JKU LINZ INSTITUTE OF TECHNOLOGY

LIT SECURE AND CORRECT SYSTEMS LAB
TÄTIGKEITSBERICHT 2019-2020

Datum: 01. März 2021
Berichtszeitraum: April 2019 bis Dezember 2020

Leitung
Univ.-Prof. Dr.-Ing. Robert Wille
Univ.-Prof. DI Dr. René Mayrhofer
A. Univ.-Prof. DI Dr. Josef Küng

Professoren
Univ.-Prof. Dr. Armin Biere, Univ.-Prof. DI Dr. Alexander Egyed MSc,
Univ.-Prof. Dr. Daniel Große, o. Univ.-Prof. DI Dr. Dr. h.c. Hanspeter Mössenböck,
Univ.-Prof. Dr. Armando Rastelli, a. Univ.-Prof. DI Dr.Johannes Sametinger,
a. Univ.-Prof. DI Dr. Josef Scharinger

PostDocs
Mag.[a] Dr.[in] Dagmar Auer, Dr. Atif Mashkoor

DoktorandInnen
DI Lukas Burgholzer, DI Daniel Hofer, DI[in] Barbara Lehner, Gabriela Michelon MSc,
Omid Mir MSc, Aya Mohamed MSc, Dipl.Inf.[in] Sibylle Möhle-Rotondi,
DI Daniel Pekarek, Michael Riegler MSc, DI Philipp Schwarz, Hannes Sochor MSc

LAND OBERÖSTERREICH

Inhaltsverzeichnis

1. Einführung

Das LIT Secure and Correct Systems Lab ist eine interdisziplinäre Forschungsplattform der Johannes Kepler Universität Linz, welche Forschungen zu sicheren und korrekten IT-Systemen (Hardware wie auch Software) auf höchstem internationalen Niveau durchführt. Es ist *die* Adresse für sämtliche Aktivitäten im Bereich Sicherheit und Korrektheit an der JKU und soll die Kompetenz und Expertise von derzeit zehn Instituten aus zwei Fachbereichen bündeln, Synergien und Potentiale heben, junge Forscherinnen und Forscher fördern sowie als einheitlicher Ansprechpartner für außeruniversitäre Kooperationen (insbesondere mit der Industrie) dienen. Das Lab wird vom Land Oberösterreich gefördert.

Das Lab wurde im Frühjahr 2019 gegründet und im Herbst 2019 offiziell eröffnet. Nach dem Aufbau des Personals und der Etablierung der Strukturen des Labs sowie der damit verbundenen Graduiertenschule wurde mit der wissenschaftlichen Arbeit begonnen und erste gemeinsame Kooperationen wurden erfolgreich gestartet. Mittlerweile hat sich das Lab zu einem Hub entwickelt, in denen gemeinsam geforscht und publiziert wird sowie gemeinsame Projekte akquiriert und durchgeführt werden.

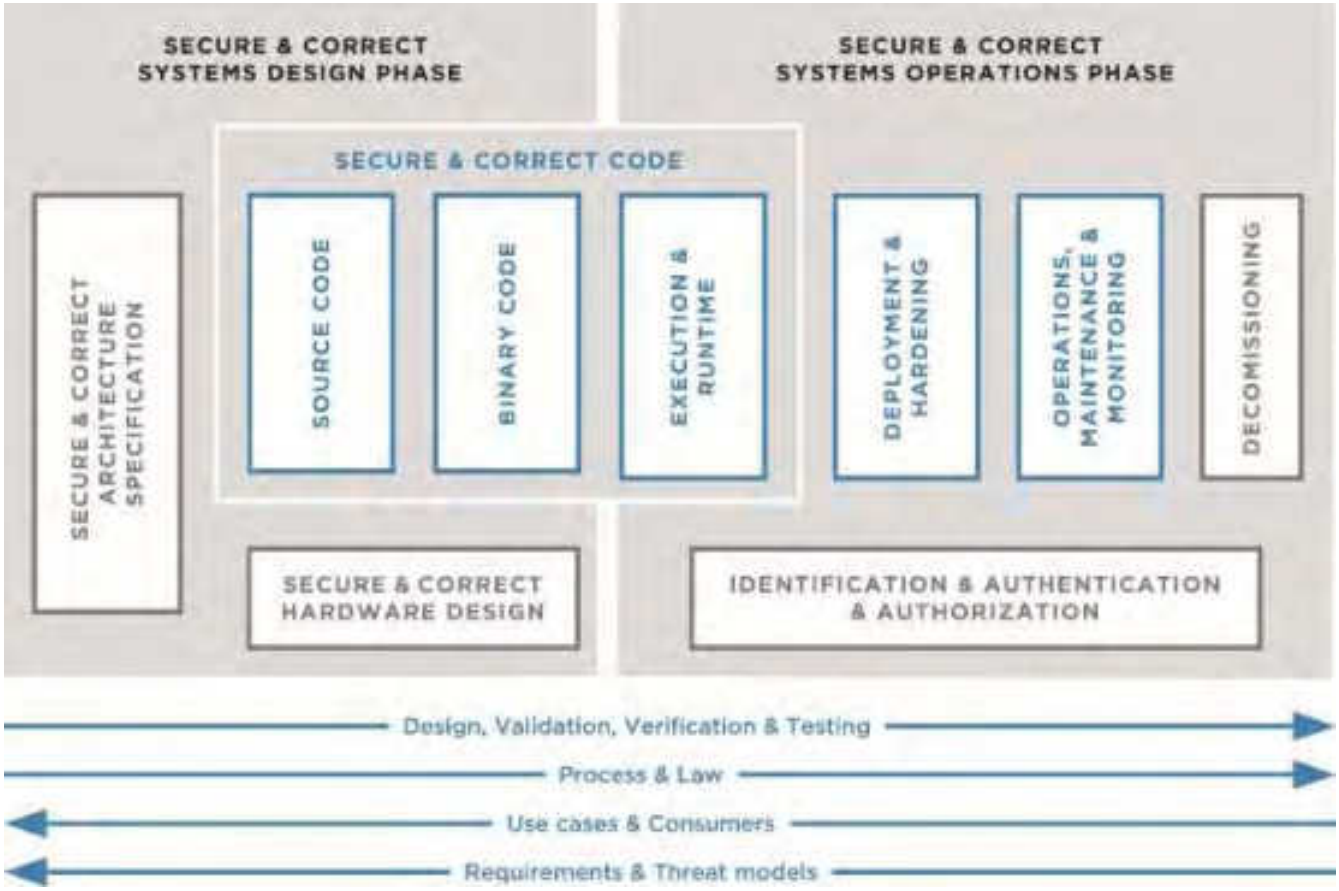
Dieser Bericht fasst den aktuellen Stand des Labs und die wesentlichen Aktivitäten im Zeitraum von April 2019 bis Dezember 2020 zusammen.

2. Kerndaten und Highlights

- Das LIT Secure and Correct Systems Lab bündelt die Aktivitäten und Expertise von derzeit zehn Instituten aus zwei Fachbereichen der Johannes Kepler Universität Linz.
- Es deckt die gesamte Kette der Erstellung und Verwendung sicherer und korrekter Systeme von der initialen Spezifikation bis zur finalen Realisierung sowie vom Beginn der Nutzung bis zur Außerbetriebnahme ab.
- Im Lab kooperieren derzeit zehn Professoren, zwei PostDocs und zehn DoktorandInnen (darunter ein weiblicher PostDoc und vier Doktorandinnen).
- Ein wesentlicher Pfeiler des Labs ist die Graduiertenschule mit einer strukturierten Doktoratsausbildung, die über die Standardanforderungen des Curriculums der JKU hinausgeht und Schwerpunkte auf klar definierte Meilensteine sowie eine Betreuung durch Teams anstatt durch Einzelpersonen setzt.
- Das Lab ist sehr publikationsaktiv: In weniger als zwei Jahren wurden aus dem Lab insgesamt 24 wissenschaftliche Arbeiten in Zeitschriften und 55 weitere wissenschaftliche Arbeiten in Tagungsbänden publiziert. Darunter auch zahlreiche gemeinsame Arbeiten mit der Industrie (z.B. mit Infineon, IBM, Google, Intel, Oracle Labs, etc.).
- Mitglieder des Labs treten in zahlreichen Funktionen für internationale Zeitschriften, Konferenzen sowie Workshops auf, organisieren Tutorials sowie Special Sessions und sind intensiv auf regionalen Veranstaltungen vertreten.
- Im Rahmen des LIT Labs konnten zahlreiche Projekte (z.B. LIT Seed-Projekte, ein ERC Consolidator Grant, drei FWF-Projekte, zwei EU-Förderungen, Direktaufträge z.B. von Google, ein Projekt mit der FH Hagenberg und weitere) erfolgreich eingeworben werden. Darüber hinaus kam ein Kooperationsvertrag mit der ENGEL GmbH zustande.
- Die im LIT Lab arbeitenden Personen wurden im Berichtszeitraum mehrfach ausgezeichnet (z.B. mit zahlreichen Medaillen bei Leistungsvergleichen, einem Best Poster and Interaction Award, einem Under-40 Innovators Award, einem Adolf-Adam-Informatikpreis, einem Best Student Contribution Award und weiteren).
- Zur offiziellen Eröffnung des LIT Secure and Correct Systems Lab am 17. Oktober 2019 erschienen circa 150 TeilnehmerInnen. Wirtschaftslandesrat Achleitner und Rektor Lukas eröffneten die Veranstaltung.
- Die Aktivitäten und Erfolge des Labs werden regelmäßig als "Aufhänger" genommen, um mit der Presse (und damit mit der Öffentlichkeit) ins Gespräch über unsere Arbeit zu kommen. Auf diesem Weg wurden bereits knapp 50 Artikel über uns in der Presse veröffentlicht (siehe auch Abschnitt 12).
- Das Lab ist eine enge Kooperation mit Partnern aus Hagenberg eingegangen. So konnten im Berichtszeitraum bereits gemeinsame Publikationen mit dem Software Competence Center Hagenberg (SCCH) veröffentlicht werden; mit der FH Hagenberg wurden Mittel für ein gemeinsames Doktoratsprojekt eingeworben und es wurde ein externer Doktorand vom SCCH in das Lab eingegliedert.
- Für eine noch stärkere Verbindung zwischen LIT Lab und dem SCCH sorgte die Ernennung von Prof. Robert Wille zum Chief Scientific Officer des Software Competence Center Hagenberg im Mai 2020.

