende Vermeidung einzelner Ausfallpunkte.

Die Netzwerkinfrastruktur vieler Internetdienste folgt dem zentralisierten Ansatz. Ein zentraler Knoten wie z. B. ein Webserver, der von einem Unternehmen oder einer Organisation gesteuert wird, dient als Rückgrat des Systems. Er fungiert als Relais bei der Kommunikation zwischen allen anderen Knoten und stellt die meisten oder alle Systemressourcen bereit. Die Teilnahme an einem solchen zentralisierten System ist einfach. Alles, was andere Knoten, das heißt Benutzer, tun müssen, ist eine Verbindung zu diesem zentralen Knoten herzustellen.

Overlay-Netze ohne zentralen Knoten.

Folglich hängt die Verfügbarkeit eines solchen Systems vollständig von der Verfügbarkeit des zentralen Knotens und der Verfügbarkeit des Netzwerkpfads dorthin 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 eines oder mehrerer dedizierter Rechenzentren implementiert. Auch wenn der Betreiber möglicherweise umfangreiche Maßnahmen ergreift, kann ein ausreichend schwerwiegender technischer Fehler, eine Fehlkonfiguration oder ein erfolgreicher Angriff dennoch zu einem nicht verfügbaren zentralen Knoten und damit zu einem nicht verfügbaren System führen. Abgesehen von technischen Fehlern oder Angriffen 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, z. B. 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, z. B. 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 bei dem zentralisierten Ansatz die Interaktion mit dem zentralen Knoten für die Teilnahme ausreicht, erfordert der vollständig verteilte Ansatz häufig die Interaktion mit mehreren Knoten. Die Identität und Anzahl dieser Knoten können von Interaktion zu Interaktion variieren.

Ein Ziel dieser Forschung ist es, große, vollständig verteilte Systeme durch Analyse und Verbesserung der Netzwerkresilienz gegen gezielte Angriffe und technische Ausfälle zu schützen. Die Mittel hierfür sind die Schaffung und Ausnutzung von Redundanzen bei der Datenspeicherung und Netzwerkkonnektivität, wobei einzelne Ausfall- und Kontrollpunkte vermieden werden und die Wahrscheinlichkeit, dass Dienste nicht verfügbar sind oder zensiert werden, verringert wird.

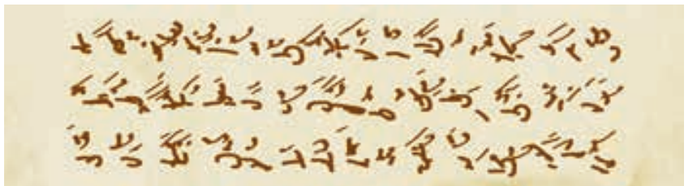
Prof. Dr. Arno Wacker
arno.wacker@unibw.de
+49 89 6004 7325
www.unibw.de/datcom

Projekt DECRYPT: Entschlüsselung historischer Manuskripte

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. So können historische Manuskripte entschlüsselt und kontextualisiert werden, welche bislang in Archiven und Bibliotheken verborgen sind.

Für unser kollektives Gedächtnis sind handgeschriebene historische Aufzeichnungen eine Schlüsselkomponente, ohne die ein Verständnis stark eingeschränkt wäre. 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 entschlüsselt. Folglich bedarf es, während ein Schlüsselaspekt 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 Forscher oft ohne Zugang zu automatischen Methoden arbeiten, die die Entschlüsselung unterstützen und beschleunigen können. Zur gleichen Zeit entwickeln Informatiker, Kryptologen und Computerlinguisten automatische Entschlüsselungsalgorithmen zur Identifizierung und Entschlüsselung verschiedener Chiffrentypen, ohne Zugang zu verschiedenen Arten von echten Geheimtexten zu haben.



In Bibliotheken und Archiven finden sich noch viele ungelöste Rätsel.

ABB.: ISTOCK / METAMORWORKS; ISTOCK / CARDUUS

Ziel des Projekts ist es, ein neues interdisziplinäres wissenschaftliches Feld der historischen Kryptologie zu etablieren, und zwar durch das Zusammenbringen des Fachwissens der verschiedenen Disziplinen für das Sammeln von Daten und den Austausch von Methoden für schnellere Fortschritte beim Entschlüsseln und Kontextualisieren historischer Manuskripte, die bisher in den Archiven und Bibliotheken verborgen sind.

