P.b.b. Verlagspostamt 1010 Wien | 02Z031460M

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

Ausgabe 01 • 2023 | Jg. 48 | EUR 5,00

DAS IT-MAGAZIN DER ÖSTERREICHISCHEN COMPUTER GESELLSCHAFT

OCG JOURNAL

IT-Nachwuchsforschung in Österreich

OCG Journal Ausgabe 01 • 2023 | Coverbilder: Autor*innen

Veranstaltungen

Social Artificial Intelligence Night
1. April 2023, St. Pölten
https://www.fhstp.ac.at/de/onepager/social-artificial-intelligence-night-saint

EDUdays
12. bis 13. April 2023, Universität für Weiterbildung Krems
https://www.edudays.at

RoboCupJunior - Austrian Open 2023
13. bis 14. April 2023, Lakeside Park und Universität, Klagenfurt
https://robocupjunior.at/

All Digital Weeks
17. April bis 7. Mai 2023, online/offline, global
https://alldigitalweeks.eu/

A-TAG - Accessible Media Beach
18. April 2023, Wien
https://atag.accessible-media.at/

Lehrer*innen-Fortbildung: Computational Thinking
25. April 2023, OCG, Wien
https://www.ocg.at/de/projekt-KIDZ

Security Forum 2023
25. und 26. April 2023, FH Oberösterreich
https://www.securityforum.at/

KI und Data Science – Themen für den Unterricht?
27. April 2023, Bildungsdirektion Wien
https://www.ocg.at/de/traindl

Informatik-Workshop für Lehrkräfte
17. Mai 2023, PH Steiermark
https://www.ocg.at/de/traindl

eBazar an der PH Wien
23. Mai 2023, Wien
https://phwien.ac.at/

Austrian Computer Science Day
5. Juni 2023, TU Graz
https://online.tugraz.at/tug_online/vag.detail?vid=110983

Imagine 2023
15. Juni 2023, Wien
https://www.imagine-ikt.at/

AI Summer School 2023 — CAIML
3. bis 7. Juli 2023, TU Wien
https://caiml.org/summerschool2023/

OCG Sommercamp -Programmieren
3. bis 7. Juli 2023, OCG Wien
https://www.ocg.at/de/sommercamps

ditact women's IT-Studies
21. August bis 2. September 2023, Salzburg/online
https://www.didact.ac.at

CEEE|Gov Days 2023
14. bis 15. September 2023, Ungarn
https://ceeegov2023.ocg.at//

IKT-Sicherheitskonferenz 2023
3. und 4. Oktober 2023, Linz
https://seminar.bundesheer.at/

Dach+ Energy Informatics 2023
4. bis 6. Oktober 2023, Wien
https://www.energy-informatics2023.org/

IMPRESSUM

Das OCG Journal ist die Mitgliederzeitschrift der Österreichischen Computer Gesellschaft (OCG). Inhaltlich wird das Journal in völliger Unabhängigkeit gestaltet und berichtet über die OCG Leitthemen Ausbildung und Qualität, Innovation und Start-ups, internationale Vernetzung und digitale Zivilgesellschaft.

ISSN 1728-743X

Medieninhaber und Herausgeber:
Österreichische Computer Gesellschaft (OCG)

Präsident: DI Wilfried Seyruck

Generalsekretär und Leitung der Redaktion: Dr. Ronald Bieber

Redaktion: Irina Scheitz, Katharina Resch-Schobel, Josefine Hiebler

Layout und DTP: OCG | Irina Scheitz, Josefine Hiebler

Lektorat: Katharina Resch-Schobel

Fotos: Archiv OCG, Autor*innen, Privatarchive, istock

Kontakt: info@ocg.at | URL: www.ocg.at

Alle: Wollzeile 1, 1010 Wien | Tel.: +43 1 512 02 35-0

Druck: Print Alliance HAV Produktions GmbH, 2540 Bad Vöslau

https://printalliance.at/fairprint

Editorial

Sehr geehrtes OCG-Mitglied,
liebe Leserin, lieber Leser!

In Zeiten wie diesen sind guten Nachrichten besonders willkommen. Wir freuen uns daher, Ihnen in diesem Heft über Österreichs IT-Nachwuchsforscherinnen und -forscher berichten zu können, die mit hervorragenden Leistungen an der Lösung aktueller Probleme arbeiten.

Die OCG bietet jungen Wissenschaftler*innen ein Forum zur Vernetzung und Publikation. In Newsletter, Journal, Presseaussendungen und auf Social-Media-Kanälen sorgt die OCG dafür, dass Österreichs IT-Nachwuchs sichtbar wird. Wir laden daher auch alle Studierenden und den wissenschaftlichen Nachwuchs dazu ein, Mitglied der Österreichischen Computer Gesellschaft zu werden, um gemeinsam die Informationstechnologie zum Nutzen der Gesellschaft zu fördern.

Der vom OCG Arbeitskreis IT-Sicherheit organisierte Young Researchers' Day findet jährlich im Rahmen der IKT-Sicherheitskonferenz des Ministeriums für Landesverteidigung statt. Dort präsentieren Dissertant*innen und Jungforscher*innen von österreichischen Universitäten, Fachhochschulen und Forschungsinstitutionen ihre aktuellen Forschungsergebnisse im IT-Sicherheitsbereich. In diesem Heft werden die Arbeiten der Teilnehmenden im Jahr 2022 vorgestellt.

Im Sinne des Vereinszieles der OCG fördern wir die jungen Wissenschaftler*innen auch mit unseren Preisen, die für ausgezeichnete akademische Arbeiten verliehen werden. Wie es Prof. Gabriele Kotsis, langjährige Jury-Vorsitzende des OCG Förderpreises in ihrem Interview (siehe Seite 24) so treffend ausdrückt: „Wir hoffen, mit den Auszeichnungen auch Impulse für zukünftige Karrieren in der Forschung – so wie es bei mir selbst der Fall war – anstoßen zu können."

So stellen wir in diesem Heft die aktuellen Beiträge der Preisträgerinnen und Preisträger der OCG Förderpreise und des Heinz Zemanek Preises vor. Es freut uns auch, dass letztes Jahr ein Österreicher den GI-Dissertationspreis gewonnen hat, der von unserer deutschen Schwestergesellschaft in Kooperation mit der OCG und der Schweizer Informatik Gesellschaft vergeben wird.

An dieser Stelle möchte ich allen Mitgliedern der Jurys danken, die ehrenamtlich die spannende – aber durchaus auch herausfordernde – Aufgabe übernommen haben, die besten Arbeiten für die Preise zu ermitteln.

Lassen Sie sich von der Begeisterung von Österreichs IT-Nachwuchs anstecken – so können wir zuversichtlich in die Zukunft blicken.

Herzlichst, Ihr

Wilfried Seyruck, Präsident OCG

Inhalt

Young Researchers‘ Day

Prämierte Arbeiten

Transnationale Forschung

Über die OCG

Die Österreichische Computer Gesellschaft (OCG) wurde 1975 vom Computerpionier Heinz Zemanek gegründet. Ziel des gemeinnützigen Vereins ist die Förderung der Informatik und Kommunikationstechnologie unter Berücksichtigung ihrer Wechselwirkung mit Mensch und Gesellschaft. Die OCG versteht sich als die Vernetzungs- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung und bietet in ihren Veranstaltungen Zugang zu Expertise in aktuellen IKT Themen. Sie vertritt Österreich in nationalen und internationalen IKT Organisationen und Verbänden.
Mit zahlreichen Projekten setzt die OCG einen Fokus auf Förderung von digitalen Kompetenzen und Verständnis für neue Technologien wie z. B. Künstliche Intelligenz oder Robotics für alle Altersgruppen und ist zudem National Operator des ECDL/ICDL – der international anerkannten Zertifizierung für digitale Kompetenzen.

Die OCG fungiert als Zertifizierungsstelle für ISMS nach ISO/IEC 27001 und als Qualifizierte Stelle nach dem NIS-Gesetz
Mittels Wettbewerben, Preisen und Auszeichnungen fördert die OCG wissenschaftlichen Nachwuchs gezielt fördern. Die Mitgliederzeitschrift, das OCG Journal, erscheint viermal im Jahr.

www.ocg.at | www.ocgcert.com | www.icdl.at

von Edgar Weippl

Österreichs IT-Nachwuchs

Die Forschungstätigkeit von „Young Researchers“ ist von zentraler Bedeutung für den Erfolg der österreichischen Wissenschaft und Forschung. Gerade in der angewandten Informatik sind Forschungsprojekte typischerweise größere Projekte, bei welchen auch Unternehmen Projektpartner sind. In diesen Projekten ist der Beitrag der Nachwuchsforscher:innen besonders essentiell, weil die Umsetzung und Evaluierung von Konzepten ein unverzichtbarer Teil der Forschung ist.

Young Researcher sind Nachwuchswissenschaftler:innen, die sich auf ein bestimmtes Forschungsthema spezialisieren. Diese Spezialisierung kann schon sehr früh im Rahmen von forschungsorientierten Bachelor- und Masterarbeiten erfolgen. Gerade wenn man von Beginn an in Forschungsprojekte eingebettet arbeitet, ist es wichtig, trotzdem einen Überblick über das Fachgebiet zu behalten.

Eine sehr gute Möglichkeit, diesen Überblick zu bekommen, ist beispielsweise der „Young Researchers‘ Day“ des Arbeitskreises für IT-Sicherheit der OCG. Ziel ist es, schon früher als üblich sehr junge Forscher:innen innerhalb der Security-Forschungscommunity in Österreich zu vernetzen. Diese nationalen Netzwerke sind aus verschiedenen Gründen wichtig. Erstens lernen junge Forscher:innen Vertreter:innen anderer Institutionen (z. B. FHs, Universitäten, außeruniversitäre Forschungszentren) kennen und somit auch die Arbeitsweisen und fachlichen Spezialisierungen außerhalb ihrer Heimatinstitution. Zweitens helfen diese Kontakte bei der Planung von Auslandsaufenthalten, die ein wichtiger Bestandteil des Forscher:innenlebens sind. Gerade Young Researcher haben selten schon sehr gute Publikationen und können daher keinen guten Track-Record aufweisen, was die Bewerbung bei ausländischen Top-Institutionen sehr schwierig macht. Referenzen und Empfehlungen international anerkannter nationaler Forscher:innen sind daher für Nachwuchswissenschafter:innen unabdingbar.

SICHTBARKEIT ÖSTERREICHS ERHÖHEN

Auch wenn heimische Universitäten, Forschungszentren und FHs kurzfristig nicht erfreut sind, wenn junge gute Mitarbeiter:innen ins Ausland gehen, so leisten diese einen wichtigen Beitrag zur internationalen Sichtbarkeit Österreichs. Beispielsweise sind Alumni unseres Forschungszentrums SBA Research als Professor:innen zu CISPA in Saarbrücken oder nach Regensburg berufen worden, zu IBM Research oder Google gegangen oder haben Forschungsstartups gegründet.

Einige dieser jungen Forscher:innen kehren später wieder nach Österreich zurück und tragen somit auch dazu bei, dass Österreichs Wissenschaft und Forschung auf internationaler Ebene wettbewerbsfähig bleiben.

WELCHE UNTERSTÜTZUNGEN HELFEN JUNGEN FORSCHER:INNEN?

1. Bereitstellung von Mentoring und Beratung. Einrichtungen können jungen Forscher:innen Ressourcen und Unterstützung in Form von Mentoring und Beratung zur Verfügung stellen. Dazu könnte gehören, junge Forscher:innen mit Fakultätsmitgliedern, die über Fachwissen auf ihrem Gebiet verfügen, bekannt zu machen, Ratschläge zu Forschungsthemen zu erteilen und während des gesamten Forschungsprozesses Rat und Unterstützung anzubieten.

2. Forschungszuschüsse und Stipendien anbieten. Einrichtungen können Zuschüsse und Stipendien anbieten, um junge Forscher:innen bei ihren Projekten zu unterstützen.

3. Zugang zu Ressourcen gewähren. Einrichtungen können jungen Forscher:innen Zugang zu Ressourcen wie Datenbanken, Bibliotheken und Labors gewähren.

4. Möglichkeiten zur Vernetzung anbieten. Einrichtungen können jungen Forscher:innen die Möglichkeit bieten, sie auf ihrem und benachbarten Gebieten zu vernetzen. Dies kann ihnen helfen, berufliche Beziehungen aufzubauen und Möglichkeiten zur Zusammenarbeit bei Forschungsprojekten zu schaffen.

5. Organisation von Veranstaltungen und Workshops. Die Einrichtungen können Veranstaltungen und Workshops organisieren, um jungen Forscher:innen zu helfen, mehr über ihr Fachgebiet zu erfahren und ihre Fähigkeiten zu entwickeln.

ANGEBOTE DER OCG

Die OCG bietet Forschungsinstitutionen einen neutralen Rahmen, um in Arbeitskreisen und ähnlichen Formaten derartige Aktivitäten durchzuführen. Aus solchen institutionsübergreifenden Aktionen können sich in Folge langfristigere Kooperationen oder Forschungscluster entwickeln. Ein Beispiel im Wiener Umfeld ist VISP (Vienna Cybersecurity and Privacy Research Cluster), der die fachliche Expertise im Bereich der IT-Security bündelt, die an der Universität Wien, dem AIT, der Technischen Universität Wien, SBA und IST Austria existiert.

OCG Arbeitskreis IT-Sicherheit

Der Arbeitskreis widmet sich den Gebieten Informationssicherheit und IT-Sicherheit. Dazu gehört auch die Förderung eines kritischen Bewusstseins gegenüber Sicherheitsfragen.

ZENTRALE THEMEN

- Sicherheitsmanagement, Sicherheitspolitik
- Risikoanalyse, Risikomanagement
- Sicherheitsanforderungen
- Sicherheitsmechanismen und -dienste
- Kryptographie und Kryptoanalyse
- Informationssicherheit in bereichsspezifischen Applikationen (Bankwesen, Verwaltung, etc.)
- Zertifizierung (z. B. ISO/IEC 27001)
- Rechtliche Aspekte, Datenschutz
- Wirtschaftlichkeit von Sicherheitsmaßnahmen
- Verantwortbarkeit des Technik-Einsatzes zwischen Verlässlichkeit, Risiko und Wirtschaftlichkeit
- Sicherheit als Kriterium für die gesellschaftliche Akzeptanz von Informationssystemen

Der Arbeitskreis fördert theoretische und angewandte wissenschaftliche Aktivitäten im Bereich IT-Sicherheit, den intensiven Ideenaustausch der an diesem Bereich beteiligten Disziplinen, die Kooperation zwischen Wissenschaft, Wirtschaft und Verwaltung sowie mit nationalen und internationalen Arbeitsgruppen. Diese Aktivitäten werden durch Vortragsveranstaltungen, Seminare, Workshops und Tagungen unterstützt.

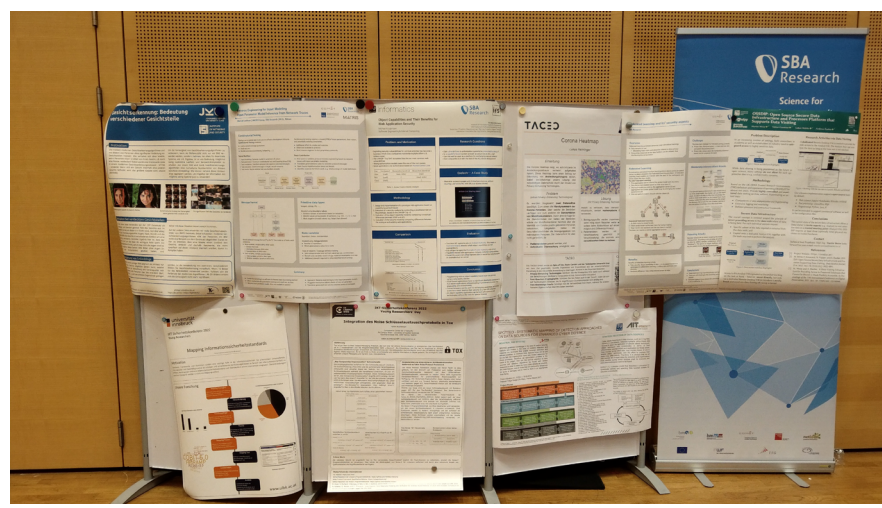
Geleitet wird der AK von Dr. Ingrid Schaumüller-Bichl. Edgar Weippl ist Stellvertretender Leiter.

DER YOUNG RESEARCHERS' DAY

Einmal im Jahr wird der Young Researchers' Day bei der IKT-Sicherheitskonferenz des Bundesministeriums für Landesverteidigung (BMLV) veranstaltet, bei dem junge Forscher*innen ihre Arbeiten mit Fachvorträgen und Postern präsentieren.

Die nächste IKT-Sicherheitskonferenz findet am 3. und 4. Oktober 2023 im Design Center Linz statt.

Univ.-Prof. Dipl.-Ing. Mag. Dr. **Edgar Weippl** ist Professor für Security und Privacy und Vizedekan der Fakultät für Informatik, Universität Wien. Seine Forschungsschwerpunkte liegen auf Distributed-Ledger-Technologien und sicheren Produktsystemen.



Die Postersammlung des Young Researchers' Day 2022

von Manuel Leithner

Unbekannte Protokolle testen

Die Anforderungen an moderne Anwendungen sind beträchtlich: Umfangreich in ihrer Funktion sollen sie sein, einfach bedienbar, performant und natürlich frei von Bugs und Schwachstellen. Dass besonders letzteres nicht selbstverständlich ist, beweisen monatliche Patch-Zyklen ebenso wie die stetig wachsende Liste an Sicherheitsvorfällen. Testen ist daher ein wichtiger Prozess in modernen Entwicklungszyklen; dabei soll verifiziert werden, ob das entwickelte Produkt sich korrekt verhält oder ob sich darin Schwachstellen verbergen.

Beliebt sind etwa Unit Tests, welche einzelne Szenarien realisieren (zum Beispiel „Führe eine Buchung durch“). Um Schwachstellen zu finden, wird oft Fuzzing eingesetzt; dabei werden Eingaben immer weiter mutiert, um - grob formuliert - das Zielsystem zu crashen. Beide Ansätze überprüfen jedoch potenziell nur einen winzigen Teil der Anwendung. Systeme mit sehr hohen Sicherheitsanforderungen können stattdessen formal verifiziert werden; der Aufwand dabei ist jedoch in der Praxis meist zu hoch.

Kombinatorisches Testen ist eine Alternative, welche mathematisch garantierte Abdeckung mit einer geringen Anzahl von Testfällen kombiniert. Dabei werden die Eingabeparameter eines Systems und ihre erlaubten Werte mittels eines sogenannten Input Parameter Models (IPM) abgebildet. Basierend auf diesem Modell und einer anwenderdefinierten Stärke wird ein Covering Array (CA) erstellt, in dem jede Spalte einem Eingabeparameter entspricht und jede Zeile einen Testfall darstellt. Das Besondere daran: Aufgrund der Eigenschaften eines CA können Sie jede beliebige Kombination von Parametern auswählen (solange die Anzahl der Parameter maximal der Stärke des CA entspricht) und haben die Garantie, dass in dem CA sämtliche Werte-Kombinationen dieser Parameter vorkommen. Laut empirischen Studien werden fast alle Bugs durch die Kombination von einigen wenigen Parametern ausgelöst; in der Praxis sind Stärken zwischen zwei und sechs ausreichend. Nachdem die Anzahl der Zeilen eines CAs stark von diesem Parameter abhängt, lässt sich damit auch die Anzahl der benötigten Testfälle minimieren. Diese werden im weiteren Verlauf noch zu konkreten Eingaben an das Zielsystem übersetzt und das Verhalten desselben wird überprüft, um festzustellen, ob alle Fälle korrekt verarbeitet wurden.

In der Praxis ist jedoch oft kein IPM verfügbar. Die Erstellung und Wartung eines solchen Modells ist für Eigenentwicklungen durchaus möglich; dabei ist der Einsatz von Analyse-Tools ratsam, denn nicht alle Änderungen am Programmcode sind für alle Beteiligten immer offensichtlich. Für proprietäre Software jedoch ist die erforderliche Dokumentation meist nicht zugänglich. Daraus ergibt sich die Frage, wie solche Objekte mittels kombinatorischer Tests verifiziert werden können.

KOMBINATORISCHES TESTEN

In meiner Diplomarbeit „Reverse Engineering for Input Modeling: Input Parameter Model Inference from Network

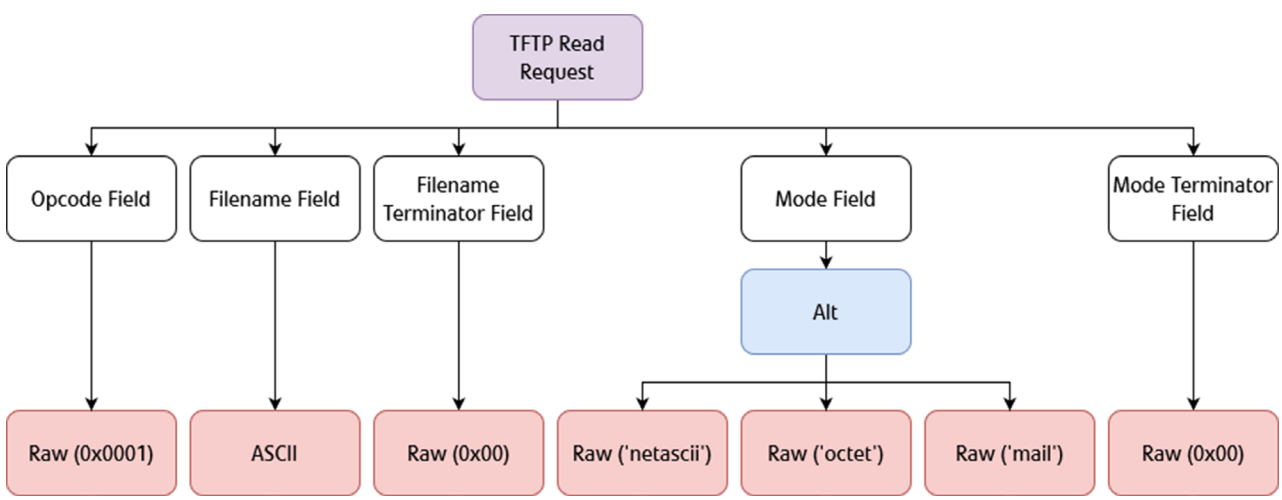


Abbildung 1: Netzob-Modell eines Nachrichtenformats. © 2022 Manuel Leithner

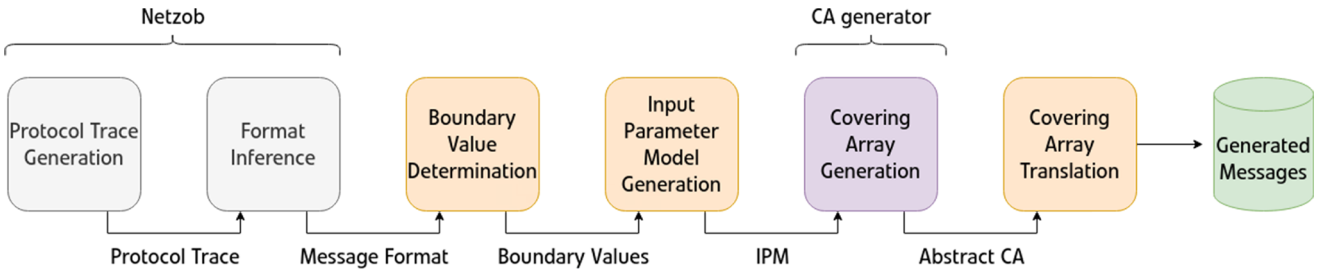


Abbildung 2: Prozess zur Erstellung und Übersetzung eines kombinatorischen Test-Sets für Netzwerkprotokolle. © 2022 Manuel Leithner

Traces" (FH St. Pölten) behandle ich diese Frage im Kontext von unbekannten Netzwerkprotokollen. Diese schreiben Format und Reihenfolge der zwischen Kommunikationspartnern ausgetauschten Nachrichten vor; sie enthalten demnach jene Informationen, die zur Erstellung eines IPMs notwendig sind. Reverse Engineering ist ein Überbegriff für Techniken, die dazu dienen, Informationen über die Funktionsweise von Software zu erhalten, deren Quellcode nicht verfügbar ist.

In der Forschung werden in diesem Bereich zwei Richtungen unterschieden: Einerseits ist es möglich, die Ausführung der Anwendungen, welche am Netzwerkverkehr teilhaben, zu überwachen. Dadurch lassen sich Rückschlüsse auf die Struktur von Nachrichten sowie ihrer Auswirkungen auf den Zustand der Software ziehen. Allerdings ist diese Art der Analyse oft langsam und mit erheblichem Aufwand verbunden. Die Alternative dazu ist die Auswertung des Netzwerk-Verkehrs, um die Syntax und Semantik der ausgetauschten Nachrichten zu erkennen. Im Allgemeinen skaliert dieser Ansatz bedeutend besser und lässt sich ohne Modifikationen an den Kommunikationsteilnehmern implementieren, denn eine rein passive Aufnahme des Netzwerkverkehrs ist als Datensatz ausreichend. Der theoretische Teil meiner Arbeit bietet eine Übersicht der verfügbaren Methoden in diesem Bereich.

Im praktischen Teil meiner Arbeit erweitere ich Netzob, ein Tool für das semiautomatische Reverse Engineering von Netzwerkprotokollen. Es bietet umfangreiche Möglichkeiten zur interaktiven Analyse: So sind etwa Clustering (um Nachrichten desselben Typs zu erkennen), die Erkennung von individuellen Komponenten (Feldern) von Nachrichten sowie die Zuweisung von Datentypen mittels einer erweiterten Python-Shell möglich. Die resultierenden Nachrichten-Formate werden in einer Baumstruktur modelliert, wobei auch verschachtelte, sich wiederholende oder durch mehrere alternative Datentypen definierte Komponenten unterstützt werden.