3. Leitbild und Ziel des Labs

Das perspektivische Ziel des LIT Secure and Correct Systems Labs ist es, die gesamte Kette der Erstellung und Verwendung sicherer und korrekter Systeme von der initialen Spezifikation bis zur finalen Realisierung sowie vom Beginn der Nutzung bis zur Außerbetriebnahme abzudecken. Dabei sollen nicht nur Probleme von heute adressiert, sondern auch Lösungen für zukünftige Herausforderungen der kommenden Jahre und Jahrzehnte entwickelt werden. Die untenstehende Abbildung fasst die hierfür abzudeckenden Themen zusammen.



Diese unterteilen sich in Themen während des Entwurfs, während des Betriebs und darüber hinaus:

- *Während des Entwurfs (Secure & Correct Systems Design Phase)*
  - Fehler sollten so früh wie möglich im Entwurf ausgeschlossen bzw. entdeckt und behoben werden (idealerweise bereits bei der Spezifikation eines neuen Systems); außerdem sind bereits bei der Spezifikation Sicherheitsthemen mit zu berücksichtigen. Beides erfordert Secure & Correct Architecture Specifications, welche im Lab durch formale Methoden unterstützt werden.
  - Anschließend müssen sowohl Software als auch Hardware korrekt umgesetzt werden und höchsten Sicherheitskriterien entsprechen. Hier ist Expertise im Bereich der Programmierung und der Programmiersprachen (Source Code, Binary Code) aber auch im Hardware-Entwurf (Hardware Design) entscheidend. Im Lab wird explizit die Verbindung von der Spezifikation zur Implementierung sowie von der Implementierung zum Betrieb hergestellt und durch formale Methoden zur Verifikation über verschiedene Phasen unterstützt.
- *Während des Betriebs (Secure & Correct Systems Operations Phase)*
  - Ein sicheres und korrektes Funktionieren der entworfenen Systeme muss natürlich auch während des Betriebes sichergestellt werden. Nicht zuletzt da die Umgebung und die Konfiguration heutiger Systeme immer breiter wird bzw. sich regelmäßig ändert, bekommt die korrekte und sichere Ausführung von Systemen während des Betriebes eine stetig größere Bedeutung (Execution and Runtime). Damit einher geht eine entsprechende korrekte und sichere Inbetriebnahme sowie die spätere Absicherung gegen Fehler und Angriffe von außen (Deployment & Hardening).
  - Betrieb, Wartung und Überwachung der Systeme (Operations, Maintenance & Monitoring) auch gegenüber neu aufkommenden Fehlern oder Gefahren (inkl. sogenannter „Black Swan"-Ereignisse) sowie der Umgang mit den Systemen nach der Außerbetriebnahme (Decommissioning) sind weitere Themen, die zwar oft vernachlässigt werden, aber unabdinglich für ein ganzheitliches Vorgehen hinsichtlich Sicherheit und Korrektheit sind. Das Lab zielt darauf, in den vorhergehenden Phasen getroffene Annahmen bis hin zum Betrieb und der Überwachung zu verifizieren und damit auf nicht spezifizierte oder ungewöhnliche Zustände reagieren zu können.
  - BenutzerInnen-/System-/Hardware-Identifikation, Vergabe und Prüfung von Zugriffsrechten (Identification, Authenticitation & Authorization) stellen eine übergreifende Thematik im Betrieb von sicheren Systemen dar, die ebenfalls berücksichtigt werden müssen; sowohl im Entwurf als auch im Betrieb. Das Lab steht für einen ganzheitlichen Ansatz zur Identifikation und Authentifizierung von Systemkomponenten und -benutzerInnen.
- *Darüber hinaus*
  - Weiters müssen interdisziplinäre Fragen zu Validierung, Verifikation und Test (Validation, Verification & Testing), zu Fragen von Prozessen und rechtlichen Fragen (Process & Law), Fallstudien und AnwenderInnen (Use Cases & Consumers) sowie den entsprechenden Anforderungen und Gefahrenmodellen (Requirements & Threat Models) betrachtet werden.

In all diesen Bereichen bietet das Lab Forschungsleistungen auf höchstem internationalem Niveau. Es versteht sich als interdisziplinäre Forschungsplattform, welche die Aktivitäten und Expertise von derzeit zehn Instituten aus zwei Fachbereichen bündelt, Synergien und Potentiale hebt, junge Forscherinnen und Forscher fördert, sowie als einheitlicher Ansprechpartner für außeruniversitäre Kooperationen (insbesondere mit der Industrie) dient. In diesem Sinne ermöglicht das Lab auch eine Fokussierung auf die Schnittstellen zwischen den beschriebenen Phasen, die bisher eher vernachlässigt wurden.

Das Lab konzentriert sich dabei auf die folgenden zwei Säulen:

- Graduate School for Secure and Correct Systems
  Ein JKU Doktoratsprogramm an der Technisch-Naturwissenschaftlichen Fakultät (TNF) mit speziellem Fokus auf sichere und korrekte Systeme (siehe auch Abschnitt 5).

- Grundlagen- und anwendungsorientierte Forschung
  mit Partnern aus Industrie/Wirtschaft und Wissenschaft.

Das Lab wird vom Land Oberösterreich gefördert.

4. Beteiligte Institute und Personal

Am LIT Secure and Correct Systems Lab sind derzeit die Institute für

- Anwendungsorientierte Wissensverarbeitung,
- Wirtschaftsinformatik - Software Engineering,
- Computational Perception,
- Formale Modelle und Verifikation,
- Integrierte Schaltungen,
- Complex Systems,
- Netzwerke und Sicherheit,
- Halbleiter- und Festkörperphysik,
- Software Systems Engineering sowie
- Sytemsoftware

beteiligt.

Während diese Institute weiterhin eigenständig und selbstständig ihren jeweiligen Forschungsaktivitäten nachgehen, sollen im Lab Gelegenheiten zum Austausch und zur Nutzung von Synergien geschaffen werden. Um den hierfür nötigen Nukleus zu bilden, sind die beteiligten Institute derzeit mit zusätzlichen DoktorandInnen-Stellen ausgestattet. Zusätzlich wird das Lab durch eine PostDoc-Stelle sowie eine Assistentenstelle unterstützt. Die Leitung des Labs obliegt den Professoren Robert Wille (Institut für Integrierte Schaltungen), René Mayrhofer (Institut für Netzwerke und Sicherheit) sowie Josef Küng (Institut für anwendungsorientierte Wissensverarbeitung).

Mit Gründung des Labs im Frühjahr 2019 waren nahezu alle oben genannten Stellen noch unbesetzt. Demgemäß lag der Aufbau der Gruppe sowie entsprechendes "Teambuilding" im Fokus der ersten Wochen und Monate. Bei der Besetzung der Stellen wurde neben der fachlichen Exzellenz insbesondere auf die Eignung für interdisziplinäre Projekte geachtet. Außerdem sollten explizit Frauen für die zu besetzenden Stellen gewonnen werden.

Erfreulich ist, dass trotz des enormen Nachwuchsproblems und der starken Konkurrenz um "die besten Köpfe" sämtliche Stellen mit hochqualifizierten Personen besetzt werden konnten; darunter auch vier Doktorandinnen sowie ein weiblicher PostDoc (damit haben wir einen für MINT-Fächer überdurchschnittlichen Anteil an Doktorandinnen). Neben Österreich stammen die MitarbeiterInnen des Labs aus Ägypten, Brasilien, Pakistan, dem Iran, der Schweiz bzw. Italien und Deutschland.

Im Folgenden werden die beteiligten Institute, die für das LIT Lab entsprechend zuständigen Professoren sowie die im Lab arbeitenden PostDocs und DoktorandInnen kurz vorgestellt. Dabei wird die Breite der Themen und die Interdisziplinarität des Labs deutlich.

4.1. Institute

Institut für anwendungsorientierte Wissensverarbeitung

Daten - Information - Wissen sind die Kernbereiche des Instituts für anwendungsorientierte Wissensverarbeitung in der Lehre, Forschung und Entwicklung. Im Besonderen sind es aktuell wissenszentrierte Systeme, Qualitätsaspekte, Semantische Technologien, Web Retrieval, Data Mining, Workflows, Geschäftsprozesse und Sicherheitsaspekte. Gemeinsam mit dem LIT Secure and Correct Systems Lab fokussieren wir uns auf Sicherheitsaspekte in Informationssystemen, aktuell gerade auf Zugriffskontrollen für Graph-strukturierte Daten und Analyse von Log-Daten, um sicherheitsrelevante Ereignisse automatisch erkennen zu können.