Konkret wird das Projekt zu einer öffentlich zugänglichen Datenbank führen, mit tausenden verschlüsselten Manuskripten und Verschlüsselungsschlüsseln mit Informationen über ihre Herkunft und anderen relevanten Dokumenten. Dem Benutzer der Datenbank wird die Möglichkeit geboten, ein verschlüsseltes Manuskript als Bild hochzuladen und den Text vom System automatisch transkribieren und decodieren zu lassen. Dies ist zurückzuführen auf Bildverarbeitungs- und Entschlüsselungsalgorithmen, die während des Projekts entwickelt und mit der Datenbank verknüpft werden. Zusätzlich entsteht auch eine große Sammlung historischer Texte aus verschiedenen Zeitperioden und Sprachmodellen für 15 europäische Sprachen in einem standardisierten Format, das Recherchen und Studien von Sprachvariationen und Veränderungen im Laufe der Zeit ermöglicht.

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.

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

Gefördert durch:
Swedish Research Council (SRC)

Addendum

Publikationen und Aktivitäten

ABB.: BIBLIOTHEK HFT STUTTGART / WIKIMEDIA CC

Prof. Dr. Florian Alt

Benutzbare Sicherheit und Privatsphäre

Publikationen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Forschungsprojekte

ubihave

Das ubihave-Projekt untersucht, wie ubiquitäre Technologien von Verhaltensmodellen profitieren können. Die Forschung ist dadurch motiviert, dass persönliche Geräte und intelligente Umgebungen dank ihrer Sensorik und Rechenleistung reichhaltige benutzerspezifischer Daten zur Verfügung stellen können. Dadurch eröffnen sich neue Wege für Anwendungen, welche Verhaltensmodelle verwenden, um sich an individuelle Benutzer und Kontexte anzupassen.

Drittmittelgeber:
Deutsche Forschungsgemeinschaft (DFG)
Laufzeit: 01/2019–07/2021

Scalable Biometrics

In diesem Projekt untersuchen wir, wie Umgebungen, in welchen Computer und Sensoren allgegenwärtig sind, genutzt werden können, um Nutzer mithilfe verhaltensbiometrischer Systeme zu identifizieren und zu authentifizieren. Ziel ist es, herauszufinden, wie solche verhaltensbiometrischen Ansätze unter Veränderungen von Umgebung, Anzahl der Personen und ihrer Eigenschaften sowie der verwendeten Technologie skalieren.

Drittmittelgeber:
Deutsche Forschungsgemeinschaft (DFG)
Laufzeit: 04/2020–03/2023

Promotionen

Michael Braun
Affective Automotive User Interfaces

Diese Dissertation erforscht affektive Benutzerschnittstellen im Fahrzeug. Der Fokus liegt auf zwei Interaktionsparadigmen: (1) Systeme, welche auf den aktuellen emotionalen Zustand des Benutzers basierend auf Echtzeitdaten reagieren; (2) Synthese emotionsgesteuerter Interaktion, welche sich dem emotionalen Zustand des Benutzers anpasst. Die Ziele dieser beiden Ansätze sind die Förderung von sicherem Verhalten und eine Verbesserung der Benutzererfahrung.

Eva Lösch
Unterstützung der Exploration von mehrbenutzerfähigen interaktiven Informationstafeln im (halb) öffentlichen Raum

Diese Dissertation entwickelt ein Konzept zur Unterstützung der Exploration von interaktiven Informationsdisplays im (halb-)öffentlichen Raum. Das Konzept basiert auf der Verwendung von visuellen Stimuli, um die Aufmerksamkeit und das Verhalten der Benutzer während der Exploration zu lenken. In insgesamt drei Studien wird dieses Konzept evaluiert und iterativ verbessert, sodass es die Benutzer in allen Phasen der Exploration zufriedenstellend unterstützt.

Lehre

11671 **Mensch-Computer-Interaktion (WT)**

11672 **Projekt Mensch-Computer-Interaktion (FT)**

36651 **Benutzbare Sicherheit (FT)**

36653 **Praktikum Design sicherer und benutzbarer Systeme (FT)**

3665-V1 **Sichere Mensch-Maschine-Schnittstellen (WT)**

Messen, Tagungen, Seminare

Mensch und Computer 2020 (Mitausrichter)

06–09/08/2020, Magdeburg

Die „Mensch und Computer" ist die größte europäische HCI-Konferenz und bringt in einer 4-tägigen Veranstaltung Forscher und Praktiker im Rahmen verschiedener Tracks und Workshops zusammen.

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

25–30/04/2020, Honolulu, HI, USA

Ziel dieses Workshops ist es, ein gemeinsames Verständnis für die Herausforderungen und Möglichkeiten zu entwickeln, die intelligente Geräte und Umgebungen für eine sichere und nutzbare Authentifizierung schaffen.

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

02–05/06/2020, Stuttgart/Ulm

Augenbewegungen sind unauffällig und daher attraktiv für Sicherheits- und Datenschutzzwecke. DerEyeSec-Workshop ermöglicht Forschenden und Praktikern, Wege für zukünftige Forschung auf diesem Gebiet zu entdecken.