Das Ziel ist es nun, basierend auf den Datentypen der Felder sowie ihrer Struktur untereinander ein IPM zu konstruieren. Bei einigen dieser Datentypen ist der konkrete Wertebereich allerdings zu groß, um ihn sinnvoll zu modellieren. Als Beispiel sei ein Zeitstempel genannt, der Sekunden kodiert: Die Verarbeitung der meisten Werte ist ident und es wäre nicht nützlich, jede einzelne Sekunde im IPM abzubilden. Wichtig sind jedoch bestimmte Grenzwerte (Boundary Values): Die Sekunde 0, der maximal erlaubte Wert, oder auch die Werte direkt darüber oder darunter. Dementsprechend verwenden wir für diese Datentypen symbolische Werte im IPM, die den Boundary Values entsprechen.

DI **Manuel Leithner** ist Sicherheitsforscher und Leiter des Teams für Combinatorial Security Testing der MATRIS-Forschungsgruppe von SBA Research, wo er sich mit kombinatorischem Testen, Web-Schwachstellen sowie Reverse Engineering beschäftigt. 2022 hat er den Master-Studiengang Information Security an der FH St. Pölten abgeschlossen.

von Diana Strauß

Federated Learning

Maschinelles Lernen (Machine Learning) findet in der heutigen Welt viele Anwendungsgebiete, zum Beispiel, um Hautkrebs zu erkennen.

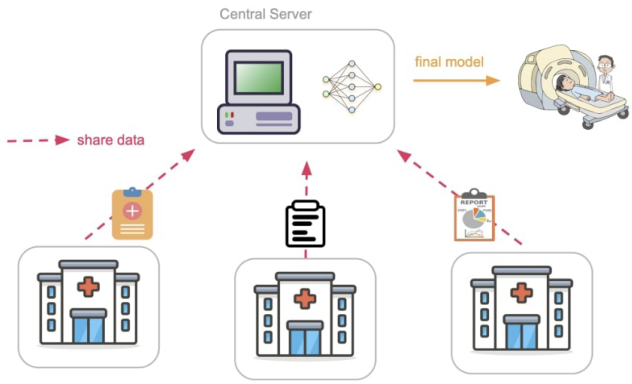
Im traditionellen Ansatz des maschinellen Lernens aus verteilten Daten senden die Teilnehmer (Clients) eines Lernsystems ihre Daten an eine zentrale Einheit (Server), wo dann auf ihnen ein Machine Learning Modell trainiert wird (siehe Abbildung 1a). Es gibt Anwendungen, die zur frühzeitigen und automatischen Erkennung von Hautkrebs verwendet werden und sich maschinelles Lernen zu Nutze machen [2]. In diesem Fall wird ein Modell, das bereits mithilfe eines Hautkrebs-Datensatzes trainiert worden ist, verwendet, sodass es in der Lage ist zwischen verschiedenen Kategorien zu unterscheiden (z. B.: Krebs, Kein-Krebs) [4]. Hier würde eine Person zum Beispiel ein Foto von der auffälligen Hautstelle machen und dieses der App zur Verfügung stellen. Das Foto würde dann an den zentralen Server gesendet werden und das Modell würde der anfragenden Person eine Vorhersage, zum Beispiel Krebs, mitteilen. Diese Diagnose muss dann mit einem/einer Dermatolog*in abgeklärt werden. Ein solches Modell heißt Neuronales Netzwerk und ist an das menschliche Gehirn angelehnt, wodurch es in der Lage ist, Muster wie das eines Melanoms zu erkennen.

Federated Learning, kurz FL, ist eine verteilte Form des maschinellen Lernens, bei der die Daten bei ihren Eigentümer*innen verbleiben und nicht an einen zentralen Server gesendet werden. Der Ablauf eines Federated Learning Systems ist folgendermaßen (siehe Abbildung 1b): Ein Aggregator sendet Kopien eines globalen Modells an die Clients des FL-Systems, die dieses Modell lokal auf ihren eigenen Daten für eine gewisse Zeit trainieren. Nach Abschluss des lokalen Trainingsverfahrens senden die Clients jeweils ihr Modell zurück an den Aggregator, der diese zu einem neuen globalen Modell aggregiert, welches in der nächsten Trainingsrunde weiter trainiert wird. Dieses Verfahren wird fortgesetzt, bis ein bestimmtes Kriterium erreicht ist, zum Beispiel, dass die Genauigkeit des globalen Modells 90 % betragen muss.

In diesem Beispiel würde das bedeuten, dass das globale Modell mit 90 %-iger Sicherheit ein Muster richtig erkennt. Um sicherzustellen, dass das Modell nicht nur die Daten, mit denen es trainiert wurde, erkennt, wird die Genauigkeit sowohl mit einem Validierungs- als auch einem Testdatensatz gemessen. Der Valdierungsdatensatz bietet eine unvoreingenommene Bewertung für die Modellanpassung an den Trainingsdatensatz, wodurch die Hyperparameter des Modells (z. B.: Architektur des Neuronalen Netzwerkes) angepasst werden. Ein Testdatensatz ist ein Datensatz, der verwendet wird, um eine unvoreingenommene Bewertung einer endgültigen Modellanpassung an den Trainingsdatensatz bereitzustellen. Wenn ein Modell für die Erkennung von Hautkrebs trainiert würde, dann bestünden diese Datensätze, zum Beispiel, aus Bildern, die Hautkrebs - oder nur normale Hautflecken - zeigen. Von den Bildern im Valdierungsdatensatz und Testdatensatz weiß man, was sie tatsächlich zeigen, da sie (manuell von Expert*innen) der Klasse „Krebs" oder „Kein-Krebs" zugeordnet wurden. Zur Validierung, ob das Modell nun richtig gelernt hat, wird der Valdierungsdatensatz verwendet[1]. Wenn das Modell 90 von 100 Bildern richtig klassifiziert, wäre das Kriterium erreicht. Falls das nicht der Fall ist, dann wird das Modell solange angepasst, bis es diesen Wert erreicht. Schlussendlich wird das finale Modell mithilfe des Testdatensatzes überprüft.

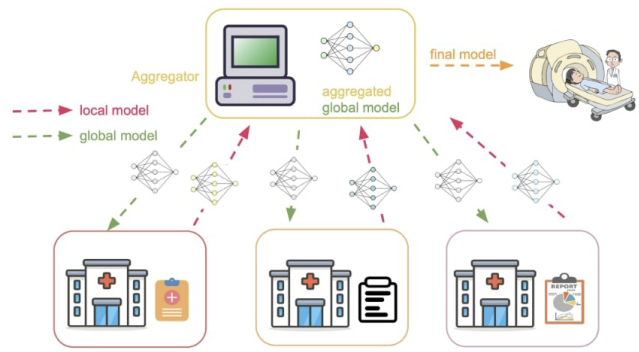
VORTEILE VON FEDERATED LEARNING

FL bietet viele Vorteile gegenüber zentralisiertem maschinellem Lernen, da die Privatsphäre der Dateneigentümer*innen gewahrt bleibt. Dadurch kann beispielsweise ein Modell, das Hautkrebs erkennt, auf Daten aus verschiedenen Krankenhäusern trainiert werden, ohne dass die Daten geteilt werden müssen. Des Weiteren bietet FL einen Schutz gegen einen „Single-Point-of-Failure", den zum Beispiel der zentrale Server im üblichen maschinellen Lernen bietet. Auf diesen Punkt könnte nämlich eine Person von außen verschiedene Attacken anwenden und somit zum Beispiel sensible Daten stehlen. Das wäre besonders im medizinischen Bereich fatal, da diese Daten einen hohen Grad an Sensibilität aufweisen. Dieses Risiko wird in FL gemindert, weil die Daten verteilt bleiben und nie die Besitzer*innen verlassen. Der/die Besitzer*in teilt mit dem Aggregator nur das mit seinen privaten Daten trainierte Modell. FL ermöglicht auch das gleichzeitige Trainieren von Modellen, womit es Zeit spart. Diese Form des maschinellen Lernens bietet mehr Datenvielfalt an, da das Modell kontinuierlich von verschiedenen Clients lernt und nicht von einem Datensatz, der potenziell die Realität verzerrt (durch z. B. zu wenig Repräsentation von einer Gruppe), wodurch das Modell repräsentativer und inklusiver wird. Beispielsweise kann ein FL-System in der Gesundheitsbranche aus mehreren Krankenhäusern bestehen, die sich in verschiedenen geografischen Gebieten befinden, was die Daten von Patient*in-



(a) Zentrales Machine Learning

Abb. 1

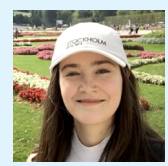


(b) Federated Learning

Abb. 2

nen diverser macht, wodurch weniger Verzerrung (Bias) entstehen kann.

Besonders im medizinischen Bereich ist internationale Kooperation (z. B. während einer Pandemie) wichtig, weshalb auch FL immer wichtiger wird. Die Modelle werden aufgrund der höheren Datendiversität durch die Zusammenarbeit von vielen Organisationen repräsentativer und bieten Schutz vor Datendiebstahl. Bereits in der Pandemie ist FL zum Einsatz gekommen, beispielsweise zur Vorhersage für den zukünftigen Sauerstoffbedarf von symptomatischen Patient*innen mit COVID-19 [3].



Diana Strauß, BSc, ist Masterstudentin in Software and Internet Computing an der TU Wien. Ihre Forschungsinteressen sind Federated Learning und Watermarking von Machine Learning Modellen.

Referenzen

[1] Bless Lord Y. Agbley u. a. "Multimodal Melanoma Detection with Federated Learning". In: 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). 2021, S. 238–244. DOI: 10.1109/ICCWAMTIP53232.2021.9674116.

[2] Kinnor Das u. a. "Machine Learning and Its Application in Skin Cancer". In: International Journal of Environmental Research and Public Health 18.24 (2021). ISSN: 1660-4601. DOI: 10.3390/ ijerph182413409. URL: https://www.mdpi.com/1660-4601/18/24/13409.

[3] Ittai Dayan u. a. "Federated learning for predicting clinical outcomes in patients with COVID-19." In: Nature Medicine 27.10 (Sep. 2021), S. 1735–1743. URL: https://www.microsoft.com/en- us/research/publication/federated-learning-for-predicting-clinical-outcomes-in- patients-with-covid-19/.

[4] Walaa Gouda u. a. "Detection of Skin Cancer Based on Skin Lesion Images Using Deep Lear- ning". In: Healthcare 10.7 (2022). ISSN: 2227-9032. DOI: 10.3390/healthcare10071183. URL: https://www.mdpi.com/2227-9032/10/7/1183.

von Manuel Kern

Mit SPOTTED Bedrohungen erkennen

Im letzten Jahrzehnt gab es einen Paradigmenwechsel. Während man lange davon ausging, dass es ausreicht, Ressourcen für die Informationssicherheit primär auf Präventions- und Schutzmaßnahmen (beispielsweise den Betrieb von Firewalls und Anti-Viren Software) oder das Durchführen von Penetrationstests zu lenken, geht man mittlerweile davon aus, dass es früher oder später einen erfolgreichen Angriff auf die Infrastruktur geben wird.

Während Präventions- und Schutzmaßnahmen nach wie vor unverzichtbar sind, investieren immer mehr Unternehmen in wichtige Erkennungs- und Reaktionsmaßnahmen. Die Tatsache, dass professionelle Angreifer oft über einen langen Zeitraum im Netz operieren, ist in der Forschung schon lange bekannt. Dennoch ist die durchschnittliche Zeit bis zur Entdeckung von Angreifern nach wie vor hoch. Im Rahmen einer von IBM Security [L1] in Auftrag gegebenen Studie wird die durchschnittliche Zeit bis zur Entdeckung eines Angriffs mit 212 Tagen beziffert. Ende 2020 wurde der katastrophale Fall von SolarWinds öffentlich [L2]. Staatliche Angreifer missbrauchten den Update-Mechanismus einer Sicherheitslösung und konnten Tausende teils wichtige staatliche Organisationen infiltrieren und viele Monate unbemerkt in den Netzwerken agieren. Kaspersky [L3] schätzt, dass Wiederherstellungskosten bei sofortiger Erkennung von Cyber-Angriffen viermal niedriger ausfallen als bei Behebung nach einer Woche. Der Versicherungsanbieter Allianz [L4] beziffert einen Gesamtschaden von 660 Millionen Euro bei 1.736 Vorfällen und einen steigenden Trend der gemeldeten Vorfälle, während der größte Teil der Kosten auf betriebliche Ausfallzeiten fällt.

EFFIZIENTE ERKENNUNGSSYSTEME

Das Projekt SPOTTED (Systematic Mapping of Detection Approaches on Data Sources), welches im Rahmen der industrienahen Dissertationen von der FFG finanziell unterstützt wird, setzt sich zum Ziel, Wissen und Methoden im Bereich der Angreifer-Erkennung zu schaffen. Die Implementierung von Erkennungs- und Reaktionsmaßnahmen sind ressourcenintensive Unterfangen. Es ist nicht nur schwierig, die richtigen Softwarelösungen aus dem rasch wachsenden Pool an Lösungen passend für ein Unternehmen auszuwählen, auch die Konfiguration und der Betrieb ist mit hohen Kosten verbunden. Es erfordert Sicherheitsexpert*innen, um diese Lösungen passend für eine IT-Infrastruktur zu konzipieren, zu installieren und zu betreiben. Sicherheitsexpert*innen sind aufgrund von Personalengpässen aktuell eher schwierig zu finden und meist auch sehr teuer. Neben dem Personalmangel sind für Erkennung und Reaktion spezielle Infrastrukturen mit hohen Leistungsanforderungen erforderlich. Effiziente Erkennungssysteme für große Infrastrukturen sind kein Produkt von der Stange, die Implementierung von infrastrukturweiten Erkennungssystemen kann schnell das gesamte IT-Sicherheitsbudget aufbrauchen. Es besteht eine hohe Wahrscheinlichkeit, dass Erkennungs- und Reaktionsprojekte von vornherein abgelehnt, abgebrochen oder unvollständig durchgeführt werden.

Die Aufgabe des Projekts SPOTTED besteht darin, diesen Problemen entgegenzuwirken, indem die Einstiegshürde für moderne Überwachungs- und Erkennungslösungen gesenkt und ihre Anwendbarkeit verbessert wird. Ein Zwischenergebnis ist das entwickelte Prozessmodell D3TECT. In Abbildung 1 wird die Wechselwirkungen von Angriffs-Techniken auf eine Organisation beleuchtet. Das Modell beschreibt ein Verfahren [L5] zur risikobasierten und priorisierten Auswahl der für die Erkennung geeigneten Datenquellen. Das Modell berücksichtigt dabei auch Einschränkungen in der Datenselektion, wenn beispielsweise eine bestimmte Datenquelle, z. B. aufgrund von Datenschutzbeschränkungen, in einem Umfeld nicht genutzt werden kann. Letztendlich löst der D3TECT-Ansatz die Herausforderung, Datenquellen strategisch auszuwählen und dabei ihre unterschiedliche Nützlichkeit für die Angriffserkennung zu berücksichtigen. Als Datengrundlage wurde das MITRE ATT&CK-Framework und zahlreiche öffentliche Datenbanken mit Cyber-Bedrohungsdaten verarbeitet. In einer weiteren, demnächst veröffentlichten Forschungsarbeit wird das Modell erweitert, um Organisationen bei der optimalen Auswahl der für sie passenden Erkennungssoftware zu unterstützen.

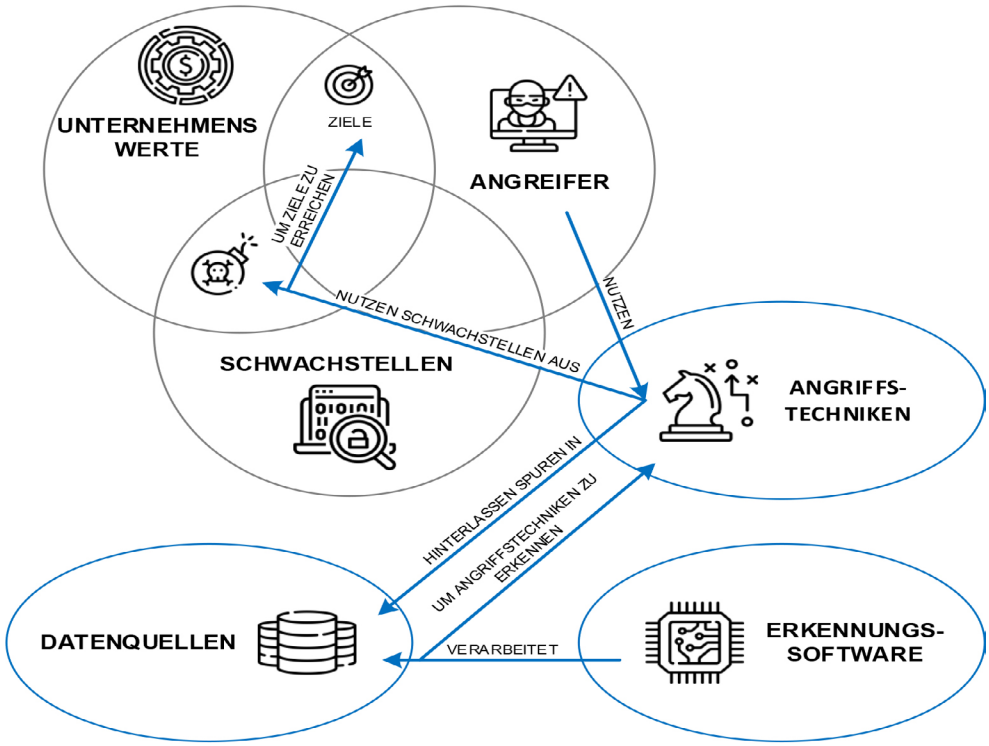
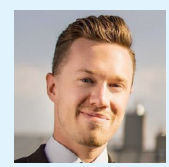


Abbildung 1: Wechselwirkungen von Angriffs-Techniken auf eine Organisation



Manuel Kern arbeitet derzeit am AIT Center for Digital Safety & Security an seiner Dissertation und als Penetration Testing Team Lead. Nebenberuflich ist er als ISO 27001 und NIS-G Auditor tätig.

Referenzen:

[L1] https://www.ibm.com/security/data-breach

[L2] https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/

[L3] https://www.kaspersky.com/blog/security_risks_report_financial_impact/

[L4] https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020.html

[L5] M. Kern, et al.: "Strategic selection of data sources for cyber attack detection in enterprise networks: A survey and approach", 37th ACM/SIGAPP Symposium On Applied Computing, 2022. https://dl.acm.org/doi/abs/10.1145/3477314.3507022

von Philipp Hofer

Dezentrale Gesichtserkennung

Biometrische Daten gehören zu den datenschutzrechtlich besonders sensiblen Daten. Immer mehr Systeme verwerten diese Daten. Da diese (zumindest technisch) ihre Existenz nicht offenlegen müssen, kann es keine vollständige Liste von Systemen geben, welche die eigenen persönlichen Daten verarbeiten. Zumindest jene Systeme, welche reale Konsequenzen verursachen, sind der Öffentlichkeit jedoch bekannt. I

n China bekommt jede Person einen Score, der sich ändert, je nachdem welche Entscheidungen im täglichen Leben getroffen werden und ob diese Entscheidungen im Einklang mit der aktuellen Regierung sind. In Indien erhält jede Person eine 12-stellige Nummer, welche laufend mit biometrischen Merkmalen ergänzt wird und für viele Teile des Lebens benötigt wird [1]. Leider häufen sich die Meldungen, dass immer mehr Datenbanken mit biometrischen Merkmalen erstellt werden. So wurde etwa in Moskau 2021 ein Gesichtserkennungssystem ausgerollt, welches das Bezahlen von Tickets in deren Metro erleichtern soll [2]. Darüber hinaus wird die Identifizierung von Personen anhand gigantischer Bilddatenbanken aus Social Media Plattformen, Zeitungen etc. als Dienstleistung angeboten [3].

GROSSE DATENMENGEN – GROSSE GEFAHREN

Der Großteil der Systeme basiert auf einem zentralen Ansatz: Riesige Datenmengen werden an einem Punkt gesammelt und gespeichert. Dies macht solche Systeme besonders anfällig für mehrere Angriffsvektoren:

1. Personen müssen ihrem Anbieter vertrauen. Nachdem die Daten an einem zentralen Punkt liegen, müssen alle Anfragen über diesen Punkt laufen. Das ermöglicht dem Betreiber umfassende Möglichkeiten zu zahlreichen Analysen dieser (Meta-)Daten und öffnet das Risiko, umfangreiche Verhaltensmuster zu identifizieren.

2. Ein zentraler Platz mit potenziell Milliarden an Personendaten ist ein ausgezeichnetes Ziel für technische, rechtliche und organisatorische Angriffe. Leider kommt es auch unter den höchsten Sicherheitsvorkehrungen selbst (oder besonders) bei den größten Anbietern immer wieder zu Datenpannen [4].

PRIVATE DIGITALE AUTHENTIFIZIERUNG – PROJEKT DIGIDOW

Um sich diesen Angriffsvektoren erst gar nicht auszusetzen, kann stattdessen auf einen dezentralen Ansatz gesetzt werden, bei dem Daten nicht an einer Stelle gesammelt werden. Dabei stellen sich neue Fragen, wie zum Beispiel eine Kamera die korrekte Stelle findet, an der die Daten für eine Person gespeichert sind oder wie Gesichtserkennung ohne große GPU-Cluster funktionieren kann.

Dazu gibt es noch wenig Forschung. Das CD-Labor Digidow [5] hat das Ziel, ein System vorzuschlagen, mit dem dezentrale, private und digitale Authentifizierung in der physischen Welt umgesetzt werden kann. Hierbei erfolgt die Berechnung auf lokaler Hardware direkt am Sensor.

Wo die Berechnung bei zentralen Systemen passiert, kann aufgrund der fehlenden technischen Details für die Öffentlichkeit nicht mit Sicherheit gesagt werden. Wahrscheinlich ist es, dass die Video-Feeds zu einem Server weitergeleitet werden, der dann die hardwareintensiven Berechnungen vornimmt. Bei dezentralen Systemen sollten alle Berechnungen am Gerät selbst stattfinden, um möglichst wenig potenziell Privatsphäre-relevante Informationen überhaupt erst zu generieren.

Deshalb experimentieren wir mit State-of-the-Art Gesichtserkennung, welche auf einem Embedded System ausgeführt werden kann. Gesichtserkennung kann entweder auf einem Video oder einem Foto basieren. Eingebettete Systeme kommen bei Video-Gesichtserkennung an ihre Leistungsgrenze, weshalb unser Systemvorschlag Foto-basierende Netzwerke verwendet und dessen Ergebnisse kombiniert. Den weitaus rechenintensiveren Teil (~ 75 %) stellt dabei das Erkennen der Gesichter (Face Detection) in einem Bild dar.

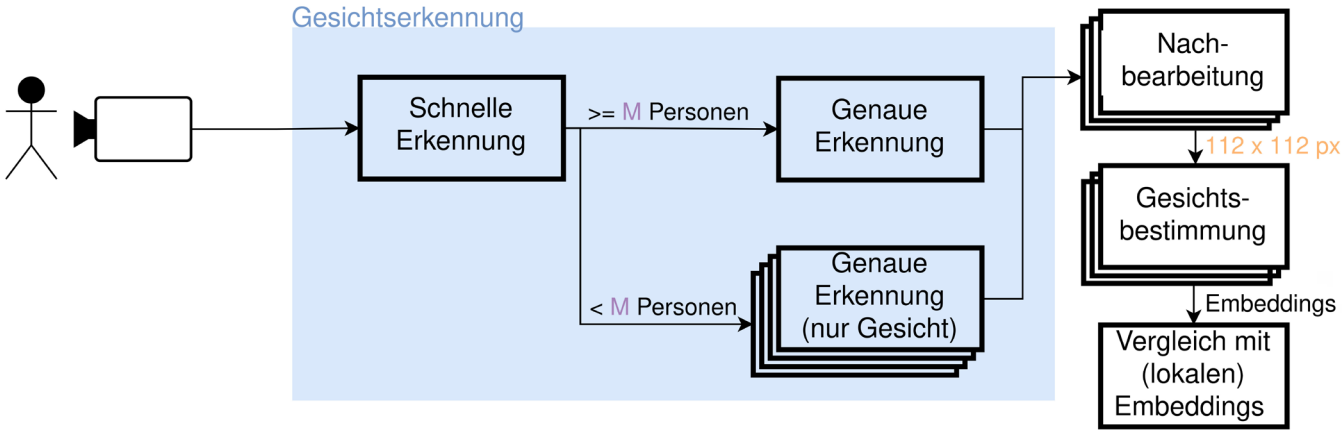
Unser Systemvorschlag kombiniert deshalb mehrere Gesichtserkennungsmodelle (siehe Abbildung):

Zuerst kommt ein weniger genaues, dafür schnelles Modell zum Einsatz, um potenzielle Gesichter im Bild zu erkennen. Diese Vorschläge werden im Anschluss mit einem genaueren, dafür langsameren Netzwerk überprüft und weiter gefiltert. Wenn jedoch das schnelle Modell so viele Personen erkennt (M), dass es rechentechnisch langsamer wäre, all diese Vorschläge zu überprüfen, wird stattdessen das gesamte Bild als Input für das genaue Netzwerk verwendet.

Anschließend wird aus dem Gesicht mithilfe von neuronalen Netzwerken ein Embedding berechnet (Face Recognition), welches eine numerische Repräsentation eines Gesichts ist. Im Vergleich zum Erkennen der Gesichter ist der Rechenaufwand für den Gesichtsabgleich mit Referenzdaten gering (auf einem Jetson Nano [6] als Beispiel für ein Embedded System ~ 150 ms).