Institut für Wirtschaftsinformatik – Software Engineering

Die Abteilung Software Engineering am Institut für Wirtschaftsinformatik sieht ihre Mission in Forschung und Lehre sowohl in der Wirtschaftsinformatik als auch im Software Engineering. Beide Bereiche werden als interdisziplinär gesehen, die technische, wirtschaftliche und soziale Inhalte integrativ betrachten. Es wird sowohl anwendungs- als auch grundlagenorientiert geforscht. Die Forschungsmethoden verfolgen einen ingenieurswissenschaftlichen Ansatz, d.h. am Beispiel startend, Design-orientiert und beschreibend hin zu Fundamentalem, Abstraktem und Erklärendem - in anderen Worten, von der Praxis zur Theorie. Der Großteil der Forschung geschieht in Zusammenarbeit mit universitären und außeruniversitären Forschungseinrichtungen sowie mit Partner-Unternehmen.

Institut für Computational Perception

Das Institut für Computational Perception untersucht und entwickelt rechnergestützte Modelle und Algorithmen, die es Computern erlauben, Aspekte der externen Welt erkennen und verstehen zu können. Somit fokussieren sich Forschung und Lehre auf Mustererkennung, Wissensextraktion, Data- und Text-Mining mit Methoden aus Bereichen wie Signalverarbeitung, Statistik-basierte Mustererkennung und Klassifikation, Machine Learning und Artificial- sowie Computational Intelligence im Allgemeinen. Die derzeitige Forschung konzentriert sich im Speziellen auf intelligente Audio- und Musik-Verarbeitung, Computer Vision, Biometrische Identifikation und Kryptographie.

Institut für formale Modelle und Verifikation

Das Institut für formale Modelle und Verifikation trägt mit der Forschung und Entwicklung von Werkzeugen für den Bereich Automatisiertes Schließen bei. Dieses Gebiet erstreckt sich von Logik über Künstliche Intelligenz und enthält im Besonderen die Unterstützung von Software- und Hardwareentwicklung. Die SAT-, SMT- und QBF-Solver des Instituts sind weltweit anerkannt und rangieren bei internationalen Vergleichen an der Spitze. Das Ziel ist grundlegende Basiskenntnisse und fortgeschrittenes Wissen zu lernen, damit Logik in allen Bereichen der Informatik und darüber hinaus angewandt werden können.

Institut für Integrierte Schaltungen

Das Institut für integrierte Schaltungen liefert Expertise für alle wesentlichen Schritte des Entwurfs und der Realisierung von integrierten Schaltungen, Embedded Systems und Cyber-Physical-Systems. Dies umfasst die Modellierung von entsprechenden Hardware- und Softwaresystemen in den frühen Phasen des Entwurfsprozesses und deren Umsetzung durch alle wesentlichen Abstraktionsstufen hinweg, wie dem Electronic System Level (ESL), dem Register Transfer Level (RTL), der Gatterebene und der Technologieabbildung auf die physische Ebene. Außerdem ist das Institut stark in der Entwicklung von Entwurfsmethoden für alternative und post-CMOS-Rechner involviert, wie etwa Microfluid-Systeme oder Quantencomputer.

Institut für Complex Systems

Das Institut für Complex Systems begegnet der immer größer werdenden Komplexität von Hardware/Software-Systemen durch den Einsatz von Virtuellen Prototypen auf Basis geeigneter Abstraktionen. Neben der Modellierung (entlang des kompletten Ablaufs bis hin zur Schaltungsimplementierung) liegt der primäre Forschungsschwerpunkt des Instituts auf der Verifikation, einem Hauptproblem im Bereich der Electronic Design Automation (EDA). Hier ist nicht nur die Korrektheit der Hardware, sondern insbesondere das Zusammenspiel von Hardware und Software die zentrale Herausforderung. Zur Demonstration der Lösungen werden moderne Designs auf Basis von RISC-V eingesetzt.

Institut für Netzwerke und Sicherheit

Das Institut für Netzwerke und Sicherheit bietet Expertise in der Analyse und dem Design von Sicherheits- und Datenschutzaspekten, auch in den Betriebssystem- und Netzwerk-Ebenen. Spezielle Schwerpunkte sind digitale Identitäten, Sicherheit in eingebetteten und mobilen Systemen sowie Netzwerkprotollsicherheit, Datenschutz und Privatsphäre.

Institut für Halbleiter- und Festkörperphysik

Das Institut für Halbleiter- und Festkörperphysik bietet Expertise in Wachstum, Nanofabrikation, Charakterisierung, Modifikation und Anwendung von halbleitenden Nanostrukturen und neuen Materialien. Für das LIT Secure and Correct Systems Lab sind vor allem die Arbeiten an hoch performanten Quellen für Quantenlicht (einzelne und Polarisations-verschränkte Photonen), geeignet für Kommunikation auf Quantenebene, relevant. Im Rahmen des Labs und eines laufenden LIT Projektes wurde eine Teststrecke für sichere Quantenkommunikation zwischen zwei Gebäuden (Halbleiterphysik und LIT Open Innovation Center) erfolgreich implementiert.

Institut für Software Systems Engineering

Das Institut für Software Systems Engineering entwickelt Theorien, Methoden und Werkzeuge für Spezifikation, Design, Implementierung, Tests, Monitoring und Evolution von großen und komplexen Softwaresystemen. Charakteristika solcher Systeme umfassen dezentralisierte Kontrolle, Unterstützung vieler Plattformen, inhärente, sich widersprechende Anforderungen, laufende Weiterentwicklung und Deployment sowie heterogene, inkonsistente und wechselnde Teile. Zusätzlich verfolgt das Institut Forschung im Bereich Modell-Driven-Engineering, Requirements-Engineering, Software Evolution, Software Monitoring, Variabilität und Produktlinien, Verifikation und Validation, Softwareprozesse und -Werkzeuge.

Institut für Sytemsoftware

Das Institut für Sytemsoftware arbeitet an Programmiersprachen, Compilern, virtuellen Maschinen und Performanzanalysen. Im Compiler-Bereich fokussiert sich das Institut auf dynamische Übersetzung (JIT-compilation), spekulative und Feedback-orientierte Compileroptimierung und selbst-optimierende Interpreter. In diesem Zusammenhang wird auch an Techniken gearbeitet, die eine sichere Ausführung von Programmen erlaubt, welche in einer grundsätzlich unsicheren Sprache, wie z.B. C/C++ oder Fortran, geschrieben wurden. Diese Arbeit kann als Forschung in Hinblick auf sicheren Code klassifiziert werden. Der Großteil der Forschung geschieht in Kooperation mit Oracle Labs. Die Ergebnisse sind nun Teil von Oracles Java HotSpotVM und Oracles Multi-Language-GraalVM mit ihren JIT-Compilern.

4.2. Professoren

Univ.-Prof. Dr.-Ing. Robert Wille

Robert Wille leitet das LIT Secure and Correct Systems Lab und das Institut für Integrierte Schaltungen. Seine Expertise liegt in der Entwicklung von Entwurfsmethoden für unterschiedlichste Anwendungsgebiete – mit einem speziellen Fokus auf dem Entwurf, der Verifikation und dem Test von Schaltkreisen und Systemen. Er berücksichtigt sowohl konventionelle als auch neu entstehende Rechnertechnologien wie Quantencomputer oder mikrofluidische Biochips. Er hat über 350 wissenschaftliche Beiträge für Zeitschriften und Konferenzen verfasst und wurde mehrmals ausgezeichnet.

Univ.-Prof. DI Dr. René Mayrhofer

René Mayrhofer leitet das Institut für Netzwerke und Sicherheit und das LIT Secure and Correct Systems Lab. Seine Hauptforschungsinteressen sind Digitale Identitäten, anwendbare sichere Systeme, Mobile Security und kryptographische Netzwerkprotokolle. Von 2017 bis 2019 war Mayrhofer Direktor der Android Plattform Security bei Google, wofür er weiterhin Berater für Android Security aktiv ist. Seit 2020 leitet René Mayrhofer das Christian Doppler Labor "Digidow".

a. Univ.-Prof. DI Dr. Josef Küng

Josef Küng ist außerordentlicher Universitätsprofessor am Institut für anwendungsorientierte Wissensverarbeitung. Seine Forschungsinteressen umfassen Informationssysteme, wissensverarbeitende Systeme und deren Sicherheitsaspekte. Regelmäßig lehrt er in diesen Bereichen und kann auf zahlreiche wissenschaftliche Publikationen und viele erfolgreiche Kooperationen mit Partnern aus der akademischen Welt, der Wirtschaft und Verwaltung verweisen. Er war und ist auch in die Organisation von wissenschaftlichen Konferenzreihen eingebunden, wie z.B. DEXA (Database and Expert Systems Applications) und FDSE (Future Data and Security Engineering).

Univ.-Prof. Dr. Armin Biere

Seit 2004 ist Armin Biere Vorstand des Instituts für formale Modelle und Verifikation an der JKU. Sein hauptsächliches Forschungsinteresse liegt in angewandten formalen Methoden mit dem Fokus auf der Entwicklung von effizienten SAT- und SMT-Beweisen. Er ist Autor von 208 Paper, ist in fünf Editorial Boards, hat fünf Konferenzen und viel andere Meetings organisiert, war in 150 Program Committees und hat 89 Medaillen in SAT, SMT und QBF-Wettbewerben gewonnen (davon 52 erste Preise).