How to do HCI research if your users are off-limits? (Moderation)

In dieser Online-Veranstaltung wurden Erfahrungen darüber ausgetauscht, wie nutzerzentrierte Forschung in Zeiten vorangetrieben werden kann, in denen keine Laborstudien möglich sind.

How to make remote HCI teaching useful, engaging and exciting? Is your online course really better than a book? (Moderation)

In dieser Talkshow diskutieren Lehrende der Mensch-Maschine-Interaktion Strategien, um Lehren und Lernen angenehm zu gestalten – auch, wenn keine Präsenzlehre möglich ist.

Patente, Preise, Auszeichnungen

Best of CHI Honorable Mention Award

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

Weitere Funktionen

Leitung des Programmkomitees

- ACM Human Factors in Computing Systems (Subcommittee Chair)
- Mensch und Computer 2020

Mitglied des Programmkomitees

- 2020 European Workshop on Usable Security (EuroUSEC 2020)
- 3rd International Conference on Artificial Intelligence & Virtual Reality (AIVR 2020)
- Augmented Humans 2020

Kooperationen

Universität Duisburg-Essen: Behavioral Biometrics

Zusammen mit Prof. Dr. Stefan Schneegass untersuchen wir im Rahmen des Projekts „Scalable Biometrics" wie verhaltensbiometrische Ansätze unter Veränderungen von Umgebung und Technologie skalieren.

Technische Universität Darmstadt (Telecooperation Lab): Mentale Modelle in Smart Homes

In einem gemeinsamen Forschungsprojekt mit Karola Marky (M.Sc.) und Prof. Dr. Max Mühlhäuser untersuchen wir die mentalen Modelle von Nutzern sowie Besuchern in Smart Home, insbesondere im Hinblick auf deren Verständnis von Datensammlung und -speicherung.

Universität Glasgow: Einsatz von Eyetracking für Benutzbare Sicherheit

Mit Dr. Mohamed Khamis arbeiten wir an der Entwicklung neuartiger Sicherheitsmechanismen basierend auf Eye Tracking und untersuchen, wie bestehende Systeme mittels Blickinformationen hinsichtlich Sicherheit und Benutzbarkeit verbessert werden können.

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

Gemeinsam mit Ludwig Trotter (M.Sc.) und Prof. Nigel Davies untersuchen wir Nutzererfahrungen im Rahmen des „Internet of Things" (IoT) – insbesondere Fälle, in denen Benutzer dauerhaft oder vorübergehend in der Nutzung oder dem Zugriff auf IoT-Geräte eingeschränkt wurden (beispielsweise durch Einstellung des Produkts/Dienstes durch den Hersteller).

Universität Lissabon: Blickverhalten in Virtueller Realität

Zusammen mit Prof. Augusto Esteves (Instituto Superior Técnico) erforschen wir den Nutzen physiologischer Benutzerschnittstellen im Kontext von persönlichen Headsets und Brillen der erweiterten Realität (Augmented Reality), insbesondere adaptive Benutzerschnittstellen, personalisierte Informationen, und neue Eingabemöglichkeiten.

LMU München: User Interfaces for Cryptocurrencies

Gemeinsam mit Prof. Dr. Albrecht Schmidt aus der Medieninformatik arbeiten wir an der Verbesserung der Benutzbarkeit von Nutzerschnittstellen für Kryptowährungen. Insbesondere entwickeln wir neuartige Oberflächenkonzepte und Interaktionstechniken unter Berücksichtigung verschiedener Bedrohungsmodelle.

Prof. Dr. Harald Baier

Digitale Forensik

Lehre

3824 **Digitale Forensik**

Messen, Tagungen, Seminare

- CAST-Workshop Forensik/Internetkriminalität am 10.12.2020, https://cast-forum.de/workshops/infos/292?ts=1606324027548

Kooperationen

- Nationales Zentrum für angewandte Cybersicherheit ATHENE
- Hochschule Darmstadt
- TU Darmstadt
- Friedrich-Alexander-Universität Erlangen-Nürnberg
- Frankfurt University of Applied Sciences
- Vietnamese German University
- Hessisches Landeskriminalamt
- Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

Publikationen

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

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

Forschungsprojekte

Airborne Cyber Security Enhancement

Das Forschungsinstitut CODE und Airbus Defence & 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.