Um an die deutlich besseren Ergebnis-

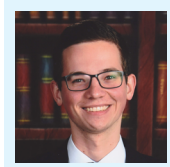
Abbildung: Beschreibung Abbildung: Digidow-Architektur für effiziente Gesichtserkennung auf einem Embedded System Skizze Hofer



se von Video-basierter Gesichtserkennung anschließen zu können, werden mehrere dieser Foto-basierten Embeddings kombiniert [7]. Wie viele Embeddings kombiniert werden müssen, um eine ausreichende Genauigkeit zu haben, ist abhängig von der spezifischen Anwendung: Das Mitprotokollieren der Anwesenheit in Vorlesungen wird wahrscheinlich weniger Genauigkeit erfordern als die Identitätsfeststellung bei einem Grenzübertritt. Deshalb entwickeln wir eine domänenspezifische Sprache, um es Anwender*innen unseres Systems allgemein zu ermöglichen, das individuelle Sicherheitslevel zu definieren.

Eine weitere Forschungsrichtung ist die Analyse der Robustheit von aktuellen Gesichtserkennungsmodellen. Wie verhalten sich die tiefen neuronalen Netzwerke, wenn die Realität sich deutlich von den Daten unterscheidet, mit denen das Netzwerk ursprünglich trainiert wurde? Ein gutes Beispiel hierfür sind die letzten Jahre: Gesichtsmasken waren (zumindest in westlichen Ländern) vor 2020 kaum verbreitet, weshalb auch Datensätze zum Trainieren von Gesichtserkennungsmethoden Bilder mit Gesichtsmasken nur im Promillebereich beinhalten [8].

Wir hoffen, dass zukünftige biometrische Authentifizierungssysteme verstärkt auf dezentrale, Privatsphäre-schonende Ansätze setzen. Das CD-Labor Digidow unterstützt dies durch die Erforschung neuer praxistauglicher Lösungsansätze.



Philipp Hofer arbeitet am Institut für Netzwerke und Sicherheit an der Johannes Kepler Universität Linz. Seine Dissertation beschäftigt sich mit globaler, Verteiler-biometrischer Authentifizierung von Personen unter minimaler Beeinträchtigung der Privatsphäre.

Referenzen:

[1]: https://uidai.gov.in/en/, zugegriffen am 2. Februar 2023

[2]: https://www.mos.ru/news/item/97579073/, zugegriffen am 2. Februar 2023

[3]: https://www.clearview.ai/, zugegriffen am 2. Februar 2023

[4]: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, zugegriffen am 2. Februar 2023

[5]: https://digidow.eu, zugegriffen am 2. Februar 2023

[6]: https://developer.nvidia.com/embedded/jetson-nano, zugegriffen am 2. Februar 2023

[7]: Philipp Hofer et al., „Efficient Aggregation of Face Embeddings for Decentralized Face Recognition Deployments". Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023). Accepted for publication. Lisbon, Portugal, Feb. 2023.

[8]: Philipp Hofer et al., „Importance of different facial parts for face detection networks". 2021 9th IEEE International Workshop on Biometrics and Forensics (IWBF). Rome, Italy: IEEE, Mai 2021, S. 1–6. doi: 10.1109/IWBF50991.2021.9465087.

von Michael Koppmann

Alternatives Autorisierungsmodell

Sicherheitsschwachstellen kosten Firmen weltweit mehrere Milliarden Euro pro Jahr. Einige dieser Schwachstellen kommen häufiger vor als andere. Es ist also sinnvoll, die großen Brocken zuerst aus dem Weg zu schaffen. Dazu gibt es einige Listen, unter anderem vom Open Web Application Security Project, der OWASP. Diese veröffentlicht regelmäßig Top-10-Listen der häufigsten Risiken in Web-Applikationen. Fehlerhafte Umsetzungen der Zugriffskontrollen belegen momentan den ersten Platz.

Heutzutage werden mehr und mehr Applikationen geschrieben, die in Browsern ausgeführt werden. Das Web dient dabei als betriebssystemunabhängige Applikationsplattform. Dadurch ändert sich auch das zugrundeliegende Autorisierungsmodell, das nun nicht mehr ausschließlich vom Betriebssystem kontrolliert wird. Stattdessen werden Berechtigungsüberprüfungen nun von den Applikationen selbst implementiert. Aufgrund der darin liegenden Komplexität führt dies jedoch zu der genannten Häufung an Schwachstellen in diesem Bereich.

Die meisten Applikationen bauen auf dem Konzept der Zugriffskontrolllisten auf, einem Sicherheitsmodell, das bestimmt, wer auf welche Objekte zugreifen darf. Dieses Modell baut auf digitalen Identitäten und deren Beziehungen zu Ressourcen auf. Jede Ressource enthält eine Liste an berechtigten Subjekten oder Gruppen, die auf diese Ressource zugreifen dürfen. Diese Zugriffskontrolle findet implizit beim Durchführen von Aktionen statt; die Überprüfung der Identität findet dabei in einem separaten Schritt statt. Dieses Prinzip ist als „Ambient Authority" bekannt. Und genau darin liegt das Kernproblem der Zugriffskontroll-Liste. (Tabelle 1)

Dieses Konzept stammt aus dem militärischen Bereich. In der physikalischen

User	/etc/passwd	/home/alice/secret.txt	/home/bob/shared.txt
Alice	(read)	(read, write)	(read)
Bob	(read)	()	(read, write)
Carol	(read)	()	()

Table 1: Access Control Matrix example

Tabelle 1:Beispiel einer Zugriffskontroll-Liste

Welt ist es leicht dieses zu erzwingen. Identitäten von Personen können überprüft werden und man möchte nicht beim Betrügen erwischt werden, wenn man vor einem Militär-Trupp steht. Doch in der digitalen Welt verschwimmen die Grenzen von Identitäten. Wir nutzen täglich Software, die von tausenden Personen weltweit entwickelt wurden. Wenn Sie ein Programm auf Ihrem Computer benutzen, läuft es mit Ihren Berechtigungen. Enthält dieses Programm bösartige Zeilen Code und ist beispielsweise eine Ransomware, kann dieses Stück Software alles machen, was Sie machen dürfen, inklusive dem Verschlüsseln aller Ihrer Daten. Das Betriebssystem kann nicht unterscheiden, ob die Aktionen absichtlich von Ihnen oder von einer bösartigen App gestartet wurden, da alles mit Ihrer Identität durchgeführt wurde.

Object Capabilities stellen ein alternatives Autorisierungsmodell dar und haben diese fundamentale Schwachstelle nicht. Sie sind vergleichbar mit Schlüsseln. Das Verweisen auf Objekte, beziehungsweise das Durchführen von Aktionen ist direkt an die Zugriffskontrolle gekoppelt und stellt keinen separaten Schritt dar. Eine Capability referenziert eine Ressource und enthält gleichzeitig bereits die freigegebenen Berechtigungen; wie ein Autoschlüssel, der an ein bestimmtes Auto gebunden ist und es ermöglicht dieses zu fahren. Sie müssen sich nicht erst im

Vulnerability class	Protection level	
	Pure OCAP system Eselsohr	
A1:2017-Injection	◐	◐
A2:2017-Broken Authentication	◐	●
A3:2017-Sensitive Data Exposure	◐	●
A4:2017-XML External Entities (XXE)	-	◐
A5:2017-Broken Access Control	●	●
A6:2017-Security Misconfiguration	○	○
A7:2017-Cross-Site Scripting (XSS)	●	●
A8:2017-Insecure Deserialization	◐	●
A9:2017-Using Components with Known Vulnerabilities	◐	●
A10:2017-Insufficient Logging & Monitoring	○	○

●=prevention ◐=mitigation; ○=no effect; -=not analyzed;

Table 2: Securitv analvsis results

Tabelle 2: Ergebnisse der Sicherheitesanalyse

Auto beim Hersteller melden und Ihre Identität bestätigen lassen, bevor Sie losfahren dürfen. Ein bösartiges Programm in einer Object Capability Welt kann daher standardmäßig gar nichts, da sie nicht im Besitz dieser Schlüssel und somit harmlos ist.

Im Zuge meiner Diplomarbeit habe ich Object Capabilities und deren Vorteile für die Sicherheit von Web-Applikationen näher analysiert. Dabei habe ich unter anderem einen Prototyp einer Web-Applikation erstellt und diesen einer Sicherheitsüberprüfung unterzogen. Die Ergebnisse sind vielversprechend und diese Sicherheitstoken bieten durchaus viele weitere Vorzüge. Es sind jedoch viele Anpassungen in bestehender Software wie Webbrowser notwendig, um von sämtlichen Vorteilen dieses Autorisierungsmodells zu profitieren.

Michael Koppmann ist Senior Information Security Consultant bei SBA Research in Wien. Neben der Durchführung von Penetrationstests, forscht er auf den Gebieten der sicheren und nachhaltigen Softwareentwicklung

Datenschutz durch Privacy-Enhancing Technologies

von Lukas Helminger

Corona Heatmap

Die Corona Heatmap zeigt, wo sich Infizierte im Ansteckungszeitraum vermehrt aufgehalten haben. Diese Heatmap kann einen Beitrag zur Erkennung von Ansteckungshotspots leisten. Dabei berücksichtigt unsere Lösung den notwendigen Datenschutz durch den Einsatz von Privacy-Enhancing Technologies.

PROBLEMSTELLUNG

Es werden insgesamt zwei Datensätze benötigt. Zum einen die Handynummern der Corona-Patient*innen, über welche die Behörden verfügen und zum anderen die Standortdaten von Mobilfunkanbietern. Durch eine Anfrage für die Standortdaten von Seiten der Behörden würde der Mobilfunkanbieter Kenntnis über die Identität von Corona-positiv getesteten Personen bekommen. Umgekehrt hätten die Gesundheitsbehörden die Bewegungsdaten von individuellen Personen. Der Datenschutz ist also nicht garantiert, da

- Patientendaten geleakt werden und
- individuelle Überwachung ermöglicht wird.

LÖSUNG

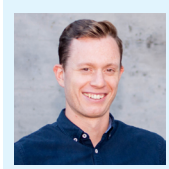
Anstatt zu vertrauen, dass niemand die Daten missbraucht, werden mathematische Sicherheiten verwendet.

- Bewegungsprofile werden zusammengefasst und wenn nötig durch Rauschen weiter anonymisiert, sodass keine Rückschlüsse auf einzelne Personen möglich sind (Differential Privacy).
- Patientendaten werden mit neuartiger Verschlüsselung geschützt (Homomorphe Verschlüsselung), die erstmals ermöglicht mit verschlüsselten Daten zu rechnen.

WEITERENTWICKLUNG

Als Konsequenz dieses und ähnlicher Forschungprojekte wurde die TACEO GmbH als Spin-off des Know-Centers und der Technischen Universität Graz mit dem Ziel gegründet, neueste Ergebnisse und Erkenntnisse aus der wissenschaftlichen Forschung in die industrielle Anwendung zu übertragen. Konkret in den folgenden Bereichen:

- Privacy-Enhancing Technologies: Schützen Sie die Privatsphäre Ihrer Daten auch während der Berechnungen (Multiparty Computation & Fully Homomorphic Encryption).
- Post-Quantum-Kryptographie: Schützen Sie Ihre Daten auch in der Zukunft, indem Sie sich auf Technologien verlassen, die für Angriffe durch Quantencomputer nicht anfällig sind.
- Zero-Knowledge-Proofs: Schützen Sie die Vertraulichkeit Ihrer Daten, während Sie anderen Parteien Eigenschaften über Ihre Daten beweisen.



Dip. Ing. **Lukas Helminger**, BSc. ist Geschäftsführer bei TACEO, einem Spin-off der TU Graz und des Know-Centers im Bereich Data Sharing und Privacy. Zuvor war er Forscher auf dem Gebiet der datenschutzfreundlichen Datenanalyse in EU-weiten Projekten tätig.

Wie Datenbesuche die Forschung stärken können

von Martin Weise

Sichere Dateninfrastrukturen in der Forschung

Fortschreitende Digitalisierung führt zur Erhebung und Speicherung von Daten in jedem Lebensbereich. Viele dieser (oft sensiblen) Datensätze sind lokal bei Dateneigentümer*innen vorhanden, jedoch unzugänglich für die einzelnen Forscher*innen. Einsicht in Kombination mit Möglichkeiten zur Analyse dieser Datensätze kann besonders hilfreich für die Beantwortung von Forschungsfragen sein, gestaltet sich aber aufwändig, um sicherzustellen, dass keine Daten die Infrastruktur der Dateneigentümer*innen verlassen können.

Kontrolle und Schutz von sensiblen Daten bei gleichzeitiger Vergabe von Zugriff an Dritte scheint nicht nur im Widerspruch zu stehen, sondern die technische Umsetzung stellt auch eine bedeutsame Herausforderung für Dateneigentümer*innen dar. Sichere Dateninfrastrukturen, die Datenbesuche in einer überwachten und kontrollierten Umgebung ermöglichen, können – falls ordnungsgemäß errichtet und betrieben – hohe Sicherheitsgarantien durch technische, juristische und prozessgetriebene Mechanismen bieten. Obwohl es weltweit viele sichere Dateninfrastrukturen gibt, die in unterschiedlichen Disziplinen eingesetzt werden, können die technischen Konzepte und grundlegenden Abläufe, um Zugriff auf sensible Daten zu erhalten mit dem Five Safes Framework [1] beschrieben werden. Dieses Bezugssystem modelliert Datenzugriffe in fünf Risikodimensionen zum Forschungsvorhaben, den Personen, den Daten, des Umfelds und den Ergebnissen, die durch Zugriff auf sensible Daten entstehen.

Um die Existenz der sensiblen Daten überhaupt zu kennen, müssen Dateneigentümer*innen, die sensible Daten Dritten zur Verfügung stellen möchten, vorerst Beschreibungen (Metadaten) zu jedem Datensatz in einem Katalog bekanntmachen. Diese Metadaten enthalten spezifische Informationen über den Datensatz, die dabei helfen, einen geeigneten Datensatz besser zu finden, Metadaten enthalten keine sensiblen Daten.

AM ANFANG STEHT DIE FORSCHUNGSFRAGE

Alles startet mit der Definition der Forschungsfrage und der anschließenden Suche in dem Datenkatalog nach einem Datensatz, der bei der Beantwortung der Forschungsfrage die notwendige Datenevidenz liefert. Falls zur Beantwortung mehrere Datensätze notwendig sind, müssen mehrere Ansuchen gestellt werden und die Dateneigentümer*innen prüfen genau, ob durch die Verlinkung ungewollte Querverbindungen möglich sind, die nicht relevant zur Forschungsfrage sind. Es ist möglich, dass eine Kommission über die Zulässigkeit der Forschungsfrage entscheiden muss. Um Zugang zu den sensiblen Daten zu erhalten, müssen Forscher*innen einen Antrag bei den Dateneigentümer*innen stellen. Dieser umfasst neben dem Datensatz, der analysiert werden soll:

- Forschungsfragen
- Informationen zur Identität des/der Forscher*in
- Liste der Applikationen, die für die Analyse notwendig sind

Nach erfolgreicher Prüfung erhalten die Forscher*innen Zugriff auf den für die Beantwortung der Forschungsfrage relevanten Teil des Datensatzes für einen bestimmen Zeitraum. Damit die Daten allerdings nicht von den Dateneigentümer*innen zu den Forscher*innen abfließen können (was einem Verlust der Kontrolle über den Datensatz gleichkommt), gibt es zwei etablierte Methoden.

Methode 1 Der relevante Teildatensatz wird auf einem isolierten Computer in einem physischen Sicherheitsraum zur Verfügung gestellt, auf dem alle für die Analyse notwendigen Applikationen bereits installiert sind. Darunter fallen auch Textsatz-Applikationen zum Verfassen von Berichten. Bis auf verifizierte Lizenzserver dieser Applikationen sind alle Verbindungen zum Internet gesperrt und es kann kein Massenspeicher an diesen Computer angeschlossen werden, die Daten verlassen die Infrastruktur nicht. Zusätzlich wird dieser Computer überwacht und Zugang zu diesem Sicherheitsraum wird nur unter Aufsicht gestattet.

Methode 2 Der relevante Teildatensatz wird auf einer virtuellen Schreibtischoberfläche zur Verfügung gestellt, die ähnlich zur ersten Methode keinerlei Verbindungen außerhalb der Infrastruktur zulässt, allerdings müssen die Forscher*innen keinen physischen Sicherheitsraum besuchen, sondern können mittels verschlüsselte Netzwerkverbindungen und der virtuellen Schreibtischoberfläche so arbeiten, als wären sie physisch in dem Sicherheitsraum anwesend. Diese Umgebung kann durch Überwa-

chung der Ein- und Ausgaben, Aufzeichnung des Videokanals durch die Dateneigentümer*innen, ob die durchgeführten Analysen weiterhin zur Forschungsfrage passen, ständig und jederzeit geprüft und - falls notwendig - der Zugriff sofort entzogen werden.

HOHE SICHERHEITSGARANTIEN FÜR SENSIBLE DATEN

Homomorphe Verschlüsselung erlaubt eine mathematische Funktion auf verschlüsselten Daten durchzuführen, ohne die unverschlüsselten Daten zu kennen. Das ist möglich aufgrund der homomorphen Eigenschaften der verschlüsselten Daten, die es erlauben, Berechnungen so auszuführen, als wären sie auf den unverschlüsselten Daten ausgeführt worden - die Ergebnisse sind gleich. Dadurch entstehen sehr hohe Sicherheitsgarantien für sensible Daten. Da Forscher*innen, besonders Angehörige von anerkannten, wissenschaftlichen Einrichtungen grundsätzlich nicht böswillig sind, werden in sicheren Dateninfrastrukturen andere Sicherheitsmodelle verwendet, die im Vergleich zur homomorphen Verschlüsselung mehr Flexibilität in der Analyse zulassen.

Ein Ansatz, um die Kontrolle und den Schutz von sensiblen Daten bei gleichzeitiger Vergabe von Zugriff an Dritte zu realisieren, wurde Februar 2022 von einem Team der Forschungsgruppe Data Science an der TU Wien publiziert [2]. die sich mit der technischen Beschreibung und prototypischen Implementierung einer quelloffenen sicheren Dateninfrastruktur beschäftigt. Der Kern des Ansatzes ist eine Luftbrücke zwischen einem zentralen Datenserver, auf dem sensible Datensets verfügbar sind und der restlichen Dateninfrastruktur. Dieser zentrale Datenserver steht in einem separaten, verschlossenen Serverschrank, zu dem nur ein vertrauenswürdiger Techniker Zugang hat, wobei der Zugang zu dem Serverraum selbst von einem anderen Techniker im Vier-Augen-Prinzip gestattet wird. Infrastruktur-interne Verbindungen, um die Luftbrücke zu schließen sind nur zum Zweck des Einspielens von neuen sensiblen Daten, Kopieren eines relevanten Teildatensets auf die virtuelle Schreibtischoberfläche und zum Durchführen von kritischen Sicherheitsaktualisierungen erlaubt und auch nur für die Dauer dieser Operationen. Der Zugriff auf Daten folgt Methode 2 und erlaubt Forscher*innen das Arbeiten mit sensiblen Daten von überall aus der Welt durch die Verwendung eines mehrschichtigen Konzeptes durch verschlüsselte Netzwerkverbindungen, Bildübertragungsprotokolle und virtuelle Schreibtischumgebungen, auf denen bereits die angeforderten Applikationen und der relevante Teildatensatz vorhanden sind. Nachdem die Forscher*innen mit der Analyse des Datensatzes fertig sind, kann bei den Dateneigentümer*innen eine Ausfuhr von Ergebnissen (Bericht, Grafik, trainiertes Machine Learning-Modell) beantragt werden, sofern keine sensiblen Daten das System verlassen.

Martin Weise ist Projektassistent an der Technischen Universität Wien. Seine Forschung befasst sich mit sicheren Dateninfrastrukturen und Management von Forschungsdaten. Derzeit entwickelt er zusammen mit einem Team der Universität Wien ein neuartiges Repositorium für Daten in Datenbanken.

Referenzen:

[1]: Desai, F., Ritchie, & R., Welpton. (2016). Five Safes. Designing Data Access for Research

[2]:M.,Weise, F., Kovacevic, N., Popper & A., Rauber. (2022). OSSDIP. Open Source Secure Data Infrastructure and Processes Supporting Data Visiting. Data Science Journal, 21(1), p.4. http://doi.org/10.5334/dsj-2022-004

von Daryna Oliynyk

Schutz des geistigen Eigentums

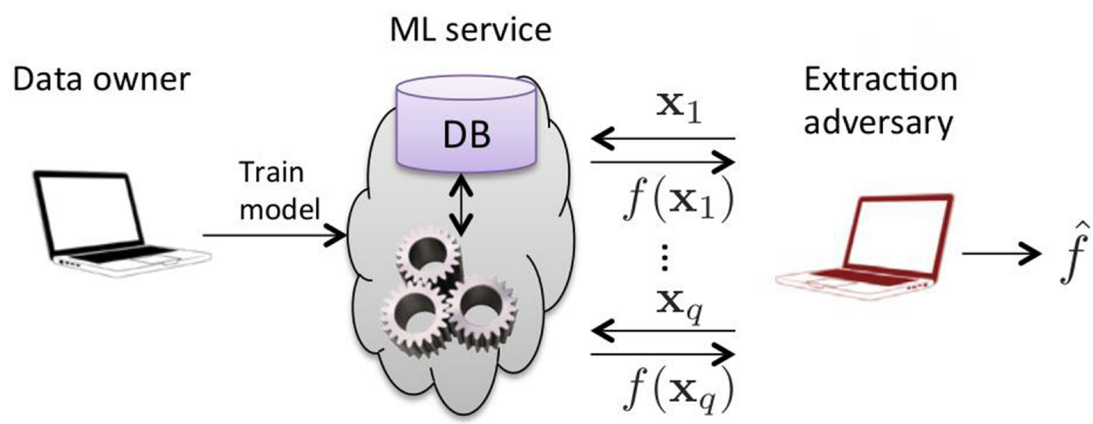
Systeme, die auf maschinellem Lernen (Machine Learning; ML) basieren, setzen sich vermehrt im Alltag durch. Eine der jüngsten Entwicklungen, ChatGPT, kann Unterhaltungen in einem menschenähnlichen Stil führen und komplexe Fragen korrekt beantworten. Die Entwicklung einer solchen Lösung, die an oder sogar über menschliche Fähigkeiten heranreicht, hat zwar viele Anwendungsmöglichkeiten, ist aber auch ein kostspieliger Prozess, der sowohl Ressourcen als auch Expertenwissen erfordert: Angefangen bei der Datenerfassung (Kontrolle ihrer Qualität, Einhaltung von Datenschutzbestimmungen, Festlegung geeigneter Schritte zur Datenvorverarbeitung) über die Definition einer geeigneten Architektur des Machine Learning Modells bis zur Überwachung von Trainingsprozess sowie der Anpassung des Modells auf Grundlage von Evaluierungsmetriken.

Da das Trainieren von Modellen ein sehr zeitaufwändiger Prozess sein kann, ist eine ausreichende Rechenleistung entscheidend. LambdaLabs hat geschätzt, dass allein das Training des GPT-3-Modells, das als Basismodell für ChatGPT dient, 4,6 Millionen Dollar gekostet hat. Die Entwicklung ist jedoch nicht nur ein teurer, sondern auch ein langwieriger Prozess. Alles in allem wird das Modell dadurch zu einem wertvollen Produkt, das als geistiges Eigentum der Besitzer*innen betrachtet werden kann.

DIEBSTAHL UND UNBEFUGTE NUTZUNG

Wenn ein ML-Modell an Kund*innen weitergegeben wird, werden die Nutzung sowie die Weitergabe des Modells in der Regel in einer Lizenzvereinbarung festgelegt und eingeschränkt. Wenn jemand jedoch gegen die Lizenz verstößt und das Modell unbefugt teilt, wird der Nachweis des Verstoßes zu einer Herausforderung. Ein Modell ist sogar auch dann gefährdet, wenn es nicht direkt als eigenständiges Produkt vom Hersteller an die Nutzer*innen ausgeliefert wurde, sondern als Teil eines anderen Produktes und beispielsweise eingebunden über eine API genutzt wird. Tramer et al. [1] haben als Erste beschrieben, wie ein als API freigegebenes Modell gestohlen werden kann. Der Diebstahlsprozess ist in Abbildung 1 dargestellt. Ein*e böswillige*r Benutzer*in sendet Eingabedaten an das Modell und sammelt die Antworten des Modelles darauf, zum Beispiel die Klassifikationsergebnisse in einer medizinischen Datenanalyse. Die gewonnenen Informationen werden dann zum Trainieren eines anderen Modells verwendet, welches schlussendlich eine vergleichbare Leistung wie das ursprüngliche Modell erbringt.

Diese Art von Angriffen wird als „Model Stealing“ bezeichnet. Ein Modell ist auch dann gefährdet, wenn es in einem Hardwaregerät verwendet wird oder in eine mobile Anwendung eingebettet ist. Es kann zum Beispiel der Netzwerkverkehr inspizieren werden, um die für den Modelldiebstahl erforderlichen Informationen zu sammeln oder es können



Abb, 1: Diebstahlsprozess in einem ML-as-a-Service Setting (Quelle: Tramer et al. [1])

verschiedene Aspekte des Modells gestohlen werden, z. B. die Architektur eines komplexen neuronalen Netzwerkes, gelernte Parameter oder Trainings-Hyperparameter [2]. Mit diesem Wissen ist ein Angriff möglich, der eine fast exakte Kopie des Originalmodells erstellt.