Univ.-Prof. DI Dr. Alexander Egyed MSc

Alexander Egyed ist Full-Professor und Leiter des Instituts für Software Systems Engineering an der JKU. Er hat ein Doktorat von der University of Southern California, USA, war PostDoc am University College London, UK, und hat viele Jahre in der Industrie gearbeitet. Am meisten bekannt ist er für seine Arbeiten an der Modellierung von Software und Systemen, im Speziellen im Bereich Variabilität, Konsistenz und Verfolgbarkeit. Er hat über 200 referierte wissenschaftliche Buch-, Journal- und Konferenzbeiträge mit bislang über 5000 Zitierungen. Er wurde in Communications of the ACM, Springer Scientometrics und Microsoft Academic Search unter die Top-1% im Bereich Software Engineering gelistet. Zusätzlich wurde er IBM Research Faculty Fellow in Anerkennung seiner Leistungen für Konsistenzprüfung, erhielt einen Recognition of Service Award der ACM, Best-Paper-Awards von COMPSAC und WICSA sowie einen Outstanding Achievement Award der USC. Er diente als Program Chair/Steering Committee Member (ASE, FASE, MoDELS, ...) und als Editorial Board Member (TSE, SoSyM, ...). Er ist Mitglied bei IEEE, IEEE Computer Society, ACM und ACM SigSoft.

Univ.-Prof. Dr. Daniel Große

Daniel Große ist Professor und Leiter des Instituts für Complex Systems an der JKU. Er arbeitet auf dem Gebiet der Electronic Design Automation (EDA). Seine Forschungsinteressen umfassen (formale) Verifikation, Virtual Prototyping, Debugging und Synthese. Er hat drei Bücher und mehr als 140 Artikel in führenden internationalen Zeitschriften und Konferenzen veröffentlicht. Daniel Große war in Programmkomitees zahlreicher Konferenzen tätig, darunter ASP-DAC, DAC, DATE, ICCAD, CODES+ISSS, FDL und MEMOCODE. Außerdem erhielt er Best Paper Awards auf der FDL 2007, DVCon Europe 2018, ICCAD 2018 und FDL 2020.

o. Univ.-Prof. DI Dr. Dr. h.c. Hanspeter Mössenböck

Hanspeter Mössenböck ist Full-Professor der Informatik und Leiter des Instituts für Sytemsoftware an der JKU. Seine Forschungsinteressen sind Programmiersprachen, Compiler und virtuelle Maschinen. Im Rahmen seiner langjährigen Kooperation mit Oracle Labs arbeitet er an Techniken für die dynamische Optimierung von Programmen in JIT-Compilern und aggressiver Feedback-orientierter Optimierung. Weitere Forschungsgebiete sind statische und dynamische Programmanalysen, Anwendungsperformanz Monitoring, Softwarefehleranalyse und sicherer Code sowie Domain-spezifische Sprachen. Er ist Autor mehrerer Bücher über Java, C#, NET und Compilertechnik.

Univ.-Prof. Dr. Armando Rastelli

Armando Rastelli ist italienischer Physiker und Professor für Halbleiterphysik an der JKU, wo er die Halbleiterphysik-Gruppe und die Nanoscale-Halbleiter-Gruppe leitet. Zusammen mit seinem Team und externen Partnern fokussiert er sich auf die Herstellung von Halbleiter-Nanostrukturen mit Hilfe von epitaxalen Methoden, deren Beschreibung und physikalischen Verständnis, der Entwicklung von Methoden, mit denen die Eigenschaften präzise kontrolliert werden können, deren Integration in photonische Bauelemente sowie deren Nutzung als Quelle für Quantenlicht für Anwendungen in neu entstehenden Quantentechnologien.

a. Univ.-Prof. DI Dr. Johannes Sametinger

Johannes Sametinger ist Professor an der JKU am Institut für Wirtschaftsinformatik - Software Engineering. Seine Forschungsinteressen umfassen unterschiedliche Aspekte des Software Engineerings im Allgemeinen und Software Sicherheit im Speziellen. Er war mehrere Jahre an Universitäten in den USA (Texas A&M University, Brown University, University of Arizona) und Canada (University of Toronto, Université de Montréal). Neben der JKU arbeitete er auch in Deutschland an der Universität von Regensburg und gemeinsam mit Siemens in München.

a. Univ.-Prof. DI Dr. Josef Scharinger

Josef Scharinger ist außerordentlicher Universitätsprofessor am Institut für Computational Perception an der Johannes Kepler Universität Linz. Seine Arbeitsschwerpunkte sind Bildverarbeitung, Kryptographie und Biometrische Identifikation. Diese Technologien erlauben es, Methoden für sichere Kommunikation, Authentifizierung und Identifikation zu entwickeln.

4.3. PostDocs

Mag.ª Dr.in Dagmar Auer

Mag.ª Dr.in Dagmar Auer ist Senior Researcher mit einem JKU-Doktorat in Wirtschaftsinformatik im Fach Software Engineering und hat mehr als 25 Jahre Erfahrung in Forschung und Entwicklung im Bereich Software- und Data Engineering. Derzeit arbeitet sie an wissensintensiven Geschäftsprozessen in Kombination mit Graph-Modellen. Graphen sind in Hinblick auf hohe Flexibilität und Anpassbarkeit, die in solchen Geschäftsprozessen benötigt werden, vielversprechend, bergen aber auch neue Herausforderungen: unter anderem passende Konzepte für Autorisierung und Zugriffskontrolle.

Dr. Atif Mashkoor

Dr. Atif Mashkoor ist Senior Researcher am LIT Secure and Correct Systems Lab und am Software Competence Center Hagenberg (SSCH). Seine Forschungsinteressen sind rigorose Methoden und Software Engineering. Er hat umfangreiche praktische Erfahrung mit der Modellierung und Analyse von sicheren Systemen. Er war Gast-Editor der Februar 2018-Ausgabe des IEEE Software Magazins zum Thema "Safety und Security". Er ist Co-Chair des internationalen Workshops "Cybersecurity and Functional Safety in Cyber-Physical Systems (IWCFS)", hat ein Doktorat der Université de Lorraine, Frankreich, und einen Master-Abschluss der Universität Umeå, Schweden, in Computer Science. Zusätzlich hat er an der Rovira i Virgili Universität, Spanien, Computational Linguistic studiert.

4.4. Alumni

Dr. Daniel Huber

Dr. Daniel Huber arbeitete im Lab als PostDoc mit einem Doktorat in Physik. Seine Forschung fokussierte sich auf Halbleiter-Quantenpunkte. Das sind Nanostrukturen, die es erlauben "on demand" einzelne Photonen und verschränkte Photonenpaare zu generieren. Insbesondere zielte er darauf ab, Halbleiterpunkte als eine Verschränkungsquelle für die aufstrebende Quantentechnologie, wie z.B. Quantencomputer und Quantenkommunikationsnetzwerke, zu etablieren.

4.5. DoktorandInnen

DI Lukas Burgholzer

DI Lukas Burgholzer besitzt einen Master in Mathematik und einen Bachelor in Informatik. In seiner Arbeit kombiniert er seine Expertise aus beiden Disziplinen, um Methoden für den Entwurf von Quantencomputer zu entwickeln. Für diese Zukunftstechnologie wird er entsprechende Datenstrukturen und Algorithmen entwickeln, die es erlauben mit der enormen Komplexität umzugehen, die entsteht, wenn man mit dieser Art von Geräten arbeitet.

DI Daniel Hofer

DI Daniel Hofer hat Informatik studiert und den Schwerpunkt Netzwerke und Sicherheit gewählt. In seiner Masterarbeit arbeitete er an der Platzierung von unsichtbaren Wasserzeichen in Texten von Webseiten und implementierte einen Prototyp dazu. Zusätzlich hat er viel Erfahrung in der Analyse von Log-Dateien, mit dem Ziel sicherheitsrelevante Vorfälle zu erkennen.

DI^{in} Barbara Lehner

DI Barbara Lehner studierte Physik in Linz und absolvierte ihr Bachelor- und Masterstudium am Institut für Halbleiter- und Festkörperphysik in der Gruppe von Armando Rastelli. Mittlerweile ist sie Teil der Graduiertenschule des LIT Secure and Correct Systems Lab. Derzeit ist sichere Kommunikation ein wichtiges Thema. Quantenphysik bietet neue Möglichkeiten, um Kommunikationen abzusichern.

Gabriela Michelon MSc

Gabriela Michelon MSc ist Softwareingenieurin und ihr Forschungsinteresse sind konfigurierbare Systeme und deren Varianten, sowohl Softwareproduktlinien als auch Versionskontrollsysteme. Ihr Ziel ist einen systematischen Mechanismus zu finden, um die Wiederverwendung von Artefakten zu erleichtern, die auf Feature-orientierter Entwicklung basieren, um daraus Varianten sicher, korrekt und automatisch ableiten zu können.

Omid Mir MSc

Omid Mir MSc schloss sein Bachelorstudium in Informatik und sein Masterstudium in Information Security ab. Seine Forschungsinteressen umfassen verschiedene Aspekte der Kryptographie mit Fokus auf sichere Protokolle: Entwicklung neuer Kryptographie-Werkzeuge, Zero-Knowledge-Proofs, Data-Privacy mit Schwerpunkt auf Authentifizierungstechnologien, Anonymous Credentials (für digitale Identitäten) und sichere Berechnungen, Blockchains sowie Functional Encryption.

Aya Mohamed MSc

Aya Mohamed MSc arbeitete in ihrer Masterarbeit an der Integration von Satellitendaten in eine No-SQL-Datenbank unter Verwendung einer Micro-Service-Architektur. Das Bachelorstudium absolvierte sie in Embedded Systems. Nun arbeitet sie an der Sicherheit, im Speziellen an der Zugriffskontrolle, im Zusammenhang mit Graph-Datenbanken.