Drittmittelgeber:
Airbus Defence & Space, Manching
Laufzeit: 2020–2024

Lehre

1009 **Seminar Ausgewählte Kapitel aus Programmiersprachen** (HT + WT)

1009 **Seminar Sprachbasierte Sicherheit** (WT + FT)

3584 **Praktikum Language-based Security** (HT)

3647 **Compilerbau** (HT)

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

Messen, Tagungen, Seminare

Organisator des „CODE Colloquium"

Das CODE Colloquium entspricht einer „Distinguished Speaker Series" aus den USA, zu der hochkarätige Wissenschaftler für Vorträge, Diskussionen und Gespräche mit Doktoranden eingeladen werden.

Weitere Funktionen

- Fakultätsratsmitglied
- Prodekan
- Prüfungsausschussvorsitzender Masterstudium Cybersecurity

Kooperationen

Mathias Payer, EPFL

Stijn Volckaert, KU Leuven

Prof. Dr. Gabi Dreo Rodosek

Kommunikationssysteme und Netzsicherheit

Publikationen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Forschungsprojekte

BGM-Tool

Erstellung eines wissenschaftlich nutzbaren Buchungs- und Reportingtools im Rahmen von Maßnahmen des betrieblichen Gesundheitsmanagements im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg).

Förderer: Sanitätsakademie der Bundeswehr
Laufzeit: 04/2018–12/2020

BMBF-Verbundprojekt BERKoS

Aufbau einer Wissens-Community-Plattform mit dem Ziel, deutsche Antragsteller bei der Einwerbung von europäischen Fördermitteln im Bereich der allgemeinen Sicherheitsforschung zu unterstützen.

Förderer: BMBF, VDI-Technologiezentrum
Laufzeit: 06/2017–02/2021

Cyber Range

Konzeption und effiziente Nutzung von Cyber Ranges in Bezug auf Cyber-Technologie-Entwicklung, Systemtests und die Ausbildung von Netzadministratoren, Netzoperatoren und IT-Sicherheitspersonal.

Förderer: BMVg, BAAINBw
Laufzeit: 2018–06/2023

FLIP – Flexible IP-Wellenform

Erstellung einer modularen Wellenform mit einzelnen, flexibel austauschbaren Bestandteilen, mit dem Ziel, eine an jeweilige Gegebenheiten angepasste und leistungsstarke sichere Datenübertragung zu ermöglichen.

Förderer: BMVg, BAAINBw
Laufzeit: 03/2017–04/2021

Horizon-2020-Projekt CONCORDIA

Errichtung eines Cybersecurity-Kompetenznetzwerks mit führenden Kapazitäten in den Bereichen Forschung, Technologie, Indust rie und Öffentlichkeit. CONCORDIA bietet Exzellenz und Führung in Technologie, Prozessen und Dienstleistungen, um ein nutzerzentriertes, EU-integriertes Cybersicherheits-Ökosystem für eine digitale Souveränität der EU zu etablieren.

Förderer: Europäische Kommission
Laufzeit: 01/2019–12/2022

IT-Trendbeobachtung Cyber für das BAAINBw aus Forschungssicht

Weltweite Beobachtung von innovativen IT-Sicherheitstrends aus Sicht der Forschung und Analyse ihrer Potenziale für die Zukunft sowie Durchführung eines jährlichen Cyber-F&T-Symposiums.

Förderer: BAAINBw
Laufzeit: 02/2018–11/2021

Mikrokernel für IT-sicherheitsrelevante Anwendungen

Konzeption und Erprobung von softwaretechnischen Maßnahmen zur Integration von sicheren und verifizierbaren Mikrokernen in IT-Sicherheitsanwendungen und sicheren IT-Systemen.

Förderer: Airbus Defence and Space
Laufzeit: 09/2019–12/2023

Moving Target Defence

Ziel ist die Identifizierung, Bewertung, Auswahl und Weiterentwicklung von netzbasierten Moving-Target-Defence-Technologien sowie die Etablierung einer starken akademischen Forschung im Bereich MTD.

Förderer: BMVg, BAAINBw
Laufzeit: 2018–06/2023

Postquantum-Kryptographie

Analyse und Entwicklung von kryptographischen Algorithmen im Themenbereich der Postquantum-Kryptographie.

Förderer: Infineon Technologies
Laufzeit: 05/2019–03/2023

TDL mit nationalen Domänen

Analyse und Evaluation von Sicherheitsaspekten bei der Implementierung von taktischen Datenlinks sowie Entwicklung von Verfahren zur Automatisierung der Implementierungsprozesse.