Die missbräuchliche Entwendung des geistigen Eigentums ist nicht die einzige Bedrohung, die diese Art von Angriff mit sich bringen kann, auch weiterführende Angriffe, die ein Modell in der korrekten Funktionsweise stören sollen, wie z. B. die Erstellung sogenannter „Adversarial Examples", werden damit ermöglicht.

ENTDECKEN UND VERHINDERN VOR DIEBSTAHL

Ein effektiver Diebstahl des Modells kann die gesamte Arbeit an der Entwicklung von ML-Lösungen zunichtemachen. Daher müssen entsprechende Gegenmaßnahmen entwickelt werden. Einer der bekanntesten Ansätze zum Schutz vor unbefugter Weitergabe ist allgemein das Einfügen eines Wasserzeichens. Bei Wasserzeichen für ML-Modelle werden eigentümerspezifische Informationen in ein Modell eingebettet, so dass der*die Eigentümer*in des Modells überprüfbar wird [3]. Dieser Mechanismus kann jedoch nur als Indiz fungieren, dass ein Modell gestohlen wurde - aber den Diebstahl selbst nicht verhindern.

Eine andere Möglichkeit, den Modelldiebstahl aufzudecken, besteht darin, das Nutzerverhalten bzw. die an das Originalmodell gesendeten Daten zu überwachen. Wenn jemand einen Angriff ausführen will, unterscheiden sich in der Regel bösartige Abfragen von gutartigen. Ähnlich wie bei Wasserzeichen können solche Monitore nicht komplett verhindern, dass Modelle gestohlen werden, sondern nur über einen laufenden Angriff informieren.

Um den Diebstahl eines Modells zu verhindern oder zu erschweren, kann entweder das ursprüngliche Modell oder seine Antworten verändern werden, indem beispielsweise Rauschen zu den Ergebnissen hinzugefügt wird, so dass diese weniger Informationen über das Modell preisgeben. Wie in vielen sicherheitsrelevanten Bereichen muss ein Kompromiss zwischen dem dadurch geringeren Nutzen und der Sicherheit des Modells gefunden werden.

Der Schutz des geistigen Eigentums beim maschinellen Lernen hat in den letzten Jahren an Aufmerksamkeit gewonnen und ist ein schnell wachsendes Forschungsgebiet - gleichzeitig entsteht ein Wettbewerb zwischen Angriff und Verteidigung. Die Forschung ist jedoch noch recht unvollständig und fragmentiert, wobei es keine universelle Verteidigung gibt, die gegen jede Art von Angriffen schützt.

Referenzen:

[1] Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart. Stealing Machine Learning Models via Prediction APIs. USENIX Security 2016.

[2] Daryna Oliynyk, Rudolf Mayer and Andreas Rauber. I Know What You Trained Last Summer: A Survey on Stealing Machine Learning Models and Defences. ACM Computing Surveys, 2023.

[3] Isabell Lederer, Rudolf Mayer and Andreas Rauber. Identifying Appropriate Intellectual Property Protection Mechanisms for Machine Learning Models: A Systematisation of Watermarking, Fingerprinting, Model Access, and Attacks. IEEE Transactions on Neural Networks, 2023.

Daryna Oliynyk
Forscherin in der Machine Learning and Data Management Group bei SBA Research. Ihre Forschungsinteressen sind Sicherheit und Privacy in Maschinellem Lernen mit Schwerpunkt auf dem Schutz des geistigen Eigentums.

Gabriele Kotsis im Gespräch mit Katharina Resch-Schobel

Mit Neugier und Leidenschaft zum Erfolg

Sie haben Informatik studiert, sich habilitiert und eine Karriere im wissenschaftlichen und akademischen Umfeld gemacht. Schon 1992 haben Sie den Förderpreis für Ihre Arbeit „Interconnection Topologies and Touting for Parallel Processing Systems" bekommen und Ihre Doktorarbeit wurde 1996 mit dem Zemanek-Preis prämiert.

Heute sind Sie als Informatikprofessorin in Forschung und Lehre an der JKU Linz tätig. Neben vielen anderen interessanten Aufgaben waren Sie auch von 2020 bis 2022 Präsidentin der weltweit größten Informatikgesellschaft, der Association for Computing Machinery.

In all diesen Jahren haben Sie den Nachwuchs in der IT-Forschung vielfältig gefördert und engagieren sich auch schon seit vielen Jahren in der OCG in zahlreichen Jurys für Nachwuchswissenschaftspreise.

Katharina Resch-Schobel: *. Die OCG Preise werden für wissenschaftliche Leistungen, d. h. Forschungsarbeiten, vergeben. Was hat bei Ihnen die Lust auf IT und Forschung geweckt?*

Gabriele Kotsis: Ich fürchte, ich bin schon seit meiner frühen Kindheit sehr neugierig, oder positiv ausgedrückt, wissbegierig. Dabei interessieren mich vor allem Fragen nach dem „Warum", das ist wohl eine gute Ausgangslage für eine wissenschaftliche Karriere. Für meine Masterarbeit hatte ich zuerst eine Programmieraufgabe gewählt, aber dann gewechselt zu einer mehr forschungsaffinen Fragestellung, der ich mich dann mit Begeisterung gestellt habe. Wirklich entfacht wurde mein Ehrgeiz und meine Leidenschaft für die Forschung dann durch sehr kritische, aber konstruktive Kommentare meines Betreuers während der Arbeit. Belohnt wurden die „Mühen" dann mit dem OCG Förderpreis und diese Anerkennung war dann wohl der richtige Startschuss für meine wissenschaftliche Karriere.

Mit welchen Schwierigkeiten hatten Sie in Ihrer Forscherinnenlaufbahn zu kämpfen – haben diese Schwierigkeiten bzw. Hindernisse sich über die Jahre verändert?

Nach Abschluss meines Studiums musste ich mich entscheiden zwischen einem finanziell sicher lukrativeren Job in der IT-Branche oder einer Tätigkeit als Universitätsassistentin mit dem Ziel einmal eine Professur zu erlangen. Dieses Ziel war schon damals nicht leicht zu erreichen, ist heute aber nochmals in vielerlei Hinsicht schwieriger geworden. Ich kann daher gut nachvollziehen, dass junge Menschen heute den Schritt in die Wirtschaft einer unsicheren und zum Teil prekären Situation an einer Universität vorziehen. Hier besteht dringender Handlungsbedarf, wenn wir weiterhin starke Forschung im Informatik-Bereich in Österreich haben wollen.

*Können Sie jungen Forscher*innen Tipps geben, wie sie durchhalten können, Hindernisse überwinden könnten und damit dann auch erfolgreich ihre Ideen in der Wissenschaftscommunity durchsetzen können?*

Ich persönlich habe immer sehr viel Kraft und Motivation aus der Weitergabe von Wissen an der Universität - also aus der Lehrtätigkeit - gewonnen. Es ist so lohnend, jemandem etwas so erklären zu können, dass Inhalte nicht nur (auswendig) gelernt, sondern auch verstanden werden und man Interesse wecken und neue Ideen hervorbringen kann. Ich lese auch gerade ein Buch, in dem die eigentliche Stärke des Menschen als Individuum, aber auch der Menschheit insgesamt, in der Fähigkeit gesehen wird, zu kooperieren. Das ist auch in der Wissenschaft ein Erfolgsrezept. Es gibt natürlich noch immer die genialen Einzelkämpfer, aber sicherer scheint mir der Weg im Team zu arbeiten. Daher mein Tipp für junge Forscher*innen: Vernetzt euch mit anderen! Das müssen nicht unbedingt immer fachlich nahestehende Personen sein, gerade auch durch Diversität und unterschiedliche Blickpunkte auf Themen entstehen die spannendsten Ideen, die euch helfen und weiterbringen werden!

War internationale Vernetzung von Anfang an ein Thema bei der Forschung?

Forschung sollte keine regionalen oder nationalen Grenzen kennen! Gesellschaftliche oder politische Umstände erschweren zwar manchmal internationale Kooperationen, aber die Vernetzung der Wissenschafter*innen ist – ganz im Sinne meiner vorigen Ausführungen – grundlegend für eine erfolgreiche Weiterentwicklung.

*Was bedeutet für Sie die Arbeit mit jungen Nachwuchsforscher*innen und im speziellen auch die Bewertung von Arbeiten in einer Preis-Jury?*

Die Erstellung einer erfolgreichen Masterarbeit erfordert eine an- und ausdauernde Beschäftigung mit dem Thema und somit auch eine gewisse Leidenschaft

dafür. Somit sind die Einreichungen ein guter Spiegel dafür, welche Themen für junge Menschen interessant sind. Die Einreichungen zeigen aber auch immer eindrucksvoll die Breite der Bereiche, in denen Informatik mittlerweile eine Schlüsseltechnologie geworden ist. Es ist schön, hier zu sehen, welche wertvollen Beiträge bereits in Masterarbeiten an österreichischen Universitäten geliefert werden, z. B. zum Thema IT-Sicherheit oder im Bereich der medizinischen Diagnostik mittels Machine Learning,

Nach welchen Gesichtspunkten entscheiden Sie, welche Arbeit, die Beste ist?

Alle Arbeiten, die eingereicht werden, sind bereits mit „Sehr gut" beurteilt. Die Jury hat also die schwierige Aufgabe, unter den sehr guten die beste(n) Arbeiten zu finden. Unsere Kriterien umfassen neben der wissenschaftlichen Relevanz und Methodik sowie der Qualität der Präsentation der Arbeit auch die Aktualität des Themas, die Anwendbarkeit der gewonnenen Erkenntnisse und die Originalität in der Bearbeitung. Eine gewisse subjektive Komponente lässt sich aber nie ganz vermeiden, deshalb entscheidet ja auch nicht eine Einzelperson, sondern ein Gremium. In einer ersten Runde bewerten die Jurymitglieder einzeln für sich die Arbeiten, dann werden die Einzelmeinungen in einer Diskussion zu einer kollektiven Bewertung verdichtet und - falls nötig - noch durch externe Gutachten ergänzt. Dieser Prozess hat sich in den letzten Jahren bewährt, sodass wir die endgültigen Entscheidungen eigentlich immer einstimmig fassen konnten. Und wir hoffen, mit den Auszeichnungen auch Impulse für zukünftige Karrieren in der Forschung – so wie es bei mir selbst der Fall war – anstoßen zu können.

Univ. Prof.in Dr.in **Gabriele Kotsis** ist Leiterin des Instituts für Telekooperation an der Johannes Kepler Universität Linz, OCG Vorstandsmitglied und ehemalige Präsidentin der OCG. sowie der weltgrößten Computer Gesellschaft ACM.

Die OCG Preise für IT-Nachwuchs

OCG Förderpreise

Die Österreichische Computer Gesellschaft (OCG) verleiht zur Förderung der Informatik und Wirtschaftsinformatik jährlich den OCG Förderpreis sowie den OCG Förderpreis-FH für hervorragende Master- und Diplomarbeiten auf dem Gebiet der Informatik, Wirtschaftsinformatik und ihren Anwendungen. Eine Jury wählt unter den eingereichten Arbeiten aus. Die Preise sind jeweils mit Euro 2.000,- dotiert.

Juryvorsitz OCG Förderpreis: Prof. Dr. Gabriele Kotsis (JKU Linz)

Juryvorsitz OCG Förderpreis-FH: FH-Prof. Mag. Dr. Johannes Lüthi (FH Kufstein)

Heinz Zemanek Preis

Die OCG verleiht zur Förderung der Informatik alle zwei Jahre den Heinz Zemanek Preis für hervorragende Dissertationen auf dem Gebiet der Informatik.

Universitäten und Forschungsstätten, die das Promotionsrecht in den oben genannten Bereichen haben, dürfen bis zu zwei ihrer ausgezeichneten Studierenden nominieren. Der Preis ist mit Euro 5.000,- dotiert.

Juryvorsitz: Prof. Dr. Stefan Szeider (TU Wien)

Kooperationen

Die OCG unterstützt auch Preise, die andere Organisationen im Bereich Informations- und Kommunikationstechnologie (IKT) vergeben:

- GI Dissertationspreis
- Helmut und Heide Balzert-Preis
- Adolf-Adam-Informatikpreis

Der GI Dissertationspreis der deutschen Gesellschaft für Informatik ist ein Preis für herausragende Informatik-Dissertationen.

Der Balzert-Preis zeichnet Leistungen im Bereich der Informatik-Didaktik aus.

Um den Adolf-Adam-Preis der JKU zu erhalten, müssen Studierende ihre ausgezeichneten Arbeiten Schüler*innen präsentieren, die für die am besten erklärte Arbeit voten.

von Fabio Francisco Oberweger

Unterstützung durch Machine Learning

Das Staff Rerostering Problem (SRRP) ist ein kombinatorisches Zeitplanungsproblem, das sich mit der Anpassung von Arbeitsplänen an unvorhergesehene Ereignisse wie Krankenständen oder anderen kurzfristigen Änderungen im Personalbedarf befasst. Insbesondere in Zeiten von Gesundheitskrisen wie der Covid-19-Pandemie ist das SRRP von großer Bedeutung. Das Ziel des SRRPs ist es, einen neuen Arbeitsplan unter Berücksichtigung dieser Störungen zu erstellen. Dabei sollte der neue Arbeitsplan alle arbeitsrechtlichen Regelungen erfüllen und so wenige Änderungen wie möglich am ursprünglichen Plan vornehmen.

In diesem Beitrag stelle ich eine Large Neighborhood Search (LNS) vor, um das SRRP effizient zu lösen. Das besondere an der verwendeten LNS ist, dass sie mit Machine Learning (ML) erweitert wurde. Traditionell besteht eine LNS aus sich wiederholenden Anwendungen einer Zerstör- und einer Reparaturmethode. Dabei wird in der Zerstörmethode eine Teilmenge der Entscheidungsvariablen eines Problems freigesetzt und die anderen auf ihre aktuellen Werten fixiert. Zum Beispiel: Für Person 1 wird die zugeordnete Schicht an Tag 5 aus dem Arbeitsplan genommen, die Person kann an diesem Tag nun einer neuen Schicht zugeordnet werden. Das Freisetzen mehrerer Entscheidungsvariablen erzeugt ein Teilproblem. Durch das genaue oder heuristische Lösen dieses Teilproblems mit der Reparaturmethode versucht die LNS die vorherige Lösung zu verbessern, indem es bessere Zuweisungen für diese „zerstörten" Variablen findet. Wenn eine neue Lösung mit einem besseren Zielwert als die vorherige gefunden wird, ist dies der Ausgangspunkt für die nächste Wiederholung. Dieser Prozess wird durchgeführt, bis ein Stoppkriterium, wie zum Beispiel ein Zeitlimit, erreicht ist.

MUSTER MIT LERNBASIERTEN TECHNIKEN ENTDECKEN

Die Teilprobleme, die durch die Zerstörmethode erzeugt werden, können effizient durch genaue Methoden gelöst werden. Das verwendete LNS-Verfahren nutzt ein gemischt-ganzzahliges lineares Programm (MILP), das mit dem Gurobi-Löser als Reparaturmethode gelöst wird. Die größere Herausforderung ist jedoch das Design der Zerstörmethode. Standard-Methoden für Zerstörungs-Operatoren sind oft problem-spezifische heuristische Verfahren, die zeitaufwändig zu entwickeln sind, aber keine Erfolgsgarantien bieten. In jüngster Zeit wurden lernbasierte Techniken angewendet, um Muster zu entdecken, die nur schwer von Hand zu finden sind. Diese Strategien reduzieren oder eliminieren sogar den Bedarf, Heuristiken manuell zu konstruieren und haben das Potenzial, Verbindungen aufzudecken, die Menschen nicht einfach sehen können. (Siehe Abb. 1)

Der Hauptbeitrag des vorgestellten Algorithmus ist daher eine ML-basierte Zerstörmethode. Es wird ein neuronales

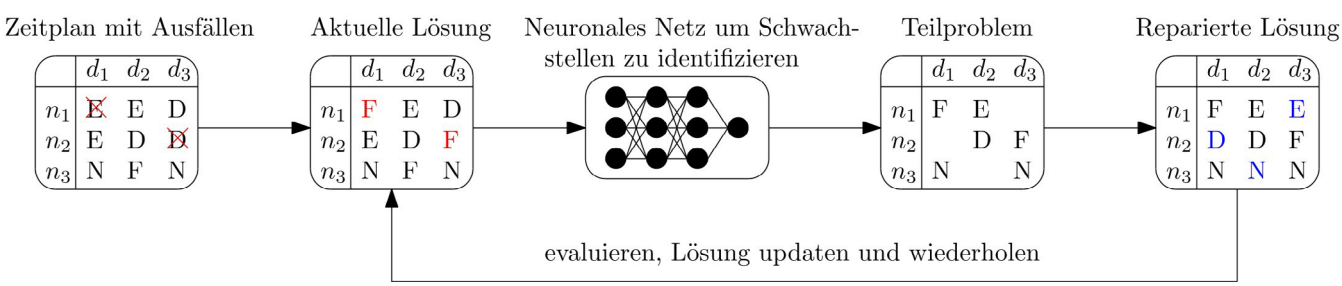


Abb. 1: Im ersten Schritt erzeugen wir eine Lösung, indem wir die Schichten für die Personen an den Tagen einfach auf die freie Schicht setzen. Danach wenden wir das neuronale Netz an, um die Schwachstellen in der aktuellen Lösung zu identifizieren. Die Schwachstellen werden dann gelöscht und wir bekommen das Teilproblem. Dieses Lösen wir dann und versuchen dabei, unseren gesamten Plan zu verbessern. Wir evaluieren die neue Lösung, nehmen sie als neue aktuelle Lösung (wenn sie besser ist) und wiederholen den Prozess.

Netz trainiert, das eine Wahrscheinlichkeitsverteilung lernt. Diese Verteilung gibt an, welche Variablen „zerstört" werden sollten. Dieses neuronale Netz ist ein Graph Neural Network (GNN), das als Eingabe einen Graphen verwendet, der eine SRRP-Instanz modelliert. Um diesem Netz beizubringen, wo die Schwachstellen in einem aktuellen Arbeitsplan liegen, wird Imitation Learning (Lernen durch Nachahmung) angewandt. Hierzu hilft ein MILP, das optimale Zerstörmengen berechnen kann. Dieses benötigt aber zu viel Zeit, um in tatsächlichen Anwendungen verwendet zu werden. Daher wird dieses nur im Vorhinein benutzt, um Trainingsdaten zu generieren und das verwendete Netz damit zu trainieren. Nachdem das Netz trainiert wurde, kann es in der Zerstörmethode verwendet werden, um schlechte Schichtzuweisungen zu identifizieren.

In den durchgeführten Experimenten konnte gezeigt werden, dass dieser Ansatz klassische, manuell-angefertigte Zerstörmethoden übertreffen konnte.

BEGEISTERUNG UND FÜR DIE FORSCHUNG

Im Zuge meines Masterstudiums an der TU Wien konnte ich an einer echten Forschungsproblemstellung und einer Publikation mitarbeiten. Durch das „Seminar in Algorithmics", in dem ich eine Literaturrecherche über Machine Learning in der kombinatorischen Optimierung schrieb, wurde ich dann auf die Forschung von Prof. Raidl aufmerksam.

So durfte ich dann diesen Algorithmus im Rahmen meiner Diplomarbeit in der Algorithms and Complexity Gruppe am Insitute of Logic and Computation der TU Wien entwickeln.

An dieser Stelle möchte ich gerne meinen Betreuern Prof. Günther Raidl und Marc Huber von der Algorithms and Complexity Group der TU Wien sowie meiner internationalen Betreuerin Prof. Elina Rönnberg, Linköping University in Schweden, meinen herzlichen Dank aussprechen. Durch die wöchentlichen Meetings, an denen ich meine neuen Ideen vorstellen und das Feedback meiner Betreuer*innen bekommen habe, konnte ich die Qualität der entwickelten Methode so verbessern, dass wir sie zusätzlich noch in einem Paper bei der CPAIOR 2022 Konferenz veröffentlichen konnten.

Trotz des Angebots die Forschung an meiner Diplomarbeit im Rahmen einer PhD-Stelle an der TU Wien fortzusetzen, entschloss ich mich einen anderen Weg zu gehen, da ich noch mehr über verschiedene Machine Learning Anwendungsbereiche und Algorithmen lernen wollte. Im Februar 2022 schloss ich mich daher dem Competence Unit „Assistive & Autonomous Systems" des Austrian Institute of Technology (AIT) an, wo angewandte Forschung betrieben wird. Mein Bereich ist dabei die Entwicklung, das Training und Deployment von Machine Learning Algorithmen für die Umgebungswahrnehmung auf verschiedenen Modalitäten.

DI **Fabio Francisco Oberweger** ist Junior Research Engineer in der Unit „Assistive & Autonomous Systems" im Center für „Vision, Automation & Control" am Austrian Institute of Technology (AIT). Er beschäftigt sich mit der Forschung und Entwicklung von Machine Learning Komponenten für die visuelle Umfeldwahrnehmung von robotischen Systemen.

von Theresa Neubauer

Multimodale Bildanalyse mit Deep Learning

In meiner Mastarbeit „Volumetric Tumor Segmentation on Multimodal Medical Images using Deep Learning“ wurden Algorithmen für die Erkennung von Tumoren auf verschiedenen radiologischen Bildern – wie Röntgen, MRT usw. – entwickelt.

Die derzeit modernste Technologie für die Bildanalyse ist Deep Learning. Hierbei handelt es sich um neuronale Netzwerke aus dem Bereich der Künstlichen Intelligenz. Auch im Bereich der biomedizinischen Bildsegmentierung kamen neuronale Netzwerke in den letzten Jahren verstärkt zum Einsatz, um Tumore und Anomalien auf radiologischen Bildern besser erkennen zu können. Allerdings gab es bis jetzt wenig Forschung darüber, wie verschiedene Bildmodalitäten beim Deep Learning bestmöglich kombiniert werden können, um das Ergebnis der Segmentierung zu verbessern.

EIN PATIENT, VIELE BILDER

Auf dem Weg zur richtigen Diagnose bei Tumorerkrankungen, etwa bei Weichteiltumoren, kommen medizinischen Scans eine besondere Bedeutung zu. Dafür analysiert medizinisches Fachpersonal visuell den Tumor auf MR-, CT- und PET-Scans – sogenannten multimodalen Bildern. Diese Bildaufnahmen nehmen dabei den Tumor in unterschiedlichen anatomischen, funktionalen und molekularen Kontexten auf und liefern somit auch verschiedene Informationen über den Tumor. Denn je nach klinischer Fragestellung – Geht es beispielsweise um die Biopsie, die Radiotherapie oder die Operationsplanung? – sind verschiedene Aspekte und Aufnahmen relevant. Die Segmentierung von Tumoren war bislang eine manuelle und zeitaufwändige Arbeit, die viel Aufmerksamkeit der Radiologinnen und Radiologen in Anspruch nimmt. Automatisierte Werkzeuge können hierbei eine wertvolle Ergänzung im klinischen Alltag sein.

ALGORITHMUS ZUR MULTIMODALEN TUMORSEGMENTIERUNG

Bisher wurde das Potenzial multimodaler Daten nur von wenigen etablierten computergestützten Bild-Segmentierungsmethoden genutzt. Im Zuge meiner Di-

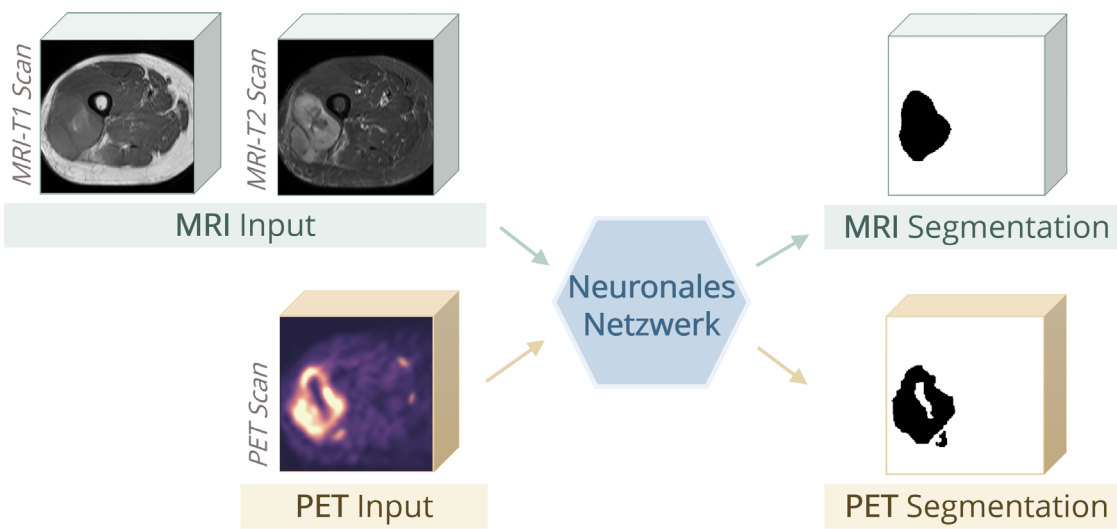


Abb. 1: Deep Learning kombiniert Daten aus MR-, CT- und PET-Bildern für eine präzisere Tumorsegmentierung. © Theresa Neubauer, Cancer Imaging Archive

plomarbeit habe ich einen innovativen Bildsegmentierungs-Algorithmus entwickelt, der es ermöglicht, komplexe multimodale Bild-Merkmale zu lernen und somit effizient mehrere Tumorsegmentierungen auf unterschiedlichen Bildmodalitäten vorhersagen zu können.

FORSCHUNG FÜR DIE PRAXIS

Meine Masterarbeit ist in Kooperation mit dem Forschungszentrum VRVis, der TU Wien und der MedUni Wien entstanden. Als Teil der Biomedical Image Informatics-Forschungsgruppe des VRVis erarbeitete ich meine Bildsegmentierungs-Pipeline in direktem Kontakt mit medizinischen Fachleuten. Durch die Zusammenarbeit mit Expert:innen aus verschiedenen Praxisfeldern ist es möglich, auch bereits im Rahmen einer Diplomarbeit Lösungen für reale Probleme und drängende Fragestellungen zu entwickeln, die zu einem tatsächlichen Mehrwert in der Praxis beitragen.