Dipl.Inf.in Sibylle Möhle-Rotondi

Der Fokus von Dipl.Inf.in Sibylle Möhle-Rotondi liegt hauptsächlich im exakten Propositional-Model-Counting mit einem Schwerpunkt auf formale Methoden. Sie erarbeitet Kalküle für Propositional-Model-Counting und verwandte Ansätze und zeigt deren Korrektheit im Zuge formaler Beweise, die sie anschließend in der Praxis evaluiert. Sie ist besonders an der Anwendung von Model-Counting und verwandten Techniken in einem breiten Feld interessiert. Dieses beinhaltet Hardware- und Softwareverifikation, Kryptographie, modellbasierte Diagnose, Produktkonfigurationen, aber auch Probablisitic Reasoning und Bayes'sche Netze in der medizinischen Diagnose und Planung.

DI Daniel Pekarek

Der Schwerpunkt der Arbeit von DI Daniel Pekarek liegt im Bereich der Compilertechnologie, um sicheren Code zu fördern, Programm-Anomalien zu erkennen und Sicherheitslücken zu finden. Dafür hat er einen x86-Interpreter entwickelt, mit dem er nun versucht, Online-Analysen durchzuführen, welche die ausgeführten Instruktionen aufzeichnen, um sie dann offline weiter analysieren zu können. Dabei wird vor allem daran gearbeitet, aus Low-Level-Informationen über den ausgeführten Maschinencode auf High-Level-Informationen der Programmlogik zu schließen, die für Sicherheitsanalysen wichtig sind.

Michael Riegler MSc

Michael Riegler MSc arbeitete nach Abschluss seines Wirtschaftsinformatik-Studiums (Schwerpunkt Software Engineering und Management) fünf Jahre für ENGEL, einem österreichischen Hersteller für Spritzguss-Maschinen. Sein Forschungsbereich umfasst Software-Sicherheit in cyber-physikalischen Systemen, wie medizinischen Geräten oder industriellen Systemen. Er ist besonders an Methoden und Werkzeugen interessiert, die es ermöglichen ein Gerät zu schützen, selbst wenn dessen ursprüngliche Sicherheitsmaßnahmen bereits überwunden wurden.

DI Philipp Schwarz

Die Arbeiten von DI Philipp Schwarz beschäftigen sich mit Fragestellungen aus dem Bereich der biometrischen Identifikation. Während er sich in seiner Masterarbeit mit Fingerabdruckerkennung befasste, konzentriert sich seine aktuelle Forschungsarbeit auf die Personenerkennung anhand der Gangart. Beim Entwickeln von Lösungen in diesen Bereichen greift er auf Methoden der Künstlichen Intelligenz, wie beispielsweise Neuronale Netzwerke, zurück.

Hannes Sochor MSc

Hannes Sochor MSc ist Doktorand mit einem Master in IT-Security von der Fachhochschule Hagenberg, wo er auch im Bereich Secure Software Analytics arbeitet. Seine Forschungsinteressen umfassen Grammatik-basiertes Fuzzing, wobei er versucht, Grammatik-Mining und Programmanalyse-Methoden einzubeziehen.

5. Strukturierte Doktoratsausbildung

Das LIT Secure and Correct Systems Lab wurde vor allem mit dem Ziel gegründet, für DoktorandInnen aus unterschiedlichen Fachbereichen eine interdisziplinäre Forschungsplattform zu bieten. Ein wesentlicher Pfeiler bildet dabei eine strukturierte Doktoratsausbildung, welche sich in einer Graduate School for Secure and Correct Systems manifestiert.

Die Graduiertenschule geht dabei über die Standardanforderungen des Curriculums der JKU für Doktoratsstudien hinaus und setzt Schwerpunkte in der strukturierten Ausbildung mit klar definierten Meilensteinen sowie einer Betreuung durch Teams anstatt durch Einzelpersonen.

Die generelle Laufzeit des Doktoratsstudiums in der Graduiertenschule ist mit vier Jahren angesetzt. Typischerweise sind die DoktorandInnen dabei am LIT Secure and Correct Systems Lab angestellt; allerdings ist das Programm auch offen für andere Studierende. Die Betreuung erfolgt wie erwähnt durch Teams (in der Regel zwei Professoren). Auf diese Weise wird sichergestellt, dass stets eine interdisziplinäre wissenschaftliche Unterstützung gewährt werden kann und das den DoktorandInnen direkt zur Verfügung stehende akademische Netzwerk wird deutlich vergrößert. Im Laufe der vier Jahre Laufzeit sind die folgenden Meilensteine geplant:

- Proficiency Exam: Der erste große Meilenstein, bei dem der/die DoktorandIn und der Forschungsplan, der in einem Exposé beschrieben und öffentlich vorgetragen werden muss, evaluiert wird. Unmittelbar nach dem positiven Abschluss wird die Dissertationsvereinbarung vorbereitet, unterschrieben und beim JKU-Prüfungs- und Anerkennungsservice eingereicht.

- Midterm Evaluations: Nach dem zweiten Jahr muss der/die DoktorandIn einen kurzen Bericht über den Status der Arbeit, erreichte Zwischenergebnisse und den weiteren Plan der Leitung der Graduate School vorlegen. Gemeinsam mit dem Betreuungsteam prüft die Lab-Leitung diesen Bericht und startet, wenn notwendig, korrigierende Aktivitäten.

- Pre-Defense. Nach dem dritten Jahr, ungefähr ein Jahr vor dem geplanten Ende des Doktorats, muss der/die DoktorandIn den aktuellen Stand der Dissertation öffentlich vor der gesamten Faculty präsentieren. Ziel ist es dabei, eine Pre-Defense zu veranstalten, in der die Studierenden und die Betreuungsteams erkennen können, ob ein Abschluss binnen eines Jahres möglich ist bzw. welche essentiellen Teile noch fehlen. Die Studierenden bekommen ein entsprechendes schriftliches Feedback.

- Einreichung und Begutachtung: Am Ende wird entsprechend dem offiziellen JKU-Regulativ die Arbeit eingereicht und begutachtet.

- Präsentation und Verteidigung: Nach erfolgreicher Begutachtung hat der/die DoktorandIn die Arbeit öffentlich zu präsentieren und zu verteidigen – ebenfalls entsprechend dem JKU-Regulativ für alle Dissertationen.

Die ersten Proficiency Exams der Graduierteschule fanden am 20.10.2020 sowie 27.11.2020 statt. Dabei wurden die folgenden Promotionsverfahren erstmalig begutachtet und entsprechende Betreuungsteams gebildet:

DoktorandIn	Titel Exposé	Supervisor-Team
Lukas Burgholzer	*Efficient and Correct Compilation of Quantum Circuits*	Robert Wille Armando Rastelli
Daniel Hofer	*Using Graph Databases for System Log Processing*	Josef Küng René Mayrhofer
Barbara Lehner	*Gallium-Arsenide Quantum Dots: A stable and reliable source of entangled photon pairs on demand?*	Armando Rastelli Robert Wille
Gabriela Michelon	*Evolving System Families in Space and Time*	Alexander Egyed Paul Grünbacher
Omid Mir	*Cryptographic Protocols for Privacy-Preserving Access Control*	René Mayrhofer Josef Scharinger
Aya Mohamed	*Access Control in the Context of Graph-Structured Data*	Josef Küng Johannes Sametinger
Daniel Pekarek	*Architecture Agnostic Type Recovery*	Hanspeter Mössenböck René Mayrhofer
Michael Riegler	*Mode-Switching for Smart Security*	Johannes Sametinger René Mayrhofer
Philipp Schwarz	*Robust Gait Recognition using 2D and 3D Information*	Josef Scharinger René Mayrhofer

Im Vorfeld der Proficiency Exams wurden entsprechende Exposés erstellt. Die Präsentationen des Dissertationsvorhabens, der Stand der Forschung in diesem Bereich, der aktuelle Status der eigenen Arbeit und der weitere Plan erfolgte dann vor der gesamten Faculty und den zusätzlichen Zweitbetreuern. Im Anschluss jeder Präsentation wurden den DoktorandInnen sehr konstruktiv von der anwesenden Professorenschaft Rückmeldungen und Vorschläge gegeben. In der darauffolgenden Faculty-Sitzung konnte problemlos für jeden/jede DoktorandIn das Proficiency-Exam als bestanden gewertet werden. Obwohl wie vorgesehen keine Noten vergeben wurden, kann berichtet werden, dass alle Exams qualitativ im oberen Bereich angesiedelt waren.

6. Wissenschaftliche Beiträge

Neben der Graduiertenschule steht die wissenschaftliche Arbeit im Fokus des LIT Secure and Correct Systems Labs. Dies zeigt sich insbesondere in der Publikation wissenschaftlicher Ergebnisse aus dem Lab sowie der Mitwirkung an der Organisation wissenschaftlicher Events.

6.1. Publikationstätigkeit

Obwohl ein Großteil der Stellen erst ab der 2. Hälfte 2019 besetzt wurden, konnte sich das Lab bereits in kurzer Zeit als außerordentlich publikationsaktiv erweisen. So wurden insgesamt 24 wissenschaftliche Arbeiten in Zeitschriften und 55 wissenschaftliche Arbeiten in Tagungsbänden veröffentlicht (dabei werden nur Publikationen gezählt, die im Rahmen des Labs erstellt wurden bzw. hiervon profitiert haben; darüber hinaus haben die jeweiligen Institute deutlich mehr wissenschaftliche Arbeiten erstellt). Diese außerordentlich erfolgreiche Publikationstätigkeit in international renommierten Organen unterstreicht die wissenschaftliche Stärke der beteiligten Institute in diesen Gebieten.