Förderer: BAAINBw
Laufzeit: 10/2019–11/2022

Promotionen

Renners, Leonard
Adaptive Prioritization of Network Security Incidents

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

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

Lehre

10102 **Netzsicherheit** (WT)

10103 **Praktikum Netzsicherheit**

10248 **Praktikum IT-Sicherheit** (HT)

102412 **Praktikum Rechnernetze**

11971 **Rechnernetze** (WT)

11972 **Mobile Kommunikationssysteme** (HT)

11975 **Praktikum Rechnernetze 2**

38202 **Praktikum Quantencomputer-Programmierung**

55131 **Sichere Mobile Systeme** (FT)

Seminar Cyber Defense (WT)

Seminar IT-Sicherheit (WT)

Messen, Tagungen, Seminare

Workshop Post Quanten Crypto

Am 28.01.2020 wurde am Forschungsinstitut CODE ein Workshop zum Thema Post-Quanten-Computer und Post-Quanten-Kryptogramme in Kooperation mit den Firmen Infineon und Giesecke + Devrient durchgeführt.

Virtueller Hackathon am IBM-Q-Hub der UniBwM

Vom 30.03. bis 03.04.2020 wurde am Forschungsinstitut CODE ein online Hackathon zum Thema Quantencomputing in Kooperation mit Kollegen des DLR und der LMU organisiert.

Virtueller Hackathon am IBM-Q-Hub der UniBw M

Vom 12.10. bis 16.10.2020 wurde am Forschungsinstitut CODE ein Online-Hackathon zum Thema Quantencomputing in Kooperation mit Kollegen des DLR und der LMU organisiert.

Patente, Preise, Auszeichnungen

Auszeichnung der wissenschaftlichen Mitarbeiter Raphael Labaca Castro und Sinclair Schneider, die mit ihren Beiträgen zum Thema „Adversarial Camouflage: Adversarial Machine Learning as Concealment for Military Operations“ und „Intelligent News Analysis“ unter die Top 10 der Einreichungen bei der Innovationstagung der CODE2020 kamen.

Weitere Funktionen

- Leitende Direktorin des Forschungsinstituts CODE
- Mitglied des Digitalrats des BMVg
- Mitglied des Beirats und Aufsichts rats der Giesecke+Devrient GmbH
- Mitglied des Aufsichtsrats der Siltronic AG
- Mitglied des Datenschutzbeirats der Deutschen Telekom AG
- Mitglied des Aufsichtsrats der BWI GmbH
- Mitglied des Global Future Council on Cybersecurity des World Economic Forums
- Mitglied der wissenschaftlichen Arbeitsgruppe des Nationalen Cybersicherheitsrats
- Mitglied des Kuratoriums der Kunsthalle
- Mitglied des Vorstands des Sicherheitnetzwerks München e. V.
- Mitglied des Fachgremiums IT der BaFin
- Mitglied des Beirats von Deutschland sicher im Netz (DsiN) e. V.
- Koordinatorin des EU-Projekts CONCORDIA
- Mitglied des Münchner Kreises
- Mitglied des Wirtschaftsbeirats Bayern
- Mitglied des Münchner Klubs
- Gutachterin für EU-H2020-Projekte
- Mitglied des Munich Security Conference Security Innovation Board

Kooperationen

Universität Twente (NL)

Die wissenschaftliche Zusammenarbeit besteht seit mehreren Jahren und umfasst den Austausch wissenschaftlichen Personals, die gemeinsame Bearbeitung von Forschungsprojekten sowie die Planung und Durchführung von Lehr- und Trainingsveranstaltungen. Es besteht weiterhin eine Kooperation zur gemeinsamen Durchführung von Promotionsvorhaben (Joint PhD Program).

Technische Universität München

Eine intensive Zusammenarbeit mit dem Lehrstuhl von Prof. Dr. Wolfgang Kellerer findet in den Bereichen Internet of Things (IoT) und 5G statt. Hier wird eine gemeinsam genutzte Forschungsinfrastruktur aufgebaut.

Munich Network Management Team (MNM-Team)

Der Lehrstuhl ist Mitglied im Munich Network Management Team (MNM-Team). Das MNM ist eine Forschungsgruppe mit Wissenschaftlern an der LMU, der TU München, dem LRZ und der Universität der Bundeswehr München (UniBw M). Seine Hauptforschungsinteressen liegen im Bereich des Managements vernetzter Systeme. Arbeiten der letzten Jahre beschäftigen sich mit Architekturen für integriertes Netz- und Systemmanagement und Implementierungen von Lösungen für spezifische Bereiche des IT-Managements, wie Konfigurations-, Abrechnungs- und Fehlermanagement.

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)

Mit ZITiS besteht in verschiedenen Themengebieten eine enge Kooperation. Aktuelle gemeinsame Forschungsvorhaben mit dem Lehrstuhl sind in den Bereichen IoT/5G, Analyse und Auswertung von Fahrzeugdaten und Quantenkommunikation angesiedelt.