THERESA NEUBAUER IM GESPRÄCH MIT DER OCG:

Was bedeutet der OCG Förderpreis für Sie?

Das Forschungsumfeld ist sehr kompetitiv und die Suche nach einer innovativen Lösung kann oft lang dauern und auch zwischendurch frustrierend sein. Umso schöner ist es, wenn man durch einen Preis wie dem OCG-Förderpreis Anerkennung für seine Arbeit erhält. Und natürlich ist die Auszeichnung für die eigene Leistung auch immer ein guter Antrieb, weiterzuforschen und nicht aufzugeben.

Wie sieht Ihr Weg durch die Informatik aus?

Ich bin eigentlich eher zufällig zur Informatik gekommen. Ich habe mich mit 14 Jahren für die HTL mit Schwerpunkt Informatik entschieden, da ich mich für Mathematik und Logik interessiert habe. Nach meiner HTL-Matura zog ich nach Wien, um Softwareentwicklerin zu werden, was ich auch rund sechs Jahre in zwei großen Unternehmen gemacht habe. Parallel dazu habe ich berufsbegleitend Wirtschaftsinformatik studiert und schließlich 2020 meinen Master in Medizinischer Informatik an der TU Wien abgeschlossen. Auch nach dem Abschluss meiner Diplomarbeit 2020 bin ich am VRVis geblieben, wo ich als Forscherin für AI und Visual Computing tätig bin. Ich beschäftige mich weiterhin mit Algorithmen für die Bildanalyse in verschiedensten Anwendungsfeldern.

Was begeistert Sie an der Forschung?

Für mich steht bei Forschung der Gedanke zu forschen, um innovative Konzepte zur Lösung wirklicher Probleme zu entwickeln an erster Stelle. Zugleich begeistert es mich, dass gute Forschung immer auch eine große Portion Kreativität erfordert. Fragen, die vorher noch niemand beantwortet hat, die Freiheit selber die Methoden zu entwickeln, eigene Lösungswege auszuprobieren und immer neugierig zu bleiben, haben mich während meiner Diplomarbeit am VRVis begeistert – und tun es bis heute.

Was würden Sie dem Forschungsnachwuchs gerne mit auf dem Weg geben?

In der Schule wird Informatik manchmal trocken und theoretisch vermittelt, aber meiner Meinung nach ist Informatik das Gegenteil: anwendungsorientiert und kreativ. Das Schöne an Informatik ist, dass man mehr oder weniger nur einen Computer braucht, um seine Ideen umzusetzen. Das Wichtigste im Studium und in der Forschung ist, dass man Spaß und eine gewisse Begeisterung hat, für das, womit man sich beschäftigt. Zugleich muss man natürlich nicht das gesamte Studium gut finden, es reicht aus, wenn man sich für einen Teilbereich interessiert. Im Job spezialisiert man sich ja auch. Auch vor großen Herausforderungen sollte man sich nicht gleich abschrecken lassen, sondern einfach ausprobieren, wie weit man es schafft. Es wäre ja auch langweilig, wenn man schon im Vorhinein weiß, dass man alles schaffen kann, was man sich vornimmt.

Theresa Neubauer hat an der TU Wien ihr Master-Studium Medizinische Informatik abgeschlossen. Seit 2020 ist sie Forscherin am VRVis in Wien und entwickelt KI-Algorithmen für die Bildanalyse für den medizinischen und industriellen Bereich.

Blockchain-Forensik

von Martin Plattner

Neuartiges Address-Clustering-Verfahren

Die Analyse von Finanztransaktionen mittels Kryptowährungen stellt Behörden vor große Herausforderungen. Begegnet wird diesem Problem mit neuen Analyseverfahren wie etwa dem Blockchain-übergreifenden Address-Clustering-Verfahren, welches ich im Rahmen meiner Masterarbeit entwickelt habe. Dazu habe ich die an der Universität Princeton entwickelte Blockchain-Analyseplattform BlockSci um einen Multi-Chain-Modus erweitert, um das Analysieren von Daten über mehrere Blockchains hinweg zu ermöglichen.

Im Jahr 2009 ist die erste - und nach wie vor bekannteste - Kryptowährung, der Bitcoin, entstanden. Erste Berührungspunkte mit dem dahinterliegenden Konzept der Blockchain hatte ich 2015 bei einem Auslandssemester im Rahmen meines Informatikstudiums in Stockholm. Ein richtiges Interesse am Bitcoin ist jedoch erst 2017 entstanden, als der Wert und die Popularität der Kryptowährung auch außerhalb der Tech-Szene rasant zugenommen haben. Zu diesem Zeitpunkt war ich Masterstudent an der Universität Innsbruck. Ich habe mehrere Kurse bei Univ.-Prof. Rainer Böhme belegt, in denen immer wieder auch Kryptowährungen behandelt wurden. Dieses Thema hat mich schnell vereinnahmt. Schließlich wurde ich Teil der internationalen Arbeitsgruppe von Rainer Böhme, dem Security and Privacy Lab, und habe dort auch meine Masterarbeit verfasst.

DAS PROBLEM

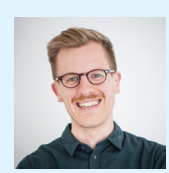
Öffentliche Blockchains wie Bitcoin beinhalten mehrere hundert Millionen Finanztransaktionen. Die Analyse dieser Transaktionen ist von erheblichem Interesse für die Forschung und für künftige kommerzielle Anwendungen, aber insbesondere auch für Behörden, da Blockchain-Systeme aufgrund ihrer Pseudonymität häufig für kriminelle Zahlungen benutzt werden. Dabei kommt erschwerend hinzu, dass User innerhalb dieser Systeme beliebig viele „Konten“ in Form von Adressen erstellen können, um Zahlungsflüsse zu verschleiern. Eine etablierte forensische Methode ist das sogenannte Address-Clustering, das mittels Heuristiken die Adressen pro User gruppiert, um deren Aktivitäten gesondert zu betrachten. Bisherige Methoden analysierten jedoch nur einzelne Blockchains für sich in sogenannten Single-Chain-Analysen.

DIE LÖSUNG

In meiner Masterarbeit habe ich die Analyse-Software BlockSci um einen Multi-Chain-Modus erweitert. Dieser ermöglicht das Analysieren von Daten mehrerer Blockchains gemeinsam in neuartigen Cross-Chain-Analysen. Dafür eignen sich besonders sogenannte Blockchain-Forks, d. h. Abspaltungen von bestehenden Blockchains, da diese aufgrund ihrer gemeinsamen Transaktionshistorie zwischen Eltern- und Fork-Chain viele Verbindungen aufweisen. Ein populäres Beispiel für einen Fork ist Bitcoin Cash, das sich im August 2017 von der Bitcoin Blockchain abgespalten hat. Durch eine Cross-Chain-Analyse beider Blockchains lassen sich neue Erkenntnisse gewinnen, etwa wie sich das Userverhalten zwischen Chains unterscheidet. Der neue Multi-Chain-Modus ermöglichte mir die Implementierung eines neuartigen Clustering-Verfahrens – dem Cross-Chain-Address-Clustering. Dabei werden die Aktivitäten von Usern über mehrere geforkte Chains hinweg kombiniert, um die Qualität des Clusterings zu verbessern.

DAS ERGEBNIS

Dieses neue Verfahren konnte ich schließlich auf Bitcoin und Bitcoin Cash anwenden und bis Dezember 2019 über 570.000 zusätzliche Cluster-Zusammenschlüsse identifizieren. Insgesamt waren davon über 30 Millionen Adressen betroffen. Die Implementierung ist flexibel gestaltet, sodass das Verfahren in Zukunft auch auf andere Blockchain-Systeme anwendbar ist. Dieses von mir entwickelte Cross-Chain-Address-Clustering konnte ich zusammen mit Forschern der Universitäten Princeton, Johns Hopkins sowie Cornell Tech erfolgreich bei der renommierten Konferenz USENIX Security 2020 zur Veröffentlichung einreichen. Zusätzlich ist die Integration meines Verfahrens in die am Austrian Insitute of Technology und Complexity Science Hub entwickelte Blockchain-Forensiksoftware GraphSense geplant, welche seit 2021 vom Spin-off Iknaio Cryptoasset Analytics als operatives Service angeboten wird. Ich hoffe damit einen wichtigen Beitrag zur effektiven Strafverfolgung innerhalb dieser immer populärer werdenden Systeme zu leisten.



Martin Plattner hat an den Universitäten Wien, Innsbruck und Stockholm Informatik studiert. Beruflich ist er im Bereich der Informationssicherheit tätig. Plattners Masterarbeit wurde 2022 als erste Arbeit der Universität Innsbruck mit dem OCG Förderpreis ausgezeichnet

MiniJava-Compiler für WebAssembly auf Basis von ANTLR und Kotlin

von Stefan Schöberl

MiniJava-Compiler

WebAssembly ist eine neue Technologie, die durch das World Wide Web Consortium (W3C) vorangetrieben wird und verspricht schnellere Ladezeiten sowie bessere Performanz im Web als beispielsweise JavaScript. Um dieses Potenzial Webentwickler*innen zugänglich zu machen, benötigt es Werkzeuge, die für bestehende Programmiersprachen WebAssembly-Bytecode erzeugen können. So können bestehende Programmiersprachen ohne Transpiler für Web-Anwendungen eingesetzt werden.

Das Ausführungsmodell von WebAssembly basiert dabei auf einer virtuellen Kellermaschine. Die Idee, eine virtuelle Kellermaschine mit eigenem Bytecode im Browser einzusetzen ist nicht neu, denn bereits Java Applets verfolgten auf Basis der Java Virtual Machine (JVM) einen vergleichbaren Ansatz. Diese gelten allerdings mittlerweile als veraltet und werden in modernen Browsern auch nicht mehr unterstützt.

Die Verwendung einiger Programmiersprachen (z. B. C/C++ oder Rust) und Frameworks (z. B. Blazor in Kombination mit C#) im Browser über WebAssembly ist bereits möglich, jedoch sind (meist) einige Anpassungen dafür im Quellcode notwendig, die Rückschlüsse auf WebAssembly geben. Besonders praktisch wäre es jedoch, wenn möglichst keine Anpassungen notwendig wären, das macht das Portieren von bestehender Software einfacher.

Das war die Motivation, einen alternativen Ansatz zu untersuchen, eine (bestehende) Programmiersprache über WebAssembly ins Web zu bringen. Dabei soll der Quellcode keine Hinweise darauf enthalten, dass dieser schlussendlich nach dem Kompilieren zur Laufzeit mit WebAssembly interagiert. Dieser Ansatz wurde anhand der Programmiersprache MiniJava, einer selbst definierten Teilmenge der Sprache Java, praktisch umgesetzt und evaluiert, indem ein Compiler für MiniJava implementiert wurde. Der Compiler wurde in Kotlin implementiert und der Scanner und Parser wurden mit ANTLR 4.8 generiert. Kotlin wurde aufgrund persönlicher Erfahrung und einiger Sprachfunktionalitäten, eleganten und robusten Code schreiben zu können, gewählt. Der Fokus bei der Implementierung lag auf dem Abbilden typischer Sprachkonstrukte (z. B. Variablen, Methoden, Verzweigungen und Schleifen) und dem Entwurf einer Schnittstelle zum Browser, sodass auch grafische Oberflächen mit MiniJava implementiert werden können. Eine Besonderheit dabei ist, dass dabei direkt auf JavaScript-Objekte im Browser zugegriffen wird, ohne dass dies im MiniJava-Quellcode sichtbar ist. Die praktische Anwendung des geschaffenen Compilers wurde anhand einer Demo-Anwendung im Browser, einem Fibonacci-Rechner, demonstriert.

FASZINATION FORSCHUNG

Compiler und die Hintergründe von Programmiersprachen faszinieren mich schon seit langer Zeit und gehören zu meinen Lieblingsthemen der Informatik. Mein Interesse wurde unter anderem durch Lehrveranstaltungen im Bachelor und Masterstudium Software Engineering am Campus Hagenberg der FH OÖ vertieft. Mit meiner Masterarbeit sah ich eine Chance, mich noch mehr mit diesem Thema anhand eines praktischen Anwendungsfalles auseinanderzusetzen.

Derzeit bin ich am Software Competence Center Hagenberg (SCCH) als Researcher und Senior Software Engineer tätig, wo ich mich im Bereich Software Science mit Themen rund um Software-Architektur sowie die Analyse von Software und Quellcode auseinandersetze. Zuvor konnte ich während meines Studiums praktische Erfahrungen in großen Softwareprojekten bei der Firma Catalysts (mittlerweile als Cloudflight bekannt) sammeln. Weiters unterrichte ich ebenfalls als nebenberuflich Lehrender am Campus Hagenberg der FH OÖ, wo ich in verschiedenen Lehrveranstaltungen mein Wissen weitergeben kann. Außerdem strebe ich derzeit ein Doktorat in Informatik an.

Link zur Masterarbeit: https://schoeberl.dev/projects/masters-thesis

Linz zur Webseite: https://schoeberl.dev

Stefan Schöberl, MSc ist als Researcher und Senior Software Engineer am Software Competence Center Hagenberg (SCCH) und als nebenberuflich Lehrender am Campus Hagenberg der FH OÖ tätig, an dem er ebenfalls Software Engineering studiert hat.

Wohl der Gesellschaft

von Benedikt Berger

Das Web sicher, effizient einsetzen

Die Technologie Blockchain (dt. Blockkette) hat in den letzten Jahren vermehrt Aufmerksamkeit auf sich gezogen und die Verbreitung dieser Technologie soll über die kommenden Jahre signifikant wachsen. Blockchain wird mit dem Begriff „Web3" verbunden, es soll also die dritte Entwicklungsstufe des Internets sein und das Web um die Möglichkeit erweitern, Besitz digital darzustellen.

Wenn es darum geht den Besitz eines Hauses, von Aktien oder ähnlichen wertvollen Dingen nachzuweisen, ist die Sicherheit, Manipulationsresistenz und Richtigkeit dieser Daten extrem wichtig. Um dies bestmöglich zu garantieren und Gefahren zu vermeiden, sind Blockchain Netzwerke von der restlichen herkömmlichen digitalen Infrastruktur abgeschottet – was die umsetzbaren Anwendungsfälle aber sehr einschränkt.

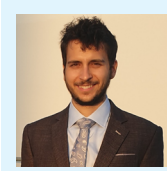
Um dies zu lösen, fungiert eine Komponente abseits des Netzwerks als Brücke zwischen den zwei Welten und schreibt Daten auf die Blockchain-Umgebung. Solch eine Komponente wird als „Oracle" (dt. Orakel) bezeichnet. Das Problem, wie ein Oracle die anfallenden Aufgaben und die Anforderungen erfüllen kann, ist als „the oracle problem" bekannt. Man könnte sich das auch so vorstellen: Unser derzeitiges Internet und alle dort vorhandenen Daten sind ein Kontinent, die Blockchain-Umgebung ist eine Insel mit meterhohen Mauern und das Oracle ist das Bindeglied zwischen Insel und Kontinent. Damit die Insel aber auch sicher bleibt, ist äußerste Sorgfalt dabei geboten welchem Oracle und dessen Daten vertraut werden kann und welchem nicht.

Oracles bringen eine Reihe von potenziellen Sicherheitslücken mit sich, welche in der Vergangenheit bereits öfters von Angreifern ausgenutzt wurden. Die Masterarbeit gibt eine Übersicht darüber, wie ein Oracle verwendet und wie diese Brücke zwischen Blockchain und der restlichen digitalen Infrastruktur am sichersten gestaltet werden kann. Es wird festgestellt, dass die Hauptmerkmale eines Oracles Ehrlichkeit, Sicherheit und Verfügbarkeit sind. Diese können durch verschiedene Ansätze erfüllt werden, welche genauer präsentiert werden. Der wichtigste Ansatz ist Verteilung, d. h. die Daten sollten von mehreren Datenlieferanten und von verschiedenen Quellen kommen. Zusätzlich wird die derzeitige Anwendung in der Industrie analysiert. Die Resultate dieser Analyse zeigen auf, dass die Angriffsflächen bei der Verwendung von Oracles noch kaum berücksichtigt werden.

EINFACHE UND SICHERE ANWENDUNG VON ORACLES

Weiters wird ein explorativer Prototyp implementiert, welcher die einfache und trotzdem sichere Anwendung von Oracles in der Entwicklung von Blockchain-Anwendungen ermöglicht. Als Beispiel wird hier der Anwendungsfall einer automatisierten Frostschutzversicherung umgesetzt. Obstbauern könnten, falls die Temperatur unter den Gefrierpunkt fällt, eine Anfrage zur Auszahlung stellen. Mehrere Oracles schreiben dann die Temperaturen, abgefragt von mehreren verschiedenen Wetterstationen, zum angefragten Zeitpunkt auf die Blockchain. Dort wird durch ein Programm der Durchschnitt aller Temperaturen errechnet und gegebenenfalls die Auszahlung der Versicherungssumme angestoßen. Der Prozess ist also vollautomatisiert und schwierig zu manipulieren, weil viele voneinander unabhängige Entitäten gleichzeitig für die Richtigkeit der Daten sorgen.

Es gibt jedoch einige Probleme im Bereich Blockchain, welche es zu lösen gilt, bevor die im Prototyp umgesetzte Architektur in einer Produktionsumgebung verwendet werden könnte. In der Arbeit werden Vorschläge für zukünftige Forschungsarbeiten in solchen Problembereichen gemacht.



Benedikt Berger, MSc, studierte an der FH Kufstein Web Communication & Information Systems. Seither spezialisierte er sich durch Zusatzdiplome im Bereich Blockchain weiter. Heute arbeitet er als Smart Contract und Fullstack Web Developer selbständig u. a. an verschiedenen Web3-Projekten.

Algorithmus der Cluster findet

von Stefan Neumann

Künstliche Intelligenz verstehen lernen

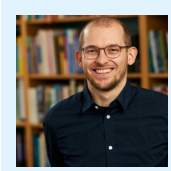
In den letzten Jahren gab es enorme Fortschritte in der Künstlichen Intelligenz (KI), die zu vollkommen neuen Einsatzbereichen geführt hat. Zum Beispiel waren automatisierte Chat-Bots wie ChatGPT oder Bild-generierende KI wie Dall-E noch vor wenigen Jahren nicht umsetzbar.

Die neuen Technologien unterscheiden sich allerdings stark von klassischen Algorithmen. Während wir früher Algorithmen entwickelten haben, die jederzeit eine korrekte Lösung ausgegeben haben, sind die neue Methoden darauf angewiesen, dass die Eingabedaten gewisse Gesetzmäßigkeiten (engl. patterns) enthalten. Als Beispiel für klassische Algorithmen kann man Dijkstras Algorithmus für kürzeste Wege betrachten: Egal welcher Graph die Eingabe ist, die Ausgabe ist immer der korrekte kürzeste Weg vom Start- zum Zielknoten. Im Gegensatz dazu kann die Ausgabe von modernen KI-Algorithmen beliebig falsch sein, wenn die Trainingsdaten keine Gesetzmäßigkeiten enthalten.

Diese Entwicklung stellt uns also vor eine neue Herausforderung: Um Algorithmen theoretisch zu erforschen, verwenden wir bisher weitgehend die Worst-Case-Analyse, die annimmt, dass die Daten keine Gesetzmäßigkeiten enthalten. Sie hilft uns also kaum, um den Erfolg von KI-Algorithmen zu erklären, und unser theoretisches Verständnis bleibt eingeschränkt. Gewissermaßen war der Fortschritt bei der Entwicklung von praktischen Algorithmen in den letzten Jahren so rasant, dass sich die Kluft zwischen dem, was praktisch möglich ist und unserem theoretischen Verständnis stark vergrößert hat.

Das Ziel meiner Dissertation war es, diese Kluft zu verringern. Dazu präsentierten wir Algorithmen, die beweisbar Gesetzmäßigkeiten in Daten finden und ausnutzen. Um den praktischen Erfolg der neuen Methoden theoretisch zu erklären, verwenden wir neue Analyse-Methoden, die die Gesetzmäßigkeiten in den Daten berücksichtigen und mathematisch modellieren.

Eines der Probleme, für die meine Dissertation neue Resultate geliefert hat, ist das Finden von Clustern in bipartiten Graphen. Dieses Problem muss etwa bei der Analyse von Online-Shopping-Daten gelöst werden, wo man Gruppen („Cluster“) von Produkten finden möchte, die häufig gemeinsam gekauft werden. In der Praxis war bekannt, dass diese Cluster oft winzig sind, zum Beispiel besteht ein mögliches Cluster aus den sieben Harry-Potter-Büchern, während Onlineshops Millionen Produkte verkaufen. Moderne KI-Algorithmen können diese winzigen Cluster erfolgreich finden, aber dies konnte bisher nicht theoretisch begründet werden. In meiner Dissertation präsentierte ich den ersten Algorithmus, der diese winzigen Cluster in Zufallsgraphen beweisbar findet. Dieses Resultat liefert also eine theoretische Begründung für den Erfolg von Algorithmen aus der Praxis. Außerdem half uns das neue theoretische Verständnis, einen besseren praktischen Algorithmus zu entwickeln, der deutlich skalierbarer als vorhandene Methoden ist. Der Algorithmus kann Eingaben mit mehreren Millionen Produkten auf einem MacBook verarbeiten und benötigt dafür weniger als eine Stunde; zudem ist es der erste Datenstromalgorithmus (”streaming algorithm”) für dieses Problem.



Stefan Neumann ist Assistenzprofessor an der Königlich Technischen Hochschule (KTH) in Stockholm, Schweden. Er erhielt sein Doktorat 2020 von der Universität Wien, wo er von Monika Henzinger betreut wurde. Seine Dissertation erhielt neben dem Heinz Zemanek Preis einen Award of Excellence vom Österreichischen Bildungsministerium.

von Daniela Kaufmann

Logik, Computeralgebra & Smart Contracts

Nach meinem Doktorat in Computer Science an der JKU Linz, meiner Forschungstätigkeit im Software Competence Center Hagenberg und dem LIT AI Lab an der JKU Linz, beschäftige ich mich heute als Postdoctoral Researcher am Institute of Logic and Computation der TU Wien mit angewandten formalen Methoden aus Logik und Computer Algebra.

Moderne kryptographische Systeme sind aus unserem digitalen Leben nicht mehr wegzudenken. Sie kommen dort zur Anwendung, wo Informationssicherheit gegeben sein soll, um Manipulation und unbefugtes Lesen von Daten zu verhindern. Sie schützen unsere Privatsphäre und ermöglichen den sicheren Austausch von Daten und Geld.

Zahlreiche Methoden moderner Kryptosysteme werden unter Verwendung von Polynomen über endlichen Körpern erstellt. Salopp formuliert sind endliche Körper endliche Zahlenbereiche, auf denen die Grundoperationen wie Addition, Subtraktion, Multiplikation und Division wohl definiert sind. Ihre Anwendung in der Kryptographie fußt auf der Tatsache, dass es in einem endlichen Körper sehr einfach ist a^x auszurechnen. Es ist jedoch kein Algorithmus bekannt, der für gegebene a und b die Gleichung a^x = b für x effizient lösen kann.

Zum Beispiel werden Algorithmen für digitale Signaturen mit auf elliptischen Kurven basierender Kryptographie (ECC) modelliert. In Österreich wird ECC seit 2004 für E-Cards und Bankkarten verwendet. Diese elliptischen Kurven lassen sich wiederum durch Polynomgleichungen über endliche Körper beschreiben. Ein weiteres kryptographisches System, welches ebenfalls durch nichtlineare arithmetische Gleichungen in endlichen Körpern modelliert werden kann, sind Zero-Knowledge Proofs. Dies sind Methoden, bei denen Teilnehmer*innen mit hoher Wahrscheinlichkeit nachweisen können, dass sie geheime Informationen kennen, ohne diese Informationen selbst preisgeben zu müssen. Zero-Knowledge Proofs finden in Smart Contracts und vielen gängigen Kryptowährungen ihren Einsatz. Man kann sich also leicht davon überzeugen, dass Polynomgleichungen über endliche Körper mittlerweile beim Entwurf moderner Kryptosysteme eine große Rolle spielen.

GERECHTFERTIGTER AUFWAND

Die Wichtigkeit von Kryptosystemen rechtfertigt die Tatsache, dass viel Aufwand betrieben wird, um ihre Korrektheit sicherzustellen. Man will garantieren können, dass diese Systeme fehlerfrei sind, um eine mögliche Gefährdung von Daten ausschließen zu können. Wie kann man nun aber überprüfen, dass ein gegebenes System bestimmte Anforderungen erfüllt? Ein naiver Weg wäre, alle möglichen Optionen auszuprobieren. Aufgrund der Komplexität von Kryptosystemen ist dies in der Praxis jedoch kaum durchführbar. Daher greift man auf logische Beweistechniken zurück, um die Korrektheit von Systemen formal und automatisiert sicherzustellen. Formale Verifikation ermöglicht es zu überprüfen, ob ein System bestimmte vordefinierte Anforderungen erfüllt. Dieses erwartete Verhalten wird dabei mittels eines formalen Modells beschrieben.

Im Fall von obigen Kryptosystemen hat man es mit einem algebraischen Modell für Polynomgleichungen über endliche Körper zu tun. Genauer gesagt wird das gegebene Kryptosystem und die Eigenschaft, die man überprüfen will mit Hilfe eines polynomialen Gleichungssystems dargestellt. In unserer Arbeit wollen wir zeigen, dass das Gleichungssystem entweder eine Lösung besitzt, also dass man allen Variablen in den Polynomen Werte zuweisen kann, sodass die einzelnen Polynomgleichungen stimmen. In diesem Fall liefern wir eine konkrete Variablenbelegung als Ergebnis. Oder aber wir zeigen, dass das Gleichungssystem keine derartige Lösung besitzt.