Dabei wurden unter anderem Themen aus dem Bereich des Tests von Schaltungen und Systemen, der Sicherheit von (medizinischen) cyber-physikalischen Systemen, der Erkennung von Seiteneffekten sowie der Konsistenzprüfung von Systemmodellen, der Anwendung von Datenbanken sowie Expertensystemen, der Lösung von so genannten Erfüllbarkeitsproblemen mit Hilfe von SAT-Beweisern (einer grundlegenden Methode für viele heutige Korrektheits- und Sicherheitsnachweise) und des Entwurfs von Quantencomputern sowie der Realisierung von Quantenverschlüsselung (d.h. zukünftiger Sicherheitstechnologien) behandelt. Besonders erwähnenswert ist/sind dabei

- die Arbeit von S. Möhle und A. Biere mit dem Titel "Combining Conflict-Driven Clause Learning and Chronological Backtracking for Propositional Model Counting" (GCAI 2019), die mit einem Best Poster and Interaction Award ausgezeichnet wurde,
- die Arbeit von S. Pointner, O. Frank, C. Hazott und R. Wille mit dem Titel "Test Your Test Programs Pre-Silicon: A Virtual Test Methodology for Industrial Design Flows" (ITC-Asia 2019), die in Kooperation mit der Infineon AG Linz entstanden ist,
- die Arbeit von S. Hartmann, J. Küng, S. Chakravarthy, G. Anderst-Kotsis, A M. Tjoa und I. Khalil mit dem Titel "Database and Expert Systems Applications", die institutsübergreifend sowie in Zusammenarbeit mit dem Software Competence Center Hagenberg (SCCH) entstanden ist,
- die Arbeit von Kotsis, Gabriele, A Min Tjoa, Ismail Khalil, Lukas Fischer, Bernhard Moser, Atif Mashkoor, Johannes Sametinger, Anna Fensel, and Jorge Martinez-Gil, eds. Database and Expert Systems Applications: DEXA 2020 International Workshops BIOKDD, IWCFS and MLKgraphs, Bratislava, Slovakia, September 14-17, 2020, Proceedings. Vol. 1285. Communications in Computer and Information Science. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-59028-4, die ebenfalls institutsübergreifend sowie in Zusammenarbeit mit dem Software Competence Center Hagenberg (SCCH) entstanden ist,
- die Arbeit von A. Zulehner, S. Hillmich und R. Wille mit dem Titel "How to Efficiently Handle Complex Values? Implementing Decision Diagrams for Quantum Computation"

(ICCAD 2019), die auf einer ohnehin bereits sehr kompetitiven Tagung für den Best Paper Award nominiert wurde,

- die Arbeit von A. Mashkoor, A. Egyed und R. Wille mit dem Titel "Model-driven Engineering of Safety and Security Systems: A Systematic Mapping Study" (derzeit als Preprint), die eine umfassende Literaturstudie zum Thema des modelgetriebenen Entwurfs von korrekten und sicheren Systemen bietet und unter anderem eine Grundlage eines gemeinsamen Forschungsantrages bildet,
- zahlreiche Arbeiten u.a. von L. Servadei, W. Ecker, und R. Wille, die in Kooperation mit der Infineon AG München entstanden sind und von der eine auf dem „Workshop on Machine Learning for CAD" (MLCAD 2020) für den Best Paper Award nominiert wurde,
- die Arbeit von L. Burgholzer, R. Raymond, und R. Wille mit dem Title "Verifying Results of the IBM Qiskit Quantum Circuit Compilation Flow" (QCE 2020), die in Kooperation mit IBM Tokio entstanden ist,
- die Arbeit von C. G. Almudever, L. Lao, R. Wille, und G. G. Guerreschi mit dem Titel "Realizing Quantum Algorithms on Real Quantum Computing Devices" (DATE 2020), die in Kooperation mit der TU Delft und Intel entstanden ist,
- die Arbeit von D. Pekarek mit dem Titel "trcview: Interactive Architecture-agnostic Execution Trace Analysis" (MPLR 2020), die in Kooperation mit Oracle Labs entstanden ist,
- die Arbeit von Christian Schimpf, Marcus Reindl, Daniel Huber, Barbara Lehner, Saimon F. Covre Da Silva, Santanu Manna, Michal Vyvlecka, Philip Walther, Armando Rastelli mit dem Titel "Quantum cryptography with highly entangled photons from semiconductor quantum dots", die am 13.02.2020 in *Science Advances* aufgenommen wurde,
- die Arbeit von Evgeny A Chekhovich, Saimon F Covre da Silva, Armando Rastelli mit dem Titel "Nuclear spin quantum register in an optically active semiconductor quantum dot", die in *Nature Nanotechnology* publiziert wurde.

Eine komplette Auflistung aller Publikationen, die im Rahmen des LIT Secure and Correct Systems Labs veröffentlicht wurden (und auch eine entsprechende Bestätigung enthalten[1]), findet sich in Form einer Kopie der entsprechenden Forschungsdokumentation im Anhang.

6.2. Organisation wissenschaftlicher Events

Mitglieder des Labs treten für Zeitschriften und auf Konferenzen sowie Workshops in zahlreichen Funktionen in Erscheinung.

Besondere Aufmerksamkeit erhielt die Organisation der ACM WiSec 2020 (https://wisec2020.ins.jku.at/), einer international wichtigen Security-Konferenz mit dem Fokus auf drahtlose und mobile Kommunikation mit langjähriger Geschichte. Das Institut für Netzwerke und Sicherheit organisierte gemeinsam mit dem LIT Secure and Correct Systems Lab im Juli 2020 die physisch an der JKU Linz geplante, aber pandemiebedingt virtuell durchgeführte, Konferenz mit 55 Beiträgen und knapp 200 Teilnehmern aus 18 Ländern.

[1] Sämtliche Arbeiten, welche im Rahmen bzw. durch Unterstützung des Labs entstanden sind, enthalten das folgende "Acknowledgement": „This work has been supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria."

ACM WiSec 2020 war dabei eine der ersten Konferenzen, die kurzfristig auf vollständig virtuelle Abhaltung umstellte und dient als organisatorisches Muster für andere Security-Konferenzen. ACM WiSec 2021 wird, ebenfalls unter organisatorischer Beteiligung von LIT Secure and Correct Systems Lab Mitgliedern, nach selben Vorbild wiederum virtuell abgehalten.

Äquivalent wurde ebenfalls das dritte Android Security Symposium mit 13 Vorträgen – u.a. von ARM, Google und Qualcomm – und knapp 300 Teilnehmern aus 40 Ländern veranstaltet. Die virtuelle Abhaltung mit kostenloser Teilnahme machte dieses Symposium damit zum bisher größten in der Serie.

Weitere Aktivitäten sind im Folgenden gelistet:

- Atif Mashkoor und Johannes Sametinger organisierten im August 2019 und im September 2020 den International Workshop on Cyber-Security and Functional Safety in Cyber-Physical Systems (IWCFS).
- Josef Küng war als Co-Program-Chair der International Conference Future Data and Security Engineering (FDSE), also Program Committee Co-Chair der 31st International Conference on Database and Expert Systems Applications sowie als Mitglied des Steering Commitees der International Conference on Advanced COMPuting and Applications (ACOMP) tätig.
- Robert Wille ist Mitglied des Leitungsgremiums in Europas führender Tagung und Messe im Bereich des Schaltungs- und Systementwurfs (der Design Automation & Test in Europe, DATE). Zudem ist er Mitherausgeber der Zeitschriften IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD) sowie Integration, the VLSI Journal. Darüber hinaus hat er einige Special Sessions und Tutorials in internationalen Tagungen organisiert.
- Im Februar 2020 organisierten Armando Rastelli und Gunther Springholz die 21. "Winter School on new developments in Solid State Physics" in Mauterndorf.

Darüber hinaus sind nahezu alle führenden Personen des Labs aktiv in Programmkomitees tätig und leisten signifikante Gutachtertätigkeit für Zeitschriften, öffentliche Mittelgeber und Promotionen an anderen Universitäten.

7. Projekte und Kooperationen

Die Etablierung von Kooperationen (insbesondere mit der Industrie) sowie die Einwerbung von Projekten sind neben der wissenschaftlichen Tätigkeit ein weiterer Schwerpunkt des Labs. Im Folgenden werden einige Projekte am LIT Secure and Correct Systems Lab kurz vorgestellt.

7.1. EQKD-QD - Entanglement-Based Quantum Key Distribution with On-Demand Photons Generated by Semiconductor Quantum Dots

---

JKU PIs: Armando Rastelli, Robert Wille
Förderung: LIT, State of Upper Austria / SEED
Förderungszeitraum: 01.02.2019 – 31.10.2021
JKU Budget: 199.040 Euro