Airbus Defence and Space

Mit Airbus Defence and Space werden gemeinsame Projekte im Bereich Sichere, verifizierbare Mikrokernels und deren Einsatz in sicheren Cloudinfrastrukturen durchgeführt. Angestrebt wird darüber hinaus ein gemeinsamer wissenschaftlicher Austausch im Bereich Digitale Souveränität Europas mit dem Fokus auf der Entwicklung souveräner Cloudlösungen.

CGI

Das FI CODE und die CGI arbeiten zusammen an der Förderung des wissenschaftlichen Austauschs, der gemeinsamen Bearbeitung von Projekten und der Förderung von Promotionsstellen im Bereich der Netzsicherheit/IT-Sicherheit. Ein Kooperationsvertrag wurde bereits unterzeichnet.

Infineon

Mit Infineon finden eine enge Zusammenarbeit und ein wissenschaftlicher Austausch im Bereich Post-Quanten-Kryptographie statt. Es werden in diesem Themenfeld bereits gemeinsame Projekte bearbeitet.

Prof. Dr. Michaela Geierhos

Data Science

Publikationen

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

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

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

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

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

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

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

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

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

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

Forschungsprojekte

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

In diesem Teilprojekt werden verschiedene Arten von Anforderungsspezifikationen behandelt, die eine erfolgreiche Suche, Zusammenstellung und Analyse von Services ermöglichen. Im Sinne agiler, partizipativer Softwareentwicklung werden Endanwender künftig mehr in den interaktiven Kompositionsprozess von on-the-fly zu erstellenden Softwareservices einbezogen. Dieser Dialog soll von einem domänenspezifischen Chatbot geführt werden, der einerseits der gezielten Nachfrage und andererseits der Auflösung von Unklarheiten dient. Darüber hinaus muss der Kompositionsprozess für Endanwender transparenter gemacht werden, sodass für eine fertige Servicekomposition klargestellt wird, welche anfänglichen Anforderungen bei der Erstellung berücksichtigt wurden und auf welche verzichtet werden musste.

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

Quanten-Internet im Großraum München (MuQuaNet)
TP: „Authority-Dependent Risk Identification and Analysis in Online Networks“

Ziel des Teilprojekts ist es, ausgewählte Apps automatisiert zu überwachen und deren gesammelte Daten zu analysieren, mit Social-Media-Profilen zu korrelieren und Personennetzwerke/-cluster zu bilden, um potenzielle Ziele zu identifizieren und ihr Gefährdungspotenzial aufgrund der gegebenen Datenlage einzustufen. Werden diese Daten noch mit weiteren (u. a. von Sicherheitsbehörden oder militärische Dienststellen) eingestuften Daten korreliert, lässt sich eine Gefährdungsplausibilität für entsprechende Personen(gruppen) oder Standorte abschätzen. Die hieraus generierten Erkenntnisse bedürfen aufgrund des Risikos einer hochsicheren Verschlüsselung bei der Übermittlung an andere Dienste.

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

Lehre

3851 **Information Retrieval**

3852 **Anwendungsgebiete der Data Science**

3853 **Analyse unstrukturierter Daten**

Weitere Funktionen

- Gewähltes Mitglied im Beirat „Deutsche Biographie“ der Historischen Kommission bei der Bayerischen Akademie der Wissenschaften
- Mitglied im Entwicklungsrat von CLARIAH-DE
- Gutachterin für die Europäische Kommission, die Fraunhofer-Gesellschaft, den DAAD, die Alexander von Humboldt-Stiftung und das Bundesministerium der Justiz und für Verbraucherschutz

Mitglied des Programmkomitees

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

Peer-Review-Tätigkeit

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

Kooperationen

FH Bielefeld, Dr. Frederik S. Bäumer

Maschinelle Identifizierung und Markierung von privatsphäregefährdenden Textbestandteilen mit Erläuterung der möglichen Risiken.

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

Angebot einer zweiwöchigen Sommerschule zu „Information Retrieval“ für Studierende der Informatik und Computerlinguistik.

MSH Medical School Hamburg, Prof. Dr. Mathias Kauff

Gemeinsame Forschung im Bereich der textuellen Nachweisbarkeit von psychologischen Effekten in nutzergenerierten Inhalten mit Fokus auf Patientenmeinungen.

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

Publikationen

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

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

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

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

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

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

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

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

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

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

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

Forschungsprojekte

Airborne Cyber Security Enhancement

Das Forschungsinstitut CODE und Airbus Defence & 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.