In der Vergangenheit haben sich hauptsächlich Wissenschaftler*innen im Bereich der Computer Algebra mit dieser Fragestellung beschäftigt. Dank des Fundamentalsatzes der Algebra und Ansätzen aus der Gröbner Basen Theorie ist das Auffinden von Lösungen für Systeme polynomialer Gleichungen über algebraisch geschlossene Körper algorithmisch lösbar und es gibt zahlreiche Algorithmen, um die Lösungen von allgemeinen Gleichungssystemen zu finden. Diese Ansätze haben aber einen gemeinsamen Nachteil, sie leiden an hohem, oft auch exponentiellem Rechenaufwand.

Seit dem Aufkommen von modernen Kryptosystemen und der Notwendigkeit ihre Korrektheit sicher zu stellen ist es allerdings notwendig, dass diese Algorithmen skalieren. Daher beschäftigt sich nun auch die Forschung im Bereich formaler Verifikation mit dieser komplexen Aufgabenstellung. In gängigen Verifikations-

methoden kommen häufig Satisfiability Modulo Theories (SMT) Solver, wie Z3 oder cvc5 zum Einsatz. SMT-Solver sind automatisierte Tools, die ein Entscheidungsproblem für logische Formeln in Bezug auf Hintergrundtheorien, wie etwa ganze oder reelle Zahlen, lösen können. Intern kombinieren SMT-Solver Suchalgorithmen mit dedizierten Lösungsalgorithmen für die zuvor definierte Hintergrundtheorie. Gängige SMT-Solver unterstützen nach aktuellem Stand jedoch keine Theorie für endliche Körper.

KOMBINATION AUS LOGIK UND COMPUTER ALGEBRA

Genau an diesem Problem setzt unsere Forschung an. In meinem Team an der TU Wien kombinieren wir Methoden aus der Logik und Computer Algebra, um SMT-Solver mit der Hintergrundtheorie über endliche Körper zu ergänzen. Wir verfolgen hier zweierlei Ansätze.

Die erste Methodik beschäftigt sich damit, die Systeme der polynomialen Gleichungen mit SMT-basierten Entscheidungsprozessen zu lösen, die direkt mit den Modellen arbeiten. Man iteriert über die Polynomgleichungen und versucht schrittweise den einzelnen Variablen Werte zuzuweisen. Dies geschieht durch logische Schlussfolgerungen, die mittels Ansätzen aus der Computeralgebra getroffen werden. Wenn keine Schlussfolgerungen möglich sind, wird ein neuer Wert geraten. Sollten wir auf diesen Weg eine Belegung für alle Variablen finden, sodass jede Polynomgleichung stimmt, haben wir eine Lösung für das System erhalten. Wenn allerdings keine Lösung gefunden wird, sondern ein Konflikt entsteht, z. B. in der Aussage 1=0, dann wird ein Teil des Lösungsweges revidiert und geratene Werte geändert. Zusätzlich lernen wir, dass die zuvor getroffenen Entscheidungen zu einem falschen Ergebnis führten und fügen dieses Wissen in Form gelernter neuer Gleichungen zu unserem System hinzu. Auf diese Art und Weise wird fortgefahren, bis entweder eine vollständige Lösung für das Gleichungssystem gefunden wird oder der gesamte Suchraum abgedeckt ist. In diesem Fall hat das Gleichungssystem keine Lösung.

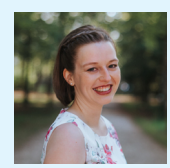
Unser zweiter Ansatz verallgemeinert die Problemstellung. Wir beschränken uns nicht mehr rein auf Polynomgleichungen über endliche Körper, sondern generalisieren auf allgemeine Restklassenpolynome modulo 2^k. Die Idee dahinter ist, dass wir mit dieser generelleren Methode eine Beweisführung über Bitvektoren, also Arithmetik modulo 2^k, betreiben können, was ebenfalls ein breites Anwendungsgebiet von SMT-Solvern ist.

Momentan betreiben gängige SMT-Solver eine so-genannte Bit-blasting Methode. Das heißt es werden Aussagen direkt über die einzelnen Bits in den Bitvektoren getroffen, anstatt den Bitvektor als eigenständige Einheit zu betrachten. Obwohl diese Methode für eine Vielzahl von Anwendungsfällen funktioniert, terminiert sie oft für Probleme mit vielen Multiplikationsschritten nicht mehr, da die Formeln mittels Bit-Blasting zu groß werden.

AUSSAGEN ZU BITVEKTOREN

Wir wollen nun eine alternative Methode finden, die es ermöglicht direkt Aussagen über Bitvektoren zu treffen. Auch in diesem Fall nutzen wir einen modellbasierten Ansatz, um Bitvektoren zu lösen. Im Gegensatz zu endlichen Körpern muss man allerdings um einiges vorsichtiger sein, da bestimmte theoretische Ergebnisse nicht mehr gelten oder undefiniert sind. Würde man diese dennoch anwenden, verliert man die Korrektheit der Lösungen. Beispielsweise gilt in endlichen Körpern die Nullteilerfreiheit, das heißt aus a*b = 0 folgt a=0 oder b=0. In allgemeinen endlichen Zahlenbereichen gilt dies jedoch nicht mehr, da 6*8 = 0 mod 16. Um dennoch den Suchraum für mögliche Lösungen korrekt einzuschränken, analysieren wir die Gleichungen und können so Intervalle von falschen Belegungen finden und die Anzahl möglicher Variablenbelegungen erfolgreich einschränken.

Mit unseren beiden Techniken können wir Eigenschaften von industriellen Kryptosystemen verifizieren und so deren Korrektheit sicherstellen. Wir arbeiten derzeit daran unsere Methoden in verfügbaren SMT-Solvern zu integrieren. Ein zukünftiges Ziel ist die Hintergrundtheorie über endliche Körper mit anderen, bereits verfügbaren SMT Hintergrundtheorien zu verknüpfen, um so allgemeinere Lösungsansätze zu erreichen.



DI Dr. **Daniela Kaufmann** ist PostDoc Reasearcher in der Automated Program Reasoning Group am Institute of Logic and Computation an der TU Wien. Ihre Forschungsinteressen sind angewandte formale Methoden im Bereich Soft- und Hardwareverifikation mittels SAT und SMT Solving und Computeralgebra.

von Markus Hecher

Strukturelle Zusammenhänge beim Lösen kombinatorischer Probleme – und ihre Grenzen

In den letzten Jahrzehnten konnte ein beachtlicher Fortschritt zum Lösen aussagenlogischer Formeln verzeichnet werden, der sich durch überwältigend effiziente Computerprogramme äußert. Einer der Gründe dieser Effizienz betrifft strukturelle Eigenschaften von Formeln, zum Beispiel der sogenannten Baumweite, die misst, wie groß der Abstand zu einfachen Strukturen (Bäumen) ist. Solche strukturellen Eigenschaften sind allerdings bei Weitem nicht auf Aufgabenstellungen in der Logik beschränkt. Dieser Artikel befasst sich mit *strukturellen Methoden und Werkzeugen* zum Lösen kombinatorisch schwieriger Probleme, wie sie beispielsweise in der Künstlichen Intelligenz (KI) relevant sind, sowie zum Beweisen deren Grenzen.

Wir präsentieren einen neuen Typ von Problemreduktion, der die ***struktursensitive*** Übersetzung solcher Probleme, beispielsweise in die Aussagenlogik, erlaubt. Diese struktursensitiven Reduktionen können gezielt Lösungsaufwand in der Baumweite auf Kosten höherer struktureller Abhängigkeiten (höherer Baumweite) tauschen und ermöglichen damit *präzise Laufzeiten (obere Schranken)* in der Baumweite. Kann man diese oberen Schranken nun signifikant verbessern? Zur Beantwortung werden wiederum struktursensitive Reduktionen verwendet. Diese dienen als Basis, um eine lange offen gebliebene Frage bezüglich der Komplexität eines kanonischen Problems bei beschränkter Baumweite zu lösen. Die Lösung dieser Frage ermöglicht schlussendlich ein neues Meta-Werkzeug zum Beweisen *präziser unterer Laufzeitschranken* für eine Vielzahl von Problemen der KI. Diese unteren Schranken bauen auf übliche Annahmen in der Komplexitätstheorie auf und machen damit signifikante Verbesserungen der oberen Schranken sehr unwahrscheinlich.

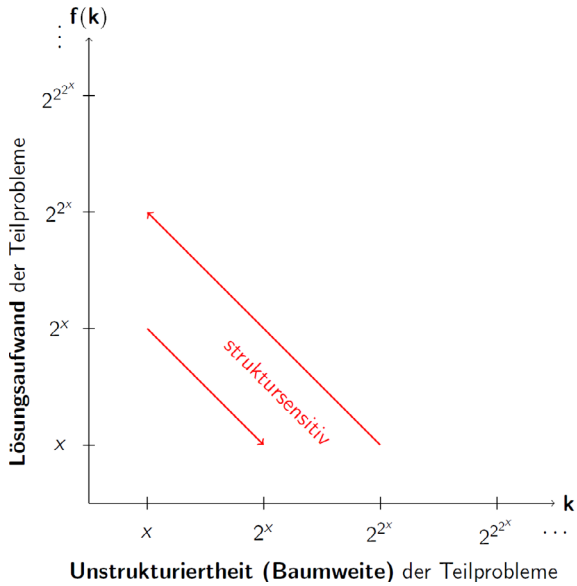
Bereits in den frühen Kinderschuhen der Informatik hat man damit begonnen, wichtige, wiederkehrende Aufgabenstellungen (Probleme) anhand ihrer *Komplexität zu klassifizieren*, was vor allem dazu geführt hat, eine Partitionierung dieser in „praktisch lösbar" und „praktisch wahrscheinlich unlösbar" zu erhalten. Das Lösen aussagenlogischer Formeln ist einer der prominentesten Vertreter der zweiten Kategorie. Heutzutage ist allerdings diese Kategorie „praktisch wahrscheinlich unlösbar" noch viel weiter unterteilt, genauer erforscht und es gibt neben schnellen Computerprogrammen zum Lösen inzwischen sogar allgemeine und gut untersuchte Methoden, um solche Probleme dennoch praktisch lösen zu können.

STRUKTURBASIERTE LÖSUNGSANSÄTZE

Eine dieser gut erforschten Lösungsmethoden nennt sich *dynamische Programmierung*, welche dem Prinzip „Teile-und-Herrsche" folgt. Dabei werden Probleme so lange in kleinere Teilprobleme zerlegt bzw. aufgeteilt, bis diese praktisch lösbar sind, sodass die Teillösungen kombiniert werden können, um eine Gesamtlösung des ursprünglichen Problems zu erhalten. Nehmen wir als Beispiel eine Logistikaufgabe, bei der ein Transportnetzwerk zwischen Wien und Berlin bedient werden soll, um Waren zu bestimmten Lagerhallen zu bringen. Aufgrund horrender Treibstoffpreise sollen kostengünstige Transportwege erreicht werden, indem Lösungen von Teilaufgaben über potenzielle Zwischenlager entsprechend kombiniert werden. Natürlich gibt es verschiedene Möglichkeiten, wie man diese Teilaufgaben erhält.

Ein sehr allgemeines Maß, anhand dessen man solche Teilaufgaben erhalten kann, ist die sogenannte ***Baumweite;*** ein Parameter, der strukturelle Zusammenhänge beispielsweise solcher Transportnetzwerke angibt. Dabei ist dieses Maß sehr vielseitig einsetzbar und gibt in gewisser Weise den Abstand zu einfachen Strukturen, nämlich zu sogenannten Bäumen, welche zumeist strukturell einfachere Teilprobleme erlauben. Jetzt möchte man meinen, dass strukturell einfachere Teilprobleme (von kleiner Baumweite) immer einfacher zu lösen sind als Teilprobleme größerer Baumweite. Nun, das kann man so allgemein nicht behaupten, denn zusätzlich hängt der erforderliche ***Lösungsaufwand der Teilprobleme*** auch immer von der ***Art des Problems*** ab. So gibt es beispielsweise Fragestellungen, bei denen sich viele Forscher*innen einig sind, dass sie sehr viel aufwändiger zu lösen sind als das oben erwähnte Logistikproblem. Wie verhalten

Abb. 1: Strukturensitive Reduktionen zum Tauschen von Lösungsaufwand auf Kosten von Unstrukturiertheit (und retour).



sich denn nun *strukturelle Abhängigkeit und Lösungsaufwand zueinander* und was genau ist mein Forschungsbeitrag?

STRUKTURSENSITIVE REDUKTIONEN ZUM VERWERTEN VON STRUKTUR

Mein Forschungsthema befasst sich mit dem Lösen schwieriger bzw. kombinatorisch harter Probleme durch Aufteilung, bei Verwendung struktureller Eigenschaften wie der Baumweite. Dabei habe ich einen neuen Ansatz entwickelt, nämlich *strukturensitive Reduktionen*, um gezielt einen *hohe Teilproblemlösungsaufwand* gegen *hohe Unstrukturiertheit* in der Form von hoher Baumweite zu tauschen. Visualisiert ist so eine strukturensitive Reduktion in Abbildung 1 (unterer roter Pfeil). Diese Reduktionen ermöglichen es, eine Vielzahl von Problemen der künstlichen Intelligenz, bei denen man davon ausgeht, dass sie schwieriger als Aussagenlogik sind, dennoch in logische Formeln zu kodieren, um präzise obere *Laufzeitschranken* zu erhalten .

GEHT ES BESSER?

Kurz gesagt: Nein! Hier sind strukturensitive Reduktionen unerlässlich beim Verkleinern hoher Unstrukturiertheit auf Kosten eines höheren Teilproblemlösungsaufwandes (siehe Abbildung 1: oberer roter Pfeil). Damit konnte ich für eine Familie an kanonischen Problemen der Logik beweisen, dass unter üblichen Annahmen in der Komplexitätstheorie, für jedes dieser Probleme ein gewisser *Teilproblemlösungsaufwand in der Baumweite* notwendig ist, was präzise untere Laufzeitschranken liefert. Mein Resultat bestätigt nun auch formal eine Vermutung, die seit beinahe 20 Jahren offengeblieben ist.

Dieses Resultat hat weitreichende Konsequenzen für eine Vielzahl an Problemen in der Logik, Wissensrepräsentation, und künstlichen Intelligenz. Es hat sich gezeigt, dass mein Ansatz ein *neues Meta-Werkzeug* einführt, das eine Vielzahl von Resultaten (untere Laufzeitschranken) liefert. Des Weiteren führt dieser Ansatz zu einer *neuartigen Klassifikation*, die Probleme entsprechend dem Problemlösungsaufwand bei Verwendung von Baumweite einteilt.

THEORETISCHE GRENZEN ALS INDIZIEN FÜR PRAKTISCHE ERFOLGSAUSSICHTEN?

Man möchte meinen, dass obige Klassifikation vorrangig von theoretischer Natur ist, sodass sich keine Auswirkungen für praktische Lösungsansätze ergeben. Eigentlich nicht! Ich habe des Weiteren noch konkrete Ansätze gebaut, wie man aufwändige Probleme auf diese Art auch praktisch lösen kann und das funktioniert noch dazu *erstaunlich gut*. Kanonische Zählprobleme in der Aussagenlogik im Bereich des quantitativen Schließens können damit Formeln bis zu Baumweiten von ca. 200 praktisch gelöst werden, was in etwa einem maximalen Aufwand (Worst Case) von 2^{200} entspricht. Aufwändigere Erweiterungen davon können bis zu einer Baumweite von ca. 100 gelöst werden, allerdings wird hier bereits im Allgemeinen ein Aufwand von $2^{2^{100}}$ erwartet. Man beachte, dass im Vergleich dazu unser *Universum aus weniger als* 22^9 *Atomen* besteht (Schätzung). Erreicht wird diese erstaunliche Effizienz durch eine hybride Technik, die bestehende Computerprogramme in diesem Bereich substanziell erweitert und verbessert, indem zusätzlich strukturelle Abhängigkeiten zielgerichtet ausgenutzt werden.

Man sieht also, dass Forschung und eine feingranulare Untersuchung struktureller Abhängigkeiten nicht nur wesentliche Beiträge zur *Klassifikation von Problemkomplexität* liefern kann. In weiterer Folge kann dies zu neuen, *kompetitiven Lösungsansätzen* führen, sodass die theoretische Klassifikation bereits entsprechende Erwartungen andeutet bzw. Erfolgsaussichten bereitstellt.

Für mehr Details verweise ich auf eine Kurzfassung in englischer Sprache (https://arxiv.org/abs/2208.11340) sowie auf mein kürzlich erschienenes Buch (https://www.iospress.com/catalog/books/advanced-tools-and-methods-for-treewidth-based-problem-solving) und weitere Folgearbeiten, welche auf meiner Homepage gelistet sind (https://dbai.tuwien.ac.at/staff/hecher).

Dr. **Markus Hecher** ist Postdoc am MIT in den USA, wo er an seinem Forschungsprojekt zum Thema quantitatives Schlussfolgern forscht. Für seine Dissertation und seine Forschungsleistung wurde er bereits mit einigen Preisen ausgezeichnet, unter anderem mit dem österreichischen Staatspreis Award of Excellence 2021, dem GI Dissertationspreis 2021, dem europäischen EurAI Dissertation Award 2021, sowie dem KR Early Career Award 2022.

von Gerald Quirchmayr und Wolfgang Klas

Go European - Go International

Forschung, die von Studierenden unter der Leitung eines erfahrenen Akademikers durchgeführt wird, ist ein wichtiger Aspekt der Nachwuchsförderung. Sie bietet der nächsten Generation die Möglichkeit, wertvolle Erfahrungen auf diesem Gebiet zu sammeln und zur Entwicklung neuer Technologien, Techniken und Strategien zum Schutz von Informationsressourcen und -systemen vor Cyberbedrohungen und Falschinformationen beizutragen.

An der Forschungsgruppe Multimedia Information Systems der Fakultät für Informatik an der Universität Wien werden in diesem Themenkreis aktuell Forschungsarbeiten in den Schwerpunkten Information Security Management und Vertrauenswürdigkeit & Korrektheit von Informationen im Internet durchgeführt. Dabei stehen einerseits nationale und europäische Forschungsprojekte, wie z. B. CS-AWARE-NEXT (Horizon Europe), COLTRANE (Erasmus+), KIRAS SHIFT (National), und andererseits forschungsgruppengestützte Aktivitäten, wie z. B. FactCheck++, durchgeführt. Beide Themenkreise bilden für die Forschungsgruppe eine strategische Basis zur Nachwuchsförderung. Diese umfasst die Unterstützung von Postdocs, Dissertanten und Studierenden in den Masterprogrammen Wirtschaftsinformatik und Informatik.

Im Rahmen dieser Forschungsprojekte angesetzte Dissertationen haben neben der Einbindung in aktuelle Fragestellungen und Konzeptentwicklungen meist auch den Vorteil der unmittelbaren Anwendung deren Projektergebnisse im industriellen Kontext. Dadurch werden Young Researchers in die Lage versetzt, realitätsnahe Fallstudien zum Test ihrer Forschungsergebnisse verwenden zu können.

Auf diese Weise wird es Young Researchers ermöglicht, an realen Problemen zu arbeiten und so einen spürbaren Einfluss auf das Gebiet zu nehmen. Sie lernen und arbeiten mit modernsten Methoden, Technologien und Techniken, was sie bei der Vorbereitung auf Karrieren in der Cybersicherheit oder verwandten Bereichen unterstützt. Als Teil dieses Umfelds präsentieren die Studierenden ihre Ideen auf internationalen Konferenzen und veröffentlichen ihre Forschungsergebnisse in wissenschaftlichen Zeitschriften. Dies ist ein wichtiger Schritt zur Etablierung ihres eigenen Rufs in diesem Bereich.

CS AWARE NEXT Vienna 12-2022 © kim_gammelgaard

Zusammen mit internationalen Austauschprogrammen bietet diese Forschungslandschaft eine herausfordernde, spannende und von vielen Entwicklungsmöglichkeiten geprägte Umgebung. Allianzen mit führenden nationalen Forschungszentren (SBA Research, AIT) eröffnen weitere Chancen zur Entwicklung einer wissenschaftlichen Karriere.

Es gibt jedoch auch Herausforderungen im Zusammenhang mit studentischen Forschungsaktivitäten. Eine der Hauptschwierigkeiten ist der anfängliche Mangel an Erfahrung und Wissen, die Studierende im Vergleich zu erfahreneren Forscher*innen haben können. Darüber hinaus haben die Studierenden möglicherweise nur begrenzten Zugang zu Ressourcen und Finanzierung, was den Umfang und die Verbreitung ihrer Arbeitsergebnisse beträchtlich verringern kann. Daher ist es unerlässlich, ihre Forschung mit – insbesondere europäischen – Projekten zu verknüpfen, damit sie Zugang zu Finanzierungsmöglichkeiten und einem Umfeld haben, das die Entwicklung von Wissen und Forschungskompetenzen fördert und beschleunigt.

In aktuellen Forschungsprojekten, z. B. CS-AWARE-NEXT, werden Modelle zur Unterstützung der Entscheidungsfindung im Anwendungsgebiet der Cybersecurity entwickelt und in konkreten Szenarien getestet. Das Management von Cybersecurity Policies, speziell deren Anwendung und laufende Weiterentwicklung in Organisationen und kollaborativen Ökosystemen, steht dabei im Zentrum. Die Möglichkeit zur Teilnahme an internationalen Projektmeetings, Konferenzen, der laufende internationale Ideenaustausch und die gemeinsam mit europäischen Partnern entwickelten Modelle, Konzepte und Prototypen sind ein wesentlicher Motivationsfaktor für Young Researchers. Diese und ver-

gleichbare Möglichkeiten auf nationaler und europäischer Ebene werden durch langjährige Partnerschaften mit Universitäten in Nordamerika, Australien und Asien ergänzt. Die dadurch geschaffene Basis versetzt Young Researchers in die Lage, sich sehr schnell international zu vernetzen, was für eine Karriere im Wissenschaftsbereich einen enormen Vorteil darstellt.

Dieses Setting ermöglicht es den Studierenden, Ressourcen und Wissen auszutauschen und Fachwissen zu bündeln, um komplexe Probleme anzugehen. Die Kooperation mit Partnern aus verschiedenen Ländern und Kulturen kann einzigartige Perspektiven und Einblicke bieten und ist ein guter Weg, um sicherzustellen, dass die Forschung in einem globalen Kontext relevant und anwendbar ist. Während der anfängliche Coaching-Aufwand durch den die Betreuer*in erheblich ist, zahlt sich diese Investition in Bezug auf die Motivation der Studierenden und die Qualität der Forschungsergebnisse definitiv aus.

PERSÖNLICHE FREUNDSCHAFTEN - INTERKULTURELLER AUSTAUSCH

Intensive wissenschaftliche Diskussionen in diesem Umfeld sind auch dazu geeignet, neue nationale und internationale Freundschaften zu bilden, mit dem angenehmen Nebeneffekt, dass neben dem rein fachlichen Wissenserwerb auch der interkulturelle Austausch intensiviert werden kann. Die internationale Ausrichtung der Forschung wird in der Forschungsgruppe als wichtige Voraussetzung gesehen, um Young Researchers bei ihrer fachlichen und persönlichen Entwicklung zu unterstützen.

Zusammenfassend kann festgehalten werden, dass jene Arbeiten, die von Studierenden unter der Aufsicht von erfahrenen Wissenschaftler*innen durchgeführt wird, ein wichtiger Aspekt bei der Gestaltung der Zukunft der Forschung und Praxis ist. Ein internationales Setting bietet Studierenden die Möglichkeit, relevante Erfahrungen zu sammeln und sich in das Feld einzubringen, idealerweise mit neuen Ideen mit spürbarer Wirkung. Die Zusammenarbeit mit nationalen und internationalen Partnern ist eine gute Möglichkeit, viele der bestehenden Schwierigkeiten und Einschränkungen zu überwinden und einzigartige Perspektiven und Einblicke in die Forschung zu bieten.

Ein neues Team-Mitglied wird willkommen geheißen.

Univ.-Prof. Dipl.-Ing. Dr. Dr. **Gerald Quirchmayr** lehrt gegenwärtig an der Fakultät für Informatik der Universität Wien. Der Fokus seiner Forschung liegt auf Informationssystemen in Wirtschaft und Verwaltung mit einem besonderen Interesse an Sicherheit, Anwendungen, formalen Darstellungen der Entscheidungsfindung und rechtlichen Fragen.

Univ.-Prof. Dipl.-Ing. Dr. **Wolfgang Klas** ist Leiter der Forschungsgruppe Multimedia Information System der Fakultät für Informatik der Universität Wien. Sein Forschungsinteresse liegt in Techniken und Methoden für die Verwaltung multimedialer semantischer Inhalte und multimedialer Umgebungen im Kontext von Webtechnologien und Blockchain-Systemen.

von Christian Luidold

Cybersicherheit für Unternehmen

Unternehmensweite Cybersecurity Policies (Organizational Policies) gelten als interne Rahmenwerke, Pozessabbildungen oder Richtlinien, welche einen strukturierten und effizienten Ablauf von Prozessen gewährleisten sollen. Dabei sollen Policies möglichst genau definiert sein, sodass in einem gegebenen Fall jede unternehmensinterne Person über ihre Verpflichtungen, sowie weitere involvierte Positionen oder externe Entitäten (z. B. Behörden) informiert ist.