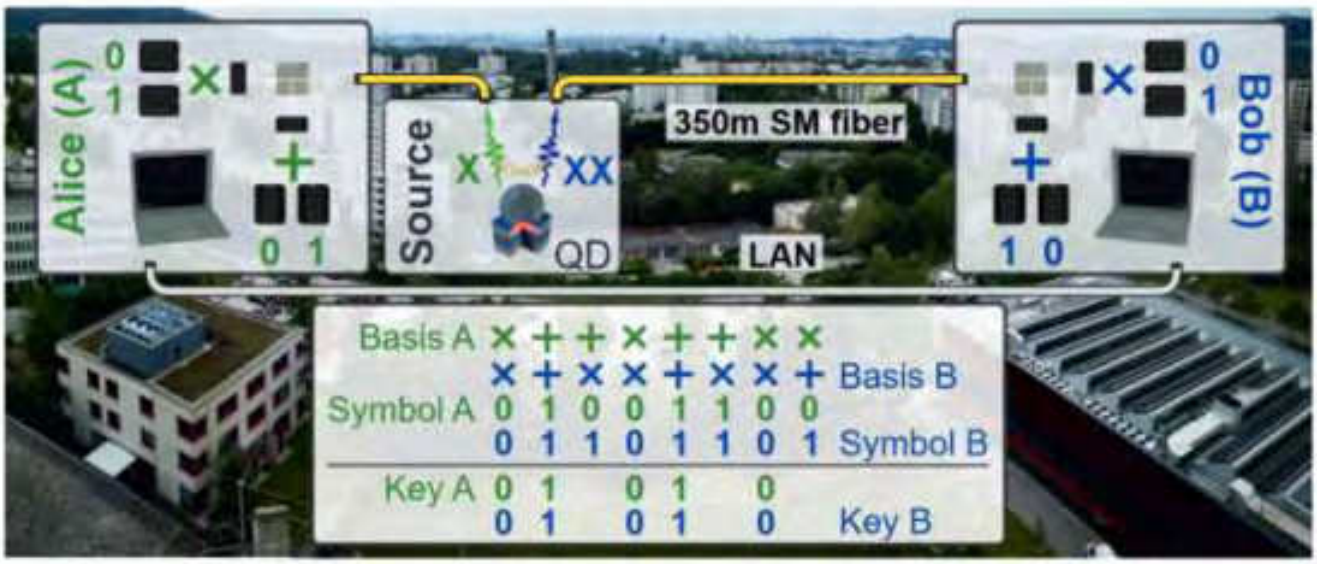
Die auf den Quantenschlüsselaustausch (QKD) basierende Quantenkryptographie gilt als eine der vielversprechendsten Strategien zur Gewährleistung einer absolut sicheren Datenkommunikation. Unter den verschiedenen QKD-Protokollen sind solche, die auf verschränkten Photonenpaaren basieren, aufgrund der erhöhten Toleranz gegenüber Verlusten und der vereinfachten Analyse der sicheren Schlüssel besonders attraktiv. Trotz beeindruckender Erfolge, zu denen die Implementierung von satellitengestützter QKD gehört, ist die maximale Übertragungsrate immer noch bescheiden, was teilweise auf die intrinsischen Einschränkungen der Quellen verschränkter Photonenpaare nach dem Stand der Technik zurückzuführen ist.

In diesem Projekt wollen wir zum ersten Mal halbleiterbasierte Quellen für polarisationsverschränkte Photonenpaare verwenden, um verschränkungsbasierte QKD mit Übertragungsraten zu implementieren, die weit über den Stand der Technik hinausgehen. Um dieses ehrgeizige Ziel zu erreichen, werden wir eine von der JKU patentierte Technologie verwenden, die es uns kürzlich ermöglicht hat, nahezu perfekt verschränkte Photonenpaare aus einer speziellen Klasse von Halbleiterquantenpunkten zu erhalten. Im Gegensatz zu den bisher verwendeten Quellen können Quantenpunkte Photonenpaare mit GHz-Raten und eine vernachlässigbare Wahrscheinlichkeit einer unerwünschten gleichzeitigen Erzeugung mehrerer Paare erreichen.

Zu den spezifischen Zielen des Projekts gehört der Entwurf und die Implementierung eines QKD-Systems zum Nachweis des Prinzips, bei dem ausschließlich Quantenpunktphotonen zur Erzeugung eines geheimen Schlüssels verwendet werden. Das System besteht aus einer stationären Quantenpunktquelle in unserem Labor und zwei Sender/Empfänger-Einheiten, die über Single-Mode-Fasern mit der Quelle verbunden sind. Diese Konfiguration ermöglicht es uns, die Übertragung unter Laborbedingungen und auf dem gesamten JKU-Campus zu analysieren. Um das Design und die Montage aller erforderlichen optischen-, elektronischen- und Softwarekomponenten zu vereinfachen, werden wir Designautomatisierungsmethoden für ausgewählte Aufgaben und

Simulationsansätze zur frühzeitigen Validierung anwenden. Dies ermöglicht uns eine schnelle Konvergenz zu einem voll funktionsfähigen bidirektionalen Punkt-zu-Punkt-QKD-System.

Durch die Quantifizierung der Qubit-Fehlerraten und Gesamtübertragungsraten von Quantenpunktquellen für verschränkungsbasierte QKD soll dieses Projekt die weitere Optimierung der Quellen leiten, ihre Grenzen erkunden und möglicherweise den Weg zur „realen Welt" ebnen.



7.2. Kooperation mit der ENGEL Austria GmbH

JKU-PI: a. Univ.-Prof. Dipl.-Ing. Dr. Johannes Sametinger
Förderung: ENGEL Austria GmbH
Förderungszeitraum: 01.08.2019 - 31.07.2023
JKU-Budget: 60.000 Euro

Das LIT Secure and Correct Systems Lab der JKU kooperiert mit dem weltweit tätigen Maschinenbauer ENGEL Austria GmbH im Bereich Cybersecurity and Functional Safety in Cyber-Physical Systems. ENGEL ist Hersteller von Spritzgießmaschinen und dazugehörigen Automatisierungsanlagen und hat eine Exportquote von über 90%. Fokus der Kooperation ist der Schutz der zunehmend vernetzten Systemarchitektur der Maschinenanlagen vor Bedrohungen durch Sicherheitsvorfälle.

ENGEL bietet Spritzgießlösungen für Automobilkomponenten, Bauteile für Elektro- und Elektronikprodukte, Haushaltswaren, Spiel- und Freizeitartikel, Verpackungen sowie für Medizintechnikprodukte. Dazu unterstützt ENGEL seine Kunden bei der Digitalisierung ihrer Fertigungsprozesse mit einer Reihe von smarten Lösungen, die eine Vernetzung der ENGEL Anlagen voraussetzen. Durch die Vernetzung eröffnen sich neue Möglichkeiten der

Datenanalyse, um ein noch tieferes Verständnis für den Spritzgießprozess und das Systemverhalten zu bekommen.

Auf dieser Grundlage entwickelt ENGEL weitere Lösungen mit dem Ziel, den Kunden in Zukunft noch besser zu unterstützen und das volle Potential der Spritzgießmaschinen und Produktionszellen auszuschöpfen.

Am Ende geht es um mehr Effizienz, eine höhere Qualität und damit um eine verbesserte Wettbewerbsfähigkeit der Kunden von ENGEL.

Datensicherheit und der Schutz von Betriebs- und Geschäftsgeheimnissen spielen bei der umfassenden Verknüpfung und Vernetzung von Technologien und Geschäftsprozessen (Industrie 4.0) eine Schlüsselrolle. Die Öffnung und Vernetzung bisher weitestgehend geschlossener Systeme bieten zahlreiche Chancen rund um Funktion und Flexibilität. Zunehmende Vernetzung, insbesondere über das Internet, erhöht aber auch das Angriffspotenzial von außen. Das LIT Secure and Correct Systems Lab der JKU bringt hier ihre Kompetenz und ihre Expertise ein. Bereits bei der Entwurfsphase von Hard- und Software hat Sicherheit eine große Bedeutung. Durch Bedrohungsmodellierung und Risikoanalysen werden systematisch mögliche Angriffe identifiziert, Risiken bewertet und entsprechende Gegenmaßnahmen eingeleitet. Während des Betriebes soll ein sicheres und korrektes Funktionieren sichergestellt werden mit dem Ziel einer automatisierten Detektion und Abwehr von Cyberangriffen auf die Maschinen- und Edge-Device-Software von ENGEL.

7.3. Quantenphotonik auf einem Chip für komplexe Quantennetzwerke

JKU PI: Armando Rastelli
Förderung: FWF / DACH
Förderungszeitraum: 01.10.2019 - 30.09.2022
JKU Budget: 290.950 Euro

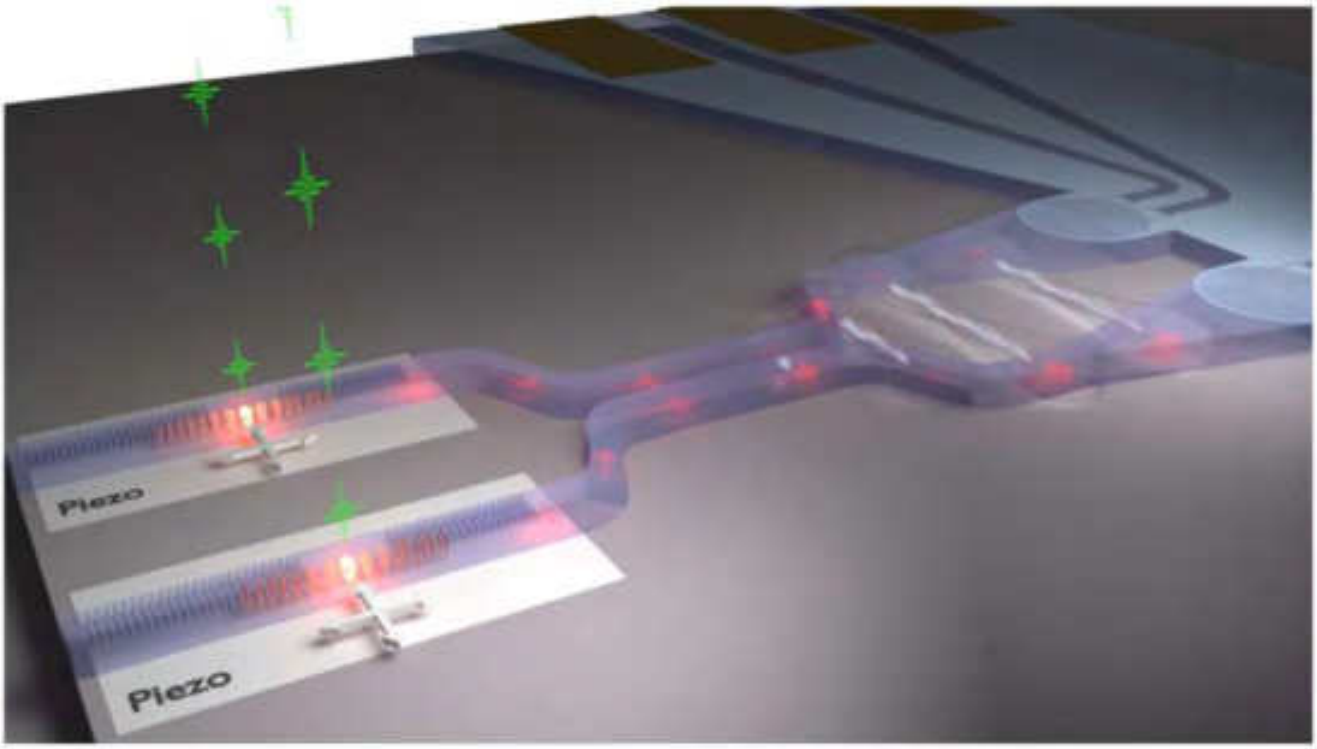
Photonen, Elementarteilchen des Lichts, sind wesentliche Ressourcen für aufkommende Quantentechnologien wie Quantenkommunikation und Quantenberechnung. Um Operationen mit Photonen durchführen zu können, müssen Schaltkreise für Licht, ähnlich wie bei elektronischen Schaltkreisen, aufgebaut werden. Diese Schaltungen erfordern Quellen, die in der Lage sind, eine genau definierte Anzahl von Photonen zu emittieren, Wellenleiter, in denen sich Photonen ausbreiten können und Elemente, die eine Wechselwirkung zwischen verschiedenen Photonen im Schaltkreis ermöglichen sowie hochempfindliche Detektoren.