Drittmittelgeber:
Airbus Defence & Space, Manching
Laufzeit: 2020–2024

Smart Hospitals – sichere Digitalisierung bayerischer Krankenhäuser

Rund 400 Krankenhäuser bilden in Bayern eine tragende Säule der Gesundheitsversorgung. Im Projekt wurde deren Status quo technischer und organisatorischer IT-Sicherheitsmaßnahmen, insbesondere im Kontext aktueller Digitalisierungsvorhaben, erfasst. Die Erkenntnisse flossen in einen Maßnahmenkatalog zur weiteren Erhöhung des Sicherheitsniveaus ein, der aktuell in Ausgabe 2020/21 vorliegt.

Drittmittelgeber: Bayerisches Staatsministerium für Gesundheit und Pflege (StMGP)
Laufzeit: 10/2018–09/2021

Digitale Identitäten für Servicekonten: Umsetzungsstrategien, Richtlinien und Sicherheitsaspekte (DISKURS)

In diesem Projekt wird der Aufbau und Betrieb der nationalen Identitätsföderation FINK wissenschaftlich begleitet, durch die eine länderübergreifende Nutzung von Onlineverwaltungsleistungen ermöglicht wird. Zusätzlich werden zukünftig relevante, auf Self-Sovereign Identity basierende Systeme untersucht und deren mögliche Einbindung in die bestehende Föderation demonstriert.

Drittmittelgeber: Bayerisches Staatsministerium für Digitales (StMD)
Laufzeit: 12/2019–03/2021

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** (HT)

5507 **Sichere vernetzte Anwendungen** (FT)

5508 **Sicherheitsmanagement** (FT)

Prof. Dr. Johannes Kinder

Programmanalyse, -transformation, -verstehen und -härtung (PATCH)

Publikationen

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

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

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

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

Forschungsprojekte

Sicherheitstests für dynamische Programmiersprachen

Dynamische Programmiersprachen bilden die Grundlage des World Wide Web und werden sowohl in Webbrowsern als auch auf Servern ausgeführt. So können schnell Funktionen, Websites und Systeme aufgesetzt werden, aber auch leicht Fehler gemacht werden. Im EASTEND-Projekt (Efficient Automatic Security TEstiNg for Dynamic Languages) entwickeln wir neue Methoden, um Fehler in JavaScript-Programmen automatisch zu finden.

Förderer: UK Government & Engineering and Physical Sciences Research Council (EPSRC)
Laufzeit: 09/2015–02/2020

Reverse Engineering trifft Deep Learning

Computerprogramme werden in Quelltext geschrieben und zur Ausführung in eine Binärform übersetzt, die nur noch der Computer versteht. Da Quelltext in vielen Situationen nicht verfügbar ist, können Menschen nur schwer einschätzen, welches mögliche Verhalten in einem binären Programm steckt. Unser maschinelles Lernsystem ist darauf trainiert, Komponenten in Binärdateien mit Namen zu versehen, die dem ursprünglichen Quelltext ähneln.

Förderer: Engineering and Physical Sciences Research Council (EPSRC) & Forschungsinstitut CODE
Laufzeit: seit 10/2016

Promotionen

Blake Loring
Practical Dynamic Symbolic Execution for JavaScript

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

Claudio Rizzo
Static Flow Analysis for Hybrid and Native Android Applications

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

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

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

Lehre

38191 **Reverse Engineering** (FT)
38192 **Praktikum Reverse Engineering** (FT)
55011 **Seminar Softwarehärtung** (HT)
55011 **Seminar Machine Learning in Reverse Engineering & Malware Detection** (FT)
55101 **Dynamische Programmanalyse** (HT)
55102 **Statische Programmanalyse** (WT)
55103 **Praktikum Fuzzing** (WT)

Messen, Tagungen, Seminare

General Chair

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

Weitere Funktionen

- Advisory Board Member, Centre for Doctoral Training in Cyber Security for the Everyday, Royal Holloway, University of London
- Gutachter für die Promotion von Ivan Radiček, Fakultät für Informatik, Technische Universität Wien
- Experte Code Review bei WTD-81, Greding

Kooperationen

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

Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

Forschungsprojekte

Hochsichere Betriebssysteme für Embedded IT (HoBIT)

Es werden Grundlagen für die Entwicklung von hochzuverlässigen und hochsicheren Betriebssystemen untersucht und Basistechnologien prototypisch aufgebaut. Dabei werden auf der Grundlage des vorhandenen seL4-Mikrokernels grundlegende Untersuchungen an einem exemplarischen Zielsystem durchgeführt. Für eine spätere Umsetzung werden zudem geeignete Werkzeuge und Nachverifizierungsmöglichkeiten untersucht.