Policies bilden unterschiedliche Themen (z. B. von Passwörtern zu Incident Management) ab und können unterschiedliche Entstehungsgründe (z. B. interne Abläufe, Gesetze und Standards) haben. So wie sich interne Prozesse innerhalb einer Organisation, wie auch das externe Umfeld ändern kann, kann gegebenenfalls Druck auf Policies ausgeübt werden. Dazu ist es notwendig diese laufend aktuell zu halten, um auch für unerwartete Situationen entsprechend vorbereitet zu sein, womit ein effizientes Management von Policies innerhalb eines Unternehmens notwendig ist.

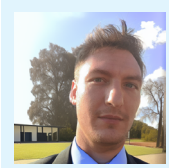
Der Prozess zur Aktualisierung von Policies kann je nach Organisation mit unterschiedlich hohem Ressourcenaufwand verbunden sein. Zusatzaufwand entsteht in der Regel durch die Anpassung der operationalen Umgebung an die in den Policies definierten Prozesse. Der Trigger zur Revision von Policies kommt primär durch externe Einflüsse, vor allem durch definierte Standards wie die ISO/IEC 27001, sowie durch die NIS-2-Richtlinie.

Die sich ständig verändernden Angriffs- und Bedrohungslandschaften erfordern ein dynamisches Konzept zur kontinuierlichen Beobachtung und Neubewertung und der daraus folgenden Anpassung. Als Basis dienen dabei die Vorgaben und Empfehlungen der jeweils zuständigen NIS-Behörden und CSIRTs, sowie die Berücksichtigung von gesammelten internen Daten, wie auch durch Externe geteilte CTI (Cyber Threat Intelligence).

ENTWICKLUNG KOLLABORATIVER LÖSUNGEN

Das Ziel der Forschungsarbeit ist die Entwicklung eines datengesteuerten und risiko-orientierten Frameworks für die Verwaltung von Policies im Bereich Cybersicherheit für Unternehmen. Anwender*innen soll eine kollaborative Lösung angeboten werden, die den gesamten Policy Life Cycle umfasst, von der Erstellung über das Monitoring eingesetzter Policies bis hin zur Überarbeitung oder dem Ersatz von Policies. Das Stichwort „kollaborativ" ist hierbei mehrschichtig zu verstehen. Zum einen dient dieser Aspekt eines lebendigen Prozesszyklus innerhalb einer Organisation der Aktualität und Anwendbarkeit. Dazu zählen auch Prozesse zur Bewertung und Anpassung der Policies und eine daraus folgende erleichterte Zusammenarbeit mit den betroffenen Mitarbeiter*innen. Zum anderen wird an der Zusammenarbeit mit Ministerien, Behörden, und CSIRTs daran geforscht, wie bestehende Prozesse verbessert und automatisiert werden können, um ein schnelleres und besser koordiniertes Handeln zu unterstützten.

Diese Bereiche werden im Zuge des Horizon Europe Projekts „CS-AWARE-NEXT" mit internationalen Forschungspartnern erforscht und in Kooperation mit Anwender*innen erprobt. In diesem Rahmen werden interoperable Ansätze untersucht, primär hinsichtlich ihrer Kompatibilität mit Incident Management & Disaster Recovery Ansätzen in Verbindung mit automatisierten Workflows. Dabei sollen von Policies definierte Prozesse ausgeführt und deren Performance beobachtet werden. In Abhängigkeit von den Resultaten dieser Prozesse werden je nach Notwendigkeit entweder die Prozesse selbst oder die dahinterstehenden Policies überarbeitet. Der Bewertungsprozess verwendet Daten (z. B. interne Logs, externe Meldungen), die zusätzliche - durch Machine Learning-Modelle entwickelte - Thresholds oder Trigger bilden können, um eine Überarbeitungsnotwendigkeit aufzeigen oder, je nach Komplexität, selbst einleiten zu können. Die Überarbeitung von komplexeren Policies wird durch aktuelle Modelle der Entscheidungsfindung unterstützt.



Christian Luidold forscht als PhD-Student an der Fakultät für Informatik der Uni Wien an nationalen und internationalen Projekten, Forschungsschwerpunkt Information Security Policy Management und Security Automation. In der OCG-Zertifizierungsstelle arbeitet er an Themen im Umfeld von ISO/IEC 27001.

Bedrohungen erkennen – Risiken bewerten – Lösungen entwickeln

von Christoph Jungbauer

Resiliente Computersysteme gegen Cyberbedrohungen

Als junger Forscher auf dem Gebiet der Entwicklung resilienter Computersysteme ist es meine Leidenschaft, neue Technologien und Strategien zu entwickeln, um kritische Informationssysteme zu schützen und ihre Resilienz angesichts von Cyberbedrohungen zu gewährleisten. Diese ist von entscheidender Bedeutung, um Störungen durch Cyberangriffe, Naturkatastrophen und andere widrige Ereignisse zu verhindern oder sich nach einem Vorfall schnell davon zu erholen.

Eine der Voraussetzungen für widerstandsfähige IT-Systeme sind resiliente IT-Systeme. Resilienz ist entscheidend für die Aufrechterhaltung der Verfügbarkeit, Vertraulichkeit und Integrität von Informationssystemen und um sicherzustellen, dass kritische Funktionen im Falle einer Unterbrechung schnell wiederaufgenommen werden können. Maßnahmen zur Stärkung der Cybersicherheit sind die erste Verteidigungslinie gegen Cyberangriffe und müssen mit Blick auf die Widerstandsfähigkeit konzipiert und umgesetzt werden. Dazu gehören umfassendes Bedrohungs-Management, regelmäßige Software-Updates und Patches sowie die angemessene Schulung und Sensibilisierung der Benutzer*innen.

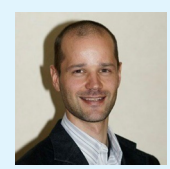
Eine zusätzliche Herausforderung bei der Entwicklung resilienter Systeme ist die Verfügbarkeit öffentlicher Daten über Angriffe beispielsweise in Unternehmen. Weiters können öffentlich verfügbare Daten zwar wertvolle Erkenntnisse über neue Bedrohungen und Schwachstellen liefern, sie können aber auch unzuverlässig, veraltet oder unvollständig sein. Daher ist es wichtig, öffentlich verfügbare Daten zu validieren und sie in Verbindung mit anderen Quellen zu nutzen, um fundierte Entscheidungen über Sicherheitsmaßnahmen zu treffen.

Die Entwicklung resilienter Systeme ist ein komplexes und sich ständig weiterentwickelndes Gebiet, das einen multidisziplinären Ansatz erfordert. Durch die Festlegung von Prioritäten bei Cybersicherheitsmaßnahmen, die konsequente Durchführung von Risikobewertungen und die Nutzung einer Kombination aus öffentlichen Daten und anderen Quellen kann die Widerstandsfähigkeit kritischer Informationssysteme gewährleistet werden und Störungen durch Cyberangriffe minimiert werden.

NATIONALE UND INTERNATIONALE ZUSAMMENARBEIT

Als Forscher, die die Chance haben mit international erfahrenen Universitätsprofessor*innen zu arbeiten, haben wir die einmalige Gelegenheit, zur Entwicklung neuer Technologien und Strategien für Entwicklung und Betrieb resilienter Systeme beizutragen. Unsere Forschung konzentriert sich darauf, akute Bedrohungen für Unternehmen und kritische Infrastrukturen zu identifizieren, Risiken zu bewerten und wenn möglich praktische Lösungen zu deren Beseitigung zu entwickeln, die letztlich zur Verbesserung der Resilienz von Informationssystemen führen. Die (virtuelle) Zusammenarbeit mit nationalen und internationalen Partnern aus Universitäten und der Industrie bietet uns die Möglichkeit, unser Wissen und unsere Erfahrung zu erweitern und innovative Lösungen zu entwickeln, die zur Verbesserung der allgemeinen Sicherheit von Informationssystemen beitragen können. Durch die Kooperation mit Partnern aus verschiedenen Ländern und Kulturen können wir bewährte Verfahren und Wissen austauschen und von unterschiedlichen Ansätzen und Lösungen lernen.

Zusammenfassend lässt sich sagen, dass die Entwicklung resilienter Systeme eine entscheidende Priorität im Bereich der Cybersicherheit ist. Als Forschende haben wir die Möglichkeit, zu dieser wichtigen Arbeit beizutragen und dabei zu helfen, die Sicherheit von Informationssystemen angesichts der sich laufend ändernden Cyberbedrohungen zu gewährleisten. Durch die persönliche und virtuelle Zusammenarbeit mit nationalen und internationalen Partnern können wir neue Lösungen entwickeln und die Sicherheit kritischer Informationssysteme insgesamt verbessern. Aktuell arbeiten wir unter anderem an den Projekten SHIFT (um sichere, technische Simulationsumgebungen für Cyber-physische Systeme zu entwerfen und zu entwickeln), COLTRANE (Ausbildung im Bereich der Cybersicherheit, Schwerpunkte: Awareness und Kooperation) und CS-AWARE-NESXT (um Organisationen und lokalen/regionalen Versorgungsnetzen im Cybersicherheitsmanagement zu unterstützen).



Christoph Jungbauer forscht als Doktorand an der Uni Wien zu Cybersecurity, Business Continuity und Disaster Recovery. sowie als Senior Researcher an der FFH Wiener Neustadt ua. zu quantitativem Risikomanagement.

von Christina Stoiber

Visualisierung gegen Informationsüberlastung

Sind Ihre Benutzer*innen an Bord? Visualisierungs-Onboarding unterstützt unerfahrene Benutzer*innen beim Lesen, Interpretieren und Extrahieren von Informationen aus komplexen Datenvisualisierungen.

In den letzten Jahrzehnten sind die Menge und die Komplexität der verfügbaren Daten enorm gestiegen. Diese zunehmende Menge an verfügbaren Daten bietet immense Möglichkeiten zur Förderung des technologischen, wirtschaftlichen und gesellschaftlichen Erfolgs in vielen Bereichen wie Industrie, Medizin oder Wissenschaft. Die Möglichkeit, Daten zu sammeln und zu speichern, wächst jedoch schneller als unsere Fähigkeit, sie zu analysieren und für Entscheidungen zu nutzen. Visuelle Schnittstellen, insbesondere Visualisierungen, sind hochleistungsfähige Gateway-Systeme zur Wahrnehmung von Strukturen, Mustern oder Verbindungen, die in den Daten versteckt sind (Card et al., 1999). Daher kann Visualisierung dazu beitragen, das Problem der Informationsüberlastung zu mildern, indem sie die leistungsstarke menschliche Wahrnehmung ausnutzt, die sehr effizient bei der Verarbeitung visueller Eingaben ist, um Daten zu verstehen, komplexe Informationsräume zu erkunden oder Muster und Beziehungen zu erkennen.

Visualisierung kann als Umwandlung von Daten in eine visuelle Form angesehen werden (Card et al., 1999). Der amerikanische Forscher Stuart K. Card definiert diese visuelle Struktur als eine Menge von Merkmalen (Punkt, Linie, Fläche, Oberfläche, Volumen), deren retinalen Kodierung (Farbe, Größe, Form, Grauwert, Ausrichtung, Textur, Verbindung, Abdeckung) sowie deren Positionen (X, Y, Z, T). Als Benutzer*in muss diese Transformation transparent sein, um die visuellen Darstellungen zu konstruieren und zu entschlüsseln und richtig über die Daten nachzudenken. Obwohl Menschen visuelle Wesen sind und visuelle Darstellungen einfacher zu verstehen sind als andere Datendarstellungen, müssen Benutzer*innen immer noch lernen, wie sie erstellt, gelesen und verstanden werden. Im Vergleich zum Lesen und Schreiben von Text lernen wir normalerweise nicht, wie wir Visualisierungen konstruieren, lesen und interpretieren, außer in einfachen Geschäftsdiagrammen (Börner et al., 2019).

Aufgrund der Komplexität und gesellschaftlichen Relevanz der COVID-19-Pandemie standen Visualisierungen von Daten im Zentrum der weltweiten Aufmerksamkeit (Shneiderman, 2020). Seit dem Ausbruch der Pandemie liefern Datenvisualisierungsforscher*innen und Expert*innen verschiedene Datenvisualisierungen für die öffentliche Bildung. Die Öffentlichkeit hat sich mit diversen Datenvisualisierungen auseinandergesetzt, die medizinische Daten wie Reproduktionszahlen, COVID-19-Fälle, Krankenhausaufenthalte und mehr darstellen.

Viele renommierte Medien haben 2020 Datengeschichten über die Verbreitung von COVID-19 veröffentlicht. Beispiele dafür, wie Datenjournalist*innen das Coronavirus illustriert haben, können zum Beispiel in Deutschland auf ZEIT ONLINE und in der Berliner Morgenpost (siehe Abb. 1) gesehen werden, in der Schweiz im Tages-Anzeiger oder in Österreich interaktiv auf ORF, DER STANDARD oder Kleinen Zeitung.

Interaktive Visualisierungen aktueller COVID-19-Fälle wurden zum Beispiel von der New York Times, der Washington Post oder dem Guardian veröffentlicht (Shneiderman 2020). Neue Formen der Interaktivität, um Datengeschichten zu erzählen,

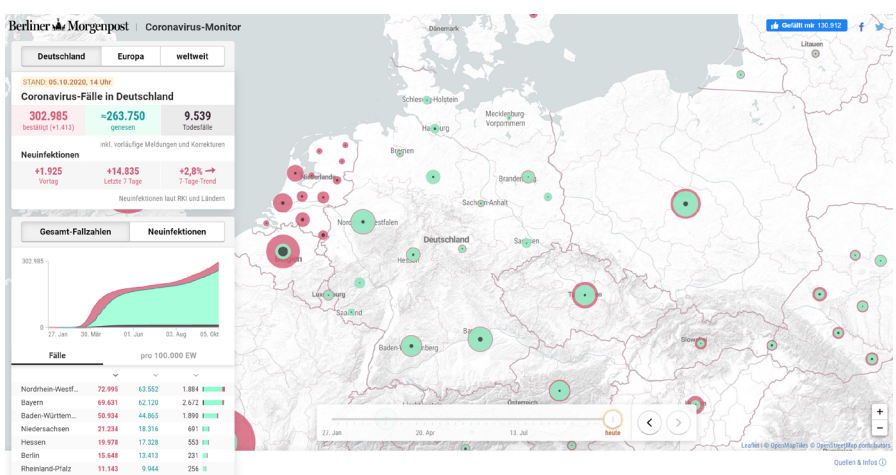
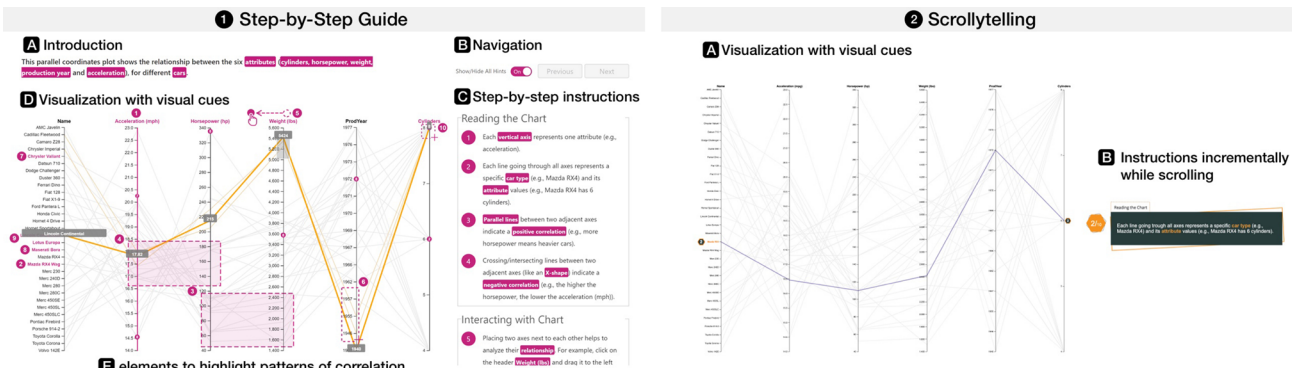


Abbildung 1: Coronavirus-Monitor der Berliner Morgenpost (Accessed: 2020-10-05)

Abb. 2: (1) Schritt-für-Schritt-Anleitung für einen Parallel Coordinates Plot. Die Schritt-für-Schritt-Anleitung basiert auf textlichen Beschreibungen und In-Place-Anmerkungen und besteht aus vier Teilen: einer kurzen textlichen Einführung mit kontextuellen Informationen über die Visualisierung, Navigationselementen zum Durchlaufen der Schritt-für-Schritt-Anweisungen und der Visualisierung selbst. Wir unterteilen die textlichen Beschreibungen in Reading the Chart, zur Interaktion mit dem Diagramm, um das Interaktionskonzept zu erläutern, und die Verwendung des Diagramms, um Einblicke zu geben. (2) Scrollytelling-Anleitung. Die Benutzer*innen können schrittweise durch die Anweisungen scrollen, während sich die Visualisierung entsprechend dem Text ändert.



finden sich in Medien wie der Washington Post durch die Integration von Simulationen (Bradshaw, 2020).

Meine Doktorarbeit zielt darauf ab, Konzepte für das Visualisierungs-Onboarding zu entwickeln, mit denen Nutzer*innen beim Lesen, Interpretieren und Extrahieren von Informationen aus visuellen Datendarstellungen unterstützt werden können (Stoiber et al., 2022a; Stoiber et al., 2022b, Stoiber et al., 2021).

Während unserer Forschung haben wir Visualisierungs-Onboarding-Ansätze aus verschiedenen Perspektiven untersucht. Es wurden vier verschiedene Konzepte für das Visualisierungs-Onboarding entwickelt und evaluiert, um das Onboarding im Detail zu untersuchen. Darüber hinaus haben wir auch abstrakte und konkrete Onboarding-Hilfetexte untersucht, um die Gestaltung und Formulierung der Hilfetexte effizienter zu gestalten.

Wir stellen das resultierende Visualisierungs-Onboarding-Konzept vor und schlagen eine JavaScript-Bibliothek namens VisAhoi vor, um selbsterklärende Visualisierungs-Onboarding-Anweisungen halbautomatisch zu generieren, die in Datenvisualisierungen integriert werden können. Wir haben auch die Anwendbarkeit unseres Ansatzes in zwei Designstudien in den Bereichen datengesteuerter Journalismus (DDJ) und biomedizinische Forschung und Entwicklung (R\&D) gezeigt. Beide Designstudien wurden im Rahmen des SEVA-Forschungsprojekts durchgeführt (https://seva.fhstp.ac.at/en, Zugriff: 2023-01-12).

Abschließend leiten wir aus den Erkenntnissen der Doktorarbeit Gestaltungsmaßnahmen (De Bruijn & Spence, 2008) für die Gestaltung von Visualisierungs-Onboarding-Konzepten ab. Wir stellen auch ein deskriptives Modell vor, um zu zeigen, wie Visualisierungs-Onboarding in verschiedenen Analysephasen eingesetzt werden sollte, um effektiv zu sein und von Benutzer*innen akzeptiert zu werden (Stoiber et al., 2022c). Es kombiniert Visualisierungs-Onboarding und Guidance (Ceneda et al., 2017) sowie wissensgestützte Visual Analytics (VA) (Keim, et al. 2010), da beide typischerweise auf dem Vorhandensein einer Wissensbasis beruhen.

Alle Referenzen finden Sie hier: https://www.ocg.at/de/referenzen-journal-1-23

Christina Stoiber ist Teil des Forschungsprojekts **Vis4Schools**, das die OCG gemeinsam mit der FH St. Pölten und der Masaryk University (MUNI) durchführt. Das transnationale Projekt wird vom FWF Wissenschaftsfonds gefördert.

https://www.ocg.at/de/vis4schools

Christina Stoiber arbeitet als Researcher am Institut für Creative/Media/Technologies an der FH St. Pölten. Ihre Forschungsinteressen sind Informationsvisualisierung, Human-Computer Interaction, Usability und ihr Dissertationsthema Visualisation Literacy.

Ein Überblick über geplante EU-Regulierungsmaßnahmen zu künstlicher Intelligenz

von Philipp Poindl und Jan Hospes

Grundrechte in Maschinenhand

Die Einführung von Systemen künstlicher Intelligenz (KI) geht mit dem Versprechen großer individueller und gesellschaftlicher Vorteile einher. Bestimmte KI-Systeme und damit verbundene maschinelle Lernverfahren bringen aber auch neue Risiken in Bezug auf die Sicherheit der Nutzer*innen und deren Grundrechte mit sich. Der Betrieb sowohl diskriminativer als auch generativer Modelle kann mit intensiven Eingriffen in verfassungsmäßig geschützte Rechtspositionen einhergehen. Zu denken ist beispielsweise an einen diskriminativen Algorithmus, der unter dem Schlagwort „computer says no" den Zugang zu essenziellen Leistungen verwehrt oder ein generatives Modell, das neue medizinische Wirkstoffe zusammenstellt, deren Einnahme zu Nebenwirkungen bei Anwender*innen führt.

DATENSCHUTZRECHTLICHE ASPEKTE

Im Zuge der Erschließung von Kontexten kann die Verarbeitung personenbezogener Daten im Rahmen des Anlernens und der Anwendung von KI-Systemen aus Sicht der betroffenen Personen zu verschiedenen Gefährdungen führen. So kann diese Verarbeitung – insbesondere, wenn sensible Daten aus vielen Quellen zusammengeführt werden – das Risiko unberechtigter Zugriffe oder zweckwidriger Verarbeitungen auf diese Daten erhöhen.

Dabei können geeignete Maßnahmen zur Minimierung der Risiken beitragen. Sollen Machine-Learning-Modelle mithilfe von Daten verschiedener Quellen trainiert werden, können „Federated Learning" (FL) oder „Secure Multiparty Computation" (SMPC) zur Anwendung kommen, um die Einsicht in Daten durch andere Stellen zu verhindern. An den Quelldatensätzen selbst setzt das Konzept „Differential Privacy" an, welcher die Bestimmbarkeit eines Individuums erschwert. Auch die homomorphe Verschlüsselung ist zu erwähnen, welche Berechnungen auf verschlüsselten Daten ermöglicht. Je nach Sensibilität der verarbeiteten Daten kann es geboten sein, mehrere der genannten Mechanismen zu kombinieren. Während die angeführten Verfahren aus datenschutzrechtlicher Sicht Abhilfe schaffen, können sie nicht unbedingt die Auswirkungen des Einsatzes der angelernten Modelle auf andere Grundrechte mitigieren.

BREITER REGULATORISCHER ANSATZ AUF EUROPÄISCHER EBENE

Bereits 2018 hat die EU-Kommission eine europäische Strategie für KI dargelegt. 2020 folgte ein Whitepaper, in welchem bereits zuvor geäußerte Überlegungen um die Schaffung einer menschenzentrierten und vertrauensbasierten KI vertieft und ambitionierte Bestrebungen für den Umgang mit KI dargestellt wurden. 2021 veröffentlichte die Kommission schließlich einen Entwurf für eine KI-Verordnung (oft kurz „AI Act" genannt), der Teile der vorangegangen Erwägungen aufgreift und in der einschlägigen Fachöffentlichkeit derzeit in aller Munde ist. Dieser durchläuft im Moment das ordentliche Gesetzgebungsverfahren, das sich insgesamt sehr dynamisch gestaltet. Daher soll im Folgenden primär jener ursprüngliche Verordnungsvorschlag angeschnitten werden.

Die grundlegende Idee der Verordnung erlebte durchaus auch positive Resonanz. Im Detail sind allerdings einige Regelungen umstritten, was sich insbesondere im öffentlichen Stellungnahmeverfahren zeigte. Inhaltlich folgt der Verordnungsvorschlag einem horizontalen, risikobasierten und einigermaßen technologieneutralen Ansatz. Ausgehend von einer allgemeinen KI-Definition, die sich insbesondere sowohl auf maschinelles Lernen als auch auf wissensbasierte Systeme bezieht, werden drei (Risiko-)Klassen von KI-Anwendungen adressiert. Gewisse eingriffsintensive Systeme, wie „Social Scoring", sollen, ob des hiervon ausgehenden (inakzeptablen) Risikos, verboten werden. Das Hauptaugenmerk des Entwurfs liegt jedoch auf Hochrisiko-KI-Systemen, für die eine Bandbreite an Anforderungen, welche etwa die technische Dokumentation, eine menschliche Aufsicht und Risikomanagement betreffen, vorgesehen wird. Als solche Anwendungen sollen KI-Systeme gelten, die als Produkte oder deren Sicherheitskomponenten unter gewisse EU-Harmonisierungsvorschriften fallen (Anhang II des Entwurfs) und zusätzlich entsprechenden Konformitätsbewertungen durch Dritte zu unterziehen sind. Außerdem enthält Anhang III des Entwurfs eine Auflistung weiterer Hochrisiko-Systeme, darunter solche zur biometrischen Fernidentifizierung natürlicher Personen. Die genannten Verpflichtungen adressieren insbesondere die (neben anderen Begriffen ebenso eigens definierten) *Anbieter* der Systeme. Daneben sollen gewisse Systeme lediglich bestimmten Transparenzverpflichtungen unterliegen, was nach dem Entwurf z. B. solche betrifft, die „Deepfakes" generieren.

Zusätzlich zum „AI-Act" hat die Kommission rezent einen Vorschlag für eine

eigene Richtlinie zur Haftung im Zusammenhang mit KI sowie eine Neufassung der Produkthaftungsrichtlinie veröffentlicht. Bestimmte Eigenschaften von KI (Komplexität, Autonomie und Undurchsichtigkeit), die als „Blackbox"-Effekt zusammengefasst werden, können die Durchsetzung von Schadenersatz erschweren. Dies soll nunmehr durch den Vorschlag für die KI-Haftungs-Richtlinie adressiert werden. Die Richtlinie soll aber zunächst keine verschuldensunabhängige Haftung statuieren, sondern nur gewisse Beweiserleichterungen im Zusammenhang mit dem verschuldensabhängigen, außervertraglichen Schadenersatz gemäß dem nationalen Zivilrecht schaffen. Dadurch sollen potenziell geschädigte Personen möglichst mit solchen gleichgestellt werden, die erwiesenermaßen geschädigt wurden, ohne dass eine KI beteiligt war.