Drittmittelgeber: Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi)
Laufzeit: 01/2018–09/2020

Erweiterung der Grundlagen für formale Verifikation von Software und deren Anwendung (SW_GruVe)

Für die Zulassung von IT-Systemen wird mit zunehmenden Zulassungsanforderungen auch das Instrumentarium evaluiert, mit dem die Systeme erstellt werden. In diesem Projekt werden entsprechende Qualitätsanforderungen evaluiert, Werkzeuge zur formalen Verifikation weiterentwickelt und besonders sicherheitskritische Betriebssystemkomponenten exemplarisch formal verifiziert.

Drittmittelgeber: Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi)
Laufzeit: 10/2020–09/2022

Mikrokernel für IT-sicherheitsrelevante Anwendungen

Für die Anwendung von Mikrokernen für statische und cloudbasierte Hochsicherheitsanwendungen werden sichere Startprozessarchitekturen untersucht. Verfügbare Lösungsansätze werden analysiert und bewertet und prototypisch im Kontext eines statischen Gateways und eines Cloudsystems umgesetzt.

Drittmittelgeber: Airbus CyberSecurity GmbH
Laufzeit: 12/2020–12/2023

Lehre

5505 **Betriebssystem-Sicherheit** (FT)

Kooperationen

- CSIRO Dat61, Canberra, Australien
- Hensoldt Cyber GmbH, Taufkirchen
- Technische Universität München

Prof. Dr. Arno Wacker

Datenschutz und Compliance

Publikationen

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

Forschungsprojekte

Redundante Strukturen in verteilten Overlay-Netzen

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 durch die Schaffung und Ausnutzung von Redundanzen bezüglich Datenspeicherung und Konnektivität und entsprechende Vermeidung einzelner Ausfallpunkte.

DECRYPT: Entschlüsseln historischer Dokumente

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, damit historische Manuskripte entschlüsselt und kontextualisiert werden können, welche bislang in Archiven und Bibliotheken verborgen sind.

Drittmittelgeber:
Swedish Research Council (SRC)
Laufzeit: 01/2019–12/2024

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)

Internationalität

Das FI CODE pflegt weltweit ein großes Netzwerk. 2020 stammten die Mitarbeitenden aus 14 Ländern. In 28 Ländern gab es 79 Kooperationspartner.

ABB.: ISTOCK / BLUE PLANET STUDIO

Mitarbeitende

Nationalität
Ägypten
Argentinien
Bangladesch
Benin
Brasilien
Bulgarien
Deutschland
Finnland
Großbritannien
Kanada
Kroatien
Österreich
Republik Korea
Spanien

Internationale Kooperationspartner

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

So erreichen Sie uns

Forschungsinstitut Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 22
81739 München

code@unibw.de

+49 89 6004 7302 oder 7303

www.unibw.de/code

Twitter: @FI_CODE

LinkedIn: Forschungsinstitut Cyber Defence (CODE)

YouTube: Forschungsinstitut Cyber Defence

Lageplan

ABB.: TAUSENDBLAUWERK.DE

Impressum

Herausgeber

Forschungsinstitut CODE
Universität der Bundeswehr München
Carl-Wery-Str. 22
81739 München

Leitung des FI CODE

Prof. Dr. Gabi Dreo Rodosek,
Leitende Direktorin

Prof. Klaus Buchenrieder, PhD,
Technischer Direktor (bis 02/2020)

Prof. Dr. Udo Helmbrecht,
Technischer Direktor (03/2020–01/2021)

Prof. Dr. Wolfgang Hommel,
Technischer Direktor (seit 02/2021)

Dipl.-Inf. Volker Eiseler,
Geschäftsführer und Akademischer Direktor

Professoren am FI CODE

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

Prof. Dr. Harald Baier,
Professor für Digitale Forensik (seit 09/2020)

Prof. Dr. Stefan Brunthaler,
Professor für Sichere Softwareentwicklung

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 (seit 04/2020)

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. 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 2020)

Aus der Fakultät für Informatik der
Universität der Bundeswehr München

Prof. Dr. Uwe Borghoff

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Wolfgang Hommel

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 von Giesecke + Devrient

Redaktion

Prof. Dr. Michaela Geierhos,
Professorin für Data Science

Lisa Scherbaum M.A.,
Referentin für Öffentlichkeitsarbeit

Art Direction

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

Benjamin Bellgrau M.Sc.,
Wiss. Mitarbeiter Professur für Data Science
(Gestaltung vorläufiges Layout)

Lektorat

Lektorat Unker
www.unker.com

Druck

Holzer Druck und Medien
www.druckerei-holzer.de

Regularien

Redaktionsschluss: Mai 2021

ISBN: 978-3-943207-55-2 | ISSN: 2748-8780

Auch erschienen als elektronische Publikation
(ISBN: 978-3-943207-56-9 | ISSN: 2748-8799)
sowie in englischer Sprache
(ISBN: 978-3-943207-57-6 | ISSN: 2748-9485).


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