Zu diesem Zweck wird insbesondere eine widerlegbare Vermutung der Kausalität zwischen dem Verschulden des Beklagten und dem vom KI-System hervorgebrachten Ergebnis geschaffen. Damit kann ein ursächlicher Zusammenhang zwischen dem Verhalten des Beklagten und einem Ergebnis, das eine KI (relativ eigenständig) hervorgebracht hat und das zu einem Schaden geführt hat, vermutet werden. Die Regelung ermöglicht die Verlagerung des durch die KI hervorgebrachten schädigenden Ereignisses hin zum verschuldensbegründenden Ereignis des Beklagten und macht Letzteren damit haftbar.

Gleichzeitig wird mit dem Vorschlag für eine neue Produkthaftungsrichtlinie auch eine Einbeziehung in ein verschuldensunabhängiges Haftungsregime bezweckt. Die EU-Produkthaftung adressiert dem Grunde nach nur bewegliche Sachen als „Produkte". Neben anderen Neuerungen soll nunmehr nach Unklarheiten bei der Auslegung des Produktbegriffs klargestellt werden, dass auch Software – und damit auch etwa ein KI-System – erfasst ist.

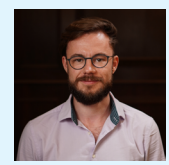
SYNERGIEEFFEKTE IN ZUSAMMENHANG MIT DEM DATENSCHUTZRECHT

Aus unserer Sicht bestünden bei der Risikobeurteilung wesentliche Synergien zwischen den geplanten KI-Regelungen und dem Datenschutzrecht: Bereits jetzt unterliegen gewisse Anwendungen von KI der Voraussetzung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO. Deren Kern stellt die datenschutzrechtliche Analyse von Risiken für die Rechte und Freiheiten natürlicher Personen durch den *Verantwortlichen* (im Sinne der DSGVO) dar.

Der geplante „AI Act" sieht demgegenüber im Zusammenhang mit Hochrisiko-KI-Systemen an mehreren Stellen eine Auseinandersetzung mit Risiken (unter anderem für Grundrechte) vor. Außerdem enthält der Entwurf der Kommission auch einen expliziten Verweis auf die Datenschutz-Folgenabschätzung. *Nutzer* von Hochrisiko-KI-Systemen werden dazu verpflichtet, bestimmte Informationen, deren Bereitstellung *Anbieter* im Zusammenhang mit solchen Systemen zu gewährleisten haben und die auch Aspekte von Grundrechtsrisiken aufgreifen, bei Erfüllung ihrer Pflicht zu einer Datenschutz-Folgenabschätzung zu verwenden.

Es stellt sich jedoch die Frage, wen entsprechende Verpflichtungen schlussendlich treffen, bzw. wann diese zusammenfallen. Denn nach dem Verordnungsentwurf der Kommission obliegt die Einhaltung der im Zusammenhang mit Hochrisiko-KI-Systemen vorgesehenen Anforderungen oft deren *Anbieter*. Der *Verantwortliche* gemäß DSGVO würde nach dem System des „AI Act" in der Praxis (nämlich bei der Verwendung einer KI) hingegen wohl oft dem *Nutzer* entsprechen. In gewissen Fällen sind nach dem Kommissionsvorschlag aber auch etwa *Nutzer* einschlägigen Pflichten eines Anbieters unterworfen, so z. B., wenn sie ein Hochrisiko-KI-System wesentlich verändern.

Insgesamt zeichnet sich ab, dass der Umgang mit KI mit Risikoerwägungen verbunden sein wird, die über jene hinausgehen, die das Datenschutzschutzrecht und die Informationssicherheit gebieten.



Philipp Poindl hat Rechtswissenschaften mit Schwerpunkt Computer und Recht in Wien studiert. Er ist wissenschaftlicher Mitarbeiter am Research Institute – Digital Human Rights Center und war zuvor auch in der Arbeitsgruppe Rechtsinformatik der Universität Wien tätig. Sein Forschungsschwerpunkt liegt derzeit auf der Regulierung von künstlicher Intelligenz.

Jan Hospes ist Jurist mit Spezialisierung auf IT-Recht und als Researcher und Consultant am Research Institute – Digital Human Rights Center tätig. Er forscht unter anderem zu datenschutzrechtlichen Aspekten maschinellen Lernens, zu Identitätsmanagementsystemen und ist Autor datenschutzrechtlicher Publikationen.

Eine Liste nützlicher Links finden Sie hier: https://www.ocg.at/de/referenzen-journal-1-23

von Celina Junghans

Cybersecurity anschaulich vermitteln

Können Sie sich dran erinnern, als Media Markt im Herbst 2021 Opfer einer Ransomware-Attacke wurde und seine Betriebsfähigkeit stark reduzieren musste? Oder als es im letzten Jahr einem Hacker fast gelang, das Wasser im öffentlichen Versorgungsnetzwerk von Florida zu vergiften? Ist Ihnen die Cyber-Attacke auf das Land Kärnten in Erinnerung, bei der begonnen wurde, die Daten des Landes zu verschlüsseln und aus Sicherheitsgründen Teile der Landes IT und damit verbundene Anwendungen stillgelegt werden mussten? Dass Cybersecurity zu einem der relevantesten Themen unserer Zeit gehört, bestreitet kaum jemand.

Die Vielfältigkeit von Cyber-Bedrohungen steigt immer mehr an. Die Gefahr, welche für Unternehmen von Cyber-Bedrohungen ausgeht, lässt sich nicht einfach durch ein qualifiziertes IT-Department abwenden. Die Bildung von Awareness gilt als unverzichtbarer Schutz im beruflichen sowie privaten Umfeld. Um die Awareness zu Cyber-Bedrohungen und Cybersecurity zu steigern, hat die OCG in Zusammenarbeit mit der Universität Wien und der ICDL Foundation einen Syllabus erstellt, welcher die wichtigsten Themen für die Workforce beinhaltet. Über den ICDL (Europäischer Computer Führerschein) werden bereits seit vielen Jahren Zertifizierungen im Bereich Cybersecurity angeboten. Die jetzige Iteration hat das Ziel, den modernen Anforderungen von Cybersecurity gerecht zu werden. Die Universität Wien ist zurzeit in mehreren europäischen Projekten involviert, die sich mit Cybersecurity in Organisationen und der Vermittlung von Lerninhalten in diesem Bereich beschäftigen. Zu diesen Projekten zählen CS-AWARE-NEXT (https://cordis.europa.eu/project/id/101069543) und COLTRANE (https://coltrane.ait.ac.at/summary/), mit denen wir uns für diese Arbeit ausführlich ausgetauscht haben.

E-LEARNING ALS LÖSUNGSANSATZ

Doch wie kann man diese Inhalte effizient und effektiv in der Arbeitswelt (Workforce) vermitteln? Hiermit befasse ich mich in meiner Masterarbeit. Während meiner Recherchearbeiten hat sich E-Learning als Möglichkeit, Lehrenden Material flexibel zur Verfügung zu stellen, als Lösungsansatz herausgestellt. Im Gegensatz zum traditionellem Klassenraumtraining erlaubt es den Lernenden, Inhalte von einer präferierten Umgebung, zu einer präferierten Zeit und in einer präferierten Geschwindigkeit abzurufen. Doch damit ist es nicht getan. Die Aufbereitung des Materials spielt ebenfalls eine entscheidende Rolle zur Steigerung der Effizienz und Effektivität. Während der Recherchearbeiten und im für die Masterarbeit geltenden Rahmen haben sich vor allem folgende Kriterien zur Steigerung von Effizienz und Effektivität herausgestellt:

- **Modularität** umfasst die Aufteilung der Lernthemen in Module. Hierbei soll jedem Thema ein Modul gewidmet sein. Ein Modul soll aus verschiedenen Lektionen bestehen, welche einzelne Aspekte des Themas behandeln. Dies ermöglicht Lernenden eine klare Übersicht und Lernstruktur der zu lernenden Themengebiete. Ein wichtiger Aspekt hierbei ist die Unabhängigkeit der einzelnen Module. So können sich Lernende ungestört und unabhängig mit einem Themengebiet befassen. Um die Lerneffizienz weiter zu steigern, empfiehlt es sich, die Lektionen in Micro-Lektionen, welche nicht länger als 10 Minuten dauern, zu gestalten.
- **Klar definierte Ziele:** Zu Beginn jedes Moduls soll dessen Intention in klar definierten Zielen ausgedrückt werden. So wissen Lernende, was auf sie zukommt und ob sie die relevanten Inhalte verstanden haben.
- Die **Relevanz der Lerninhalte** muss für die Lernenden nachvollziehbar sein. Dies fördert ihre Motivation.
- **Interaktivität** mit dem Lerninhalt hilft, die Aufmerksamkeit der Lernenden und ihre Retentionsrate zu erhöhen.
- Kontinuierliches **Feedback** ermöglicht Lernende gleichzeitig Inhalte zu wiederholen und ihre Lernleistung zu evaluieren.
- **Storyboards:** Geschichtenerzählen gilt als eine der effektivsten Lernmethoden. Lernende haben die Möglichkeit, von den Erfahrungen anderer zu lernen, ohne selbst die Konsequenzen zu erfahren. Zusätzlich merken sich Lernende Fakten besser, wenn sie in einer Geschichte verpackt sind, als wenn sie als Liste präsentiert werden.

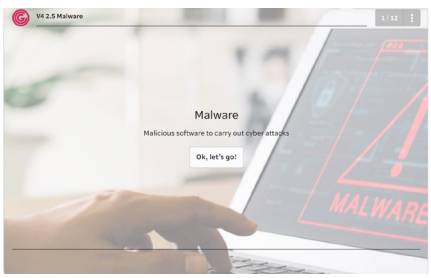
Wie effizient und effektiv der umgesetzte Lerninhalt ist, wird anhand der Faktoren Retention und Lernerfahrung evaluiert. Die Evaluierung der Retention erfolgt mithilfe eines Vor- und Nachtestes, welche die gleichen Fragen beinhalten. Der Vortest wird vor Bearbeitung des Moduls beantwortet, der Nachtest wird im Anschluss an die Bearbeitung ausgefüllt. Anhand der erreichten Verbesserung lässt sich die Effektivität des E-Learning Kurses ermitteln. Zur Evaluierung der Lernerfahrung füllen Lernende im Anschluss an das Lernmodul ein Fragebogen zur objektiven Bewertung verschiedener Aspekte aus.

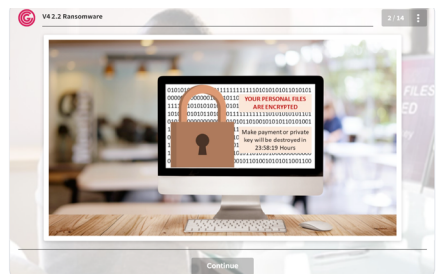
Die Testung erfolgt in mehreren Itera-

tionen: Eine erste Prototyptestung hat innerhalb der OCG stattgefunden. Die daraus aufkommenden Verbesserungen wurden bereits integriert. Eine weitere Testung wird im Rahmen mehrerer Lernveranstaltungen an der Uni stattfinden.

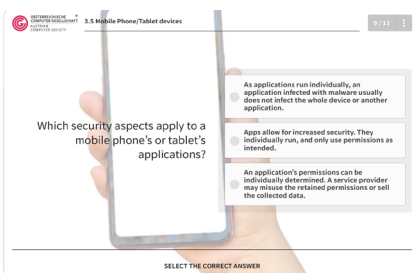
Das Ziel ist es, aus dieser Arbeit in Zusammenarbeit mit der ICDL Foundation einen internationalen Standard für Cybersecurity für Workforce Training und Zertifizierung zu entwickeln.

Bis Ende 2023 soll der Kurs und die Zertifizierung zusammen mit der ICDL Foundation angeboten werden können.





Klare Ziele sollen Lernenden die Intention der Lektion vermitteln. Die Relevanz der Lerninhalte wird mit Alltagsbeispielen beschrieben.



Interaktivität und Feedback sollen die Aufmerksamkeit von Lernenden stärken und ihre Retentionsrate erhöhen.

Storyboards verbessern die Lernerfahrung und helfen Lernenden, Inhalte besser aufzunehmen.

Celina Junghans, BSc, studiert an der Universität Wien im Master Wirtschaftsinformatik. Während ihres Bachelorstudiums an der Universität zu Köln hat sie als Softwareentwicklerin gearbeitet. Heute arbeitet sie neben ihrer Tätigkeit bei der OCG als Data Scientist bei einer Unternehmensberatung.

ICDL ist eine international anerkannte Zertifizierung für digitale Kompetenzen.

Mehr Informationen:

Demonstration einer Replay Attack

von Fatih Varli und Fabio Birnegger

Radio Hacking mit SDRs

Unsere Forschung beschäftigt sich mit Radio-Hacking mithilfe des Software Defined Radios ‚HACKRF One' und dem spezifischen Einsatz davon im kriminellen Umfeld. Im Rahmen der IT-S NOW 2022 Sicherheitskonferenz, demonstrierten wir live eine Replay Attacke. In der Demonstration wurde eine Alarmanlage, die durch eine wireless Fernbedienung aktiviert und deaktiviert werden kann, erfolgreich durch das Klonen des Signals ausgeschaltet.

ELEKTROMAGNETISCHE WELLEN

Elektromagnetische Wellen sind Schwingungen eines elektromagnetischen Feldes, die sich in Lichtgeschwindigkeit ausbreiten. Beispiele dafür sind Infrarotstrahlung, Röntgenstrahlung und UV-Strahlung. Die Wellen unterscheiden sich hauptsächlich durch die Frequenz und die Wellenlänge.

Funkwellen sind eine Art von elektromagnetischen Wellen und liegen im Frequenzbereich zwischen 10 kHz und 300 GHz. Sie werden zur Übertragung von Daten und Signalen verwendet.

FREQUENZBEREICHE

Es gibt standardisierte Frequenzbereiche (ISM-Bänder), in denen die meisten Anwendungen und Geräte eines bestimmten Typs operieren. Zum Beispiel liegen Alarmanlagen vor allem im Frequenzbereich zwischen 868 MHz und 870 MHZ.

SOFTWARE DEFINED RADIOS

Software Defined Radios (SDR) sind Geräte, die in der Lage sind, Radiosignale zu empfangen und zu senden. Die Hardware übernimmt dabei die beidseitige Umsetzung zwischen digitalem und analogem Signal. Die Signalverarbeitung wird durch Software realisiert. Diese übernimmt das Aufbereiten, Verarbeiten und Generieren von Signalen.

GNU RADIO COMPANION

Das Programmierwerkzeug GNU Radio Companion wird für die Digitale Signalverarbeitung (DSP) in Verbindung mit SDRs verwendet. In der grafischen Oberfläche wird ein gewünschter ‚Flowgraph' erstellt, welcher durch das Tool in Python Code umgewandelt wird. Die Hardware kann nun basierend auf diesem Code Signale empfangen oder aussenden.

Bei einer *Replay Attack* wird ein Radiosignal, das von einem legitimen Gerät (z. B. Fernbedienung) ausgesendet wird, aufgezeichnet, um es später wieder auszusenden und das legitime Gerät zu imitieren. Für die Attacke sind grundsätzlich drei Schritte nötig, welche folgend erklärt werden.

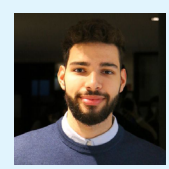
SCHRITT 1: Zuerst muss die Frequenz des Geräts ermittelt werden. Dies kann z. B. durch folgendes Vorgehen geschehen: Durch die, oben erwähnten, standardisierten Frequenzbereiche wird für ein bestimmtes Gerät eine Frequenz angenommen (z. B. Alarmanlagen zwischen 868 MHz und 870 MHz oder Funkfernbedienungen generell häufig auf 868 MHz). Dann wird durch das Verwenden von bestimmten Programmen die angenommene Frequenz verifiziert bzw. genau bestimmt.

SCHRITT 2: Das gewünschte analoge Signal wird aufgenommen und als digitales Signal in einer Datei abgespeichert. Für die Signalverarbeitung wird die Software GNU Radio Companion verwendet. In dem Programm legen wir die Frequenz fest, auf der wir das Signal mithören und aufnehmen wollen.

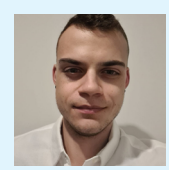
SCHRITT 3: Im letzten Schritt wird nun das aufgenommene Signal aus Schritt 2 ausgesendet. Es wird wieder GNU Radio Companion verwendet, um das Signal (Datei aus Schritt 2) und die Frequenz festzulegen.

ERGEBNISSE

Für den Versuch wurde ein HackRF One (SDR) als Gerät des Angreifers und eine Technaxx Alarmanlage als Gerät des Opfers verwendet. Die Alarmanlage kann durch eine mitgelieferte Fernbedienung aktiviert und deaktiviert werden. Das Signal zum Deaktivieren wurde aufgezeichnet und abgespeichert sowie, nach dem erneuten legitimen Aktivieren der Alarmanlage wieder ausgesendet. Der Versuch zeigte, dass die Alarmanlage tatsächlich durch das Aussenden des geklonten Signals deaktiviert wurde. Wir waren also in der Lage, das legitime Signal zur Deaktivierung erfolgreich zu klonen und die Fernbedienung zu imitieren.



Fatih Varli BSc studiert IT-Security (MSc) an der FH Campus Wien und arbeitet als Digital Forensiker. Er ist speziell im Bereich DFIR interessiert.



Fabio Birnegger BSc studiert IT-Security und arbeitet als Penetration Tester bei TÜV AUSTRIA. Er ist besonders an Software- und Cloud-Security interessiert.

Referenzen:

https://its-now.science/?review
https://elvis.science/?w=HackRF_One:_Setup

Übersicht der Preisträger*innen

1988

OCG Förderpreis

Mit dem OCG Förderpreis werden jedes Jahr die Verfasser*innen der besten Diplom/Masterarbeiten von Informatik-nahen Studienrichtungen an Österreichs Universitäten ausgezeichnet. 1988 wurde der Preis erstmals verliehen.

Der Preis ist heute mit EUR 2.000,- dotiert und kann auch geteilt werden. Bis heute wurden 46 Personen ausgezeichnet. Links sehen Sie die Namen der Preisträger*innen in alphabetischer Reihenfolge.

Gerald Bachmaier | Harald Beck | Robert Bill | Adam Celarek | Werner Dietl | Franz Franchetti | Philipp Frauenthaler | Christian Freude | Sebastian Gabmeyer | Markus Grabner | Andrei Grecu | Andreas Grimmer | Nicolas Grossmann | Bernd Hirschler | Patrick Huber | Christian Humer | Heinz Kantz | Theodorich Kopetzky | Gabriele Kotsis | Gerhard Kramler | Thomas Krennwallner | Thomas Kucera | Martin Lackner | Hans Wolfgang Loidl | Christian Mannes | Herwig Mayr | Michael Morak | Harald Nekvasil | Theresa Neubauer | Sebastian Neumaier | Fabio F. Oberweger | Maria Magdalena Ortiz de la Fuente | Roland Perko | Martin Plattner | Daniela Pohl | Axel Polleres | Thomas Reiter | Dietmar Schabus | Christian Schallhart | Wolfgang Schreiner | Ernst Schwartz | Johannes Sorger | Christoph Weinzierl-Heigl | Ingomar Wenzel | Alexander Wilkie | Christian Wimmer | Stefan Woltran

1985

Heinz Zemanek Preis

Anlässlich des 65. Geburtstages unseres Vereinsgründers und Computerpioniers Heinz Zemanek wird der erste Heinz Zemanek Preis ausgeschrieben.

Der Preis wird heute alle zwei Jahre an herausragende Disserationen, die an österreichischen Universitäten verfasst wurden, vergeben und ist mit EUR 5.000,- dotiert.

Bis heute wurden insgesamt 26 Personen mit dem Heinz Zemanek Preis ausgezeichnet. Die Namen der Preisträger*innen finden Sie rechts in alphabetischer Reihenfolge.

Keith Andrews | Alexander Felfernig | Alois Ferscha | Michael Fink | Daniel Gruss | Helwig Hauser | Daniela Kaufmann | Alfred Kobsa | Gabriele Kotsis | Andreas Krall | Sebastian Krinninger | Arnold Krommer | Eva Kühn | Peter Lang | Jan Mendling | Gustaf Neumann | Stefan Neumann | Marko Samer | Wolfgang Schwabl | Siegfried Selberherr | Wolfgang Slany | Markus Steinberger | Christoph Überhuber | Andreas Uhl | Thomas Würthinger | Alwin Zulehner

2008

OCG Förderpreis-FH

Mit dem OCG Förderpreis-FH werden die besten Informatik-nahen Masterarbeiten an Österreichs Fachhochschulen ausgezeichnet.

Der Preis ist mit EUR 2.000,- dotiert und wurde für 2008 das erste Mal ausgeschrieben. Bis heute zählen wir 16 Preisträger*innen, die Sie rechts in alphabetischer Reihenfolge finden.

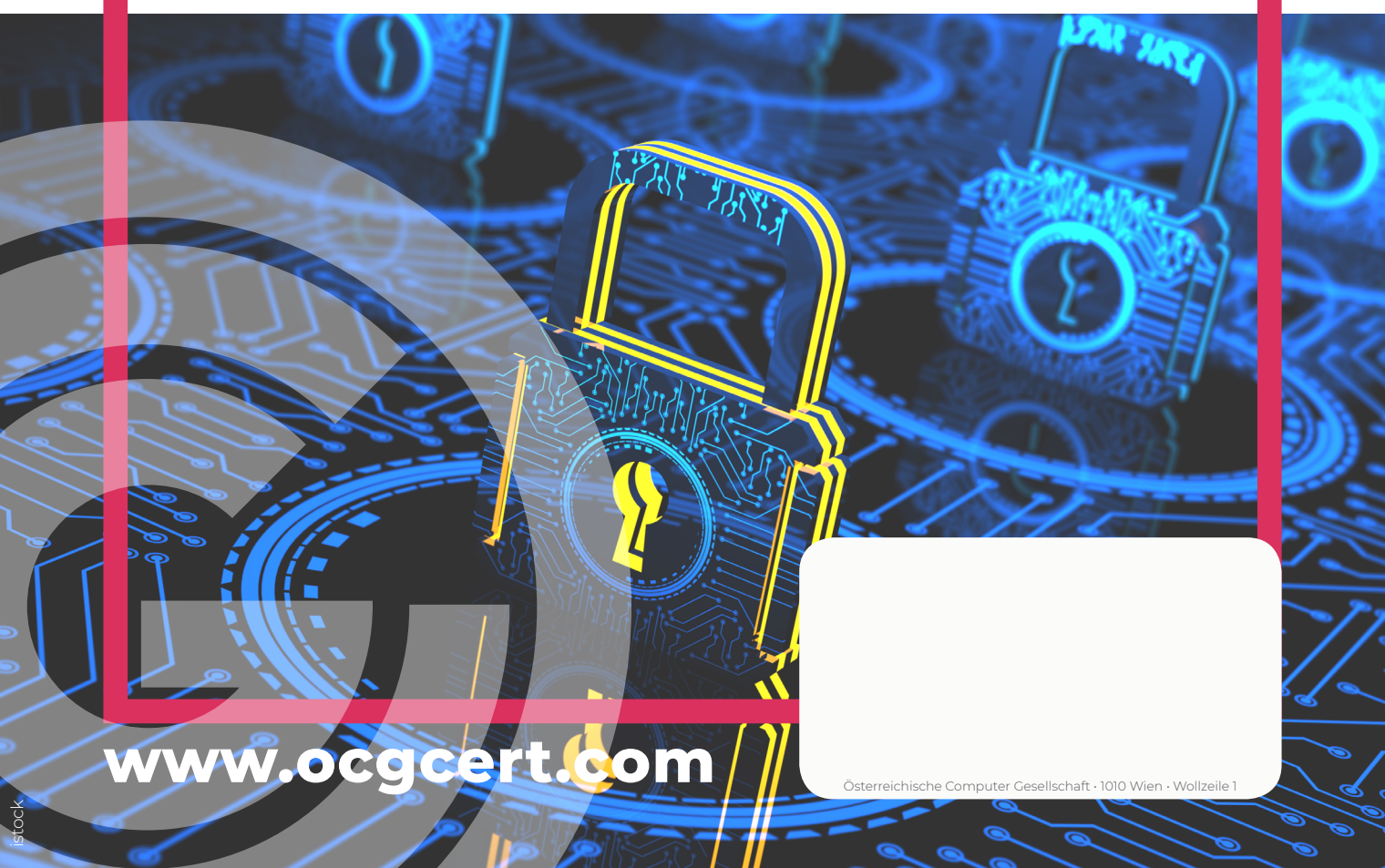
Christian Backfrieder | Benedikt Berger | Patricia Derler | René Draschwandtner | Rainhard Findling | Michael Kirchner | Georg Knabl | Günther Lanner | Lisa Obritzberger | Kathrin Probst | Jonathan Rameseder | Thomas Reinbacher | Stefan Schöberl | Tina Schuh | Kornelia Stoiber | Thomas Weiß

OESTERREICHISCHE COMPUTER GESELLSCHAFT®
AUSTRIAN COMPUTER SOCIETY

IT-Sicherheit zertifizieren

ISO/IEC 27001

Wir zertifizieren Ihre Informationssicherheit nach ISO/IEC 27001 und bieten als **Qualifizierte Stelle auch Prüfungen nach dem NISG an.**



www.ocgcert.com

Österreichische Computer Gesellschaft · 1010 Wien · Wollzeile 1