Unter den verschiedenen Strategien, um solche "quantenphotonische Schaltkreise" zu erhalten, sind Halbleiterplattformen aufgrund der gut entwickelten Fertigungstechnologien und der Möglichkeit, hochwertige Photonenquellen in die Schaltung zu integrieren, besonders attraktiv. Die natürliche Wahl für die Halbleiterquelle stellen sogenannte Quantenpunkte dar, bei denen es sich um nanoskopische Strukturen handelt, die im Gegensatz zu klassischen Quellen Einzelphotonen "on demand" emittieren können. Trotz des Potenzials, mit dieser Architektur komplexe Netzwerke aufzubauen, ist der Fortschritt mit nur einem Quantenpunkt auf einige Anwendungen beschränkt. Der Grund ist, dass sich verschiedene Quantenpunkte in einem Chip normalerweise an nicht optimalen Positionen befinden und Photonen mit unterschiedlichen Farben und unterschiedlichen Eigenschaften emittieren. Dies behindert die effiziente Wechselwirkung zwischen verschiedenen Photonen und schränkt den Anwendungsbereich stark ein.

Ziel dieses Projekts ist die Entwicklung und Nutzung einer innovativen Plattform, die den gleichzeitigen Betrieb mehrerer Quantenpunktquellen in einer photonischen Schaltung ermöglicht. Um dieses Ziel zu erreichen, werden wir komplementäres Know-how der Universitäten Stuttgart und Linz kombinieren, um photonische Chips aufzubauen, bei denen Farbe und Eigenschaften der von verschiedenen Quantenpunkten emittierten Photonen durch mechanische Deformation präzise gesteuert werden können. Letzteres wird wiederum erreicht, indem die photonischen Schaltkreise auf einer patentierten piezoelektrischen Plattform platziert werden, die angelegte Spannungen in steuerbare Deformationen umwandelt.

Anders als in der Literatur vorgestellten Ansätze werden wir Quantenpunkte genau an den Eingängen der photonischen Schaltkreise platzieren und die Emissionseigenschaften unabhängiger Quellen durch unsere neue piezoelektrische Plattform präzise steuern.

Um die Erfolgschancen zu maximieren, werden wir an zwei verschiedenen Halbleitermaterialsystemen arbeiten. Auf diese Weise werden wir in der Lage sein, die bisher höchsten Photonwechselwirkungen zu demonstrieren und den Weg zu komplexen Netzwerken ebnen.

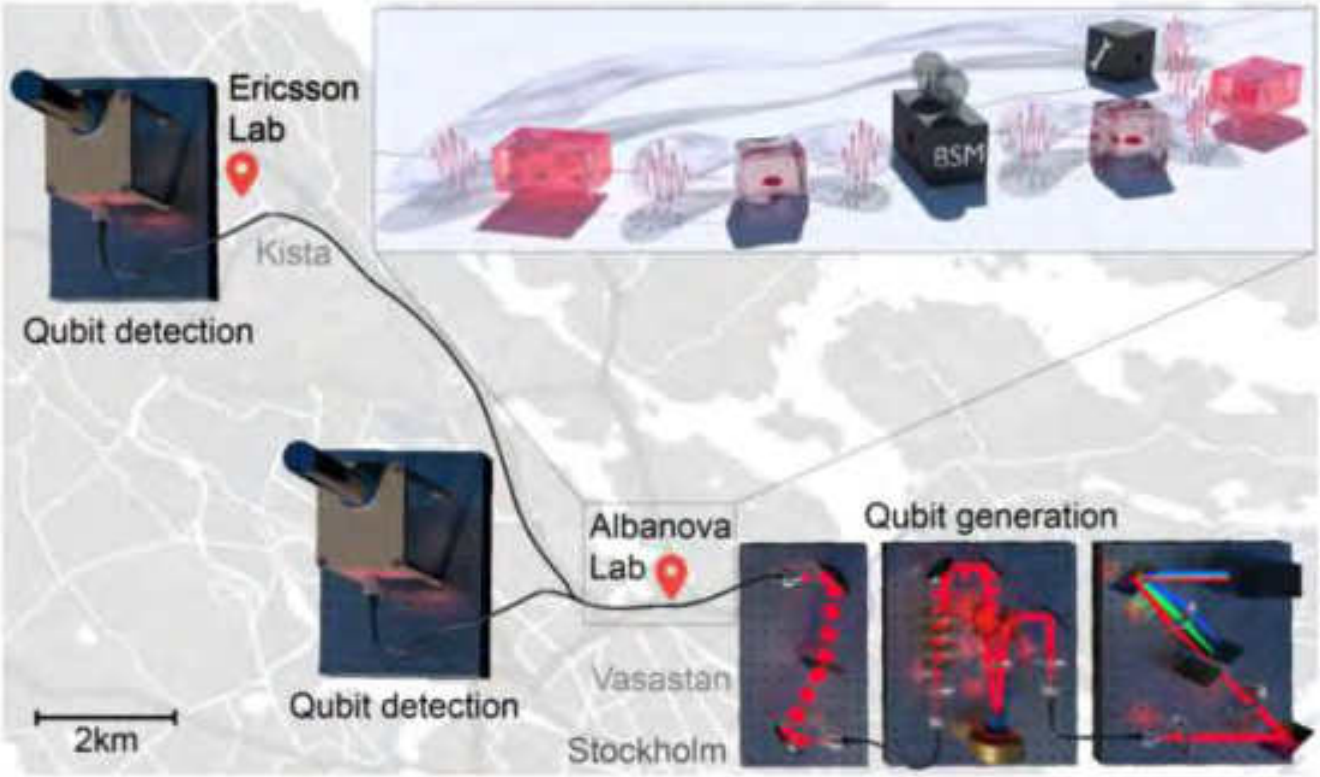


7.4. QUROPE - Quantum Repeaters using On-demand Photonic Entanglement

JKU PI: Armando Rastelli
Förderung: EU, H2020 FET Open
Förderungszeitraum: 01.09.2020 - 31.08.2023
Webpage: https://www.qurope-team.eu/
JKU Budget: 470.363 Euro

Ziel von Qurope ist es, eine hybride Quanten-Repeater-Architektur zu entwickeln, die auf unterschiedlichen Quantensystemen basiert und ihre Leistung in realen Anwendungen zu testen. Die geplante Implementierung basiert auf zwei disruptiven Technologien, die während des Projekts Pionierarbeit leisten werden: (i) Nahezu ideale quantenpunktbasierte Quellen verschränkter Photonenpaare, die gleichzeitig hohe Helligkeit und Ununterscheidbarkeit, einen nahezu perfekten Verschränkungsgrad, eine abstimmbare Wellenlänge und Betrieb auf "Knopfdruck" aufweisen. (ii) Effiziente und breitbandige Quantenspeicher, die speziell entwickelt und konstruiert werden, um polarisationsverschränkte Photonen aus Quantenpunkten zu speichern und abzurufen. Verschiedene Quantenpunkt-Quanten-Speichersysteme werden kombiniert, um Quanten-

Repeater zu entwickeln, die dann unter Verwendung von Quantenschlüsselaustauschprotokollen basierend auf Verschränkung getestet werden. Dies wird in der im Konsortium verfügbaren elementaren Quantennetzinfrastruktur geschehen – ein wichtiger Durchbruch, der den Weg für eine künftige groß angelegte Implementierung einer sicheren Quantenkommunikation ebnen wird.



7.5. FG5 - Multiphotonen-Experimente mit Halbleiter-Quantenpunkten

JKU PI: Armando Rastelli (Coordinator)
Förderung: FWF / Research Group
Förderungszeitraum: 01.09.2020 - 31.08.2025
Webpage: http://www.jku.at/hfp/fg5
JKU Budget: 401.860 Euro

Die Quantenphysik hat uns zu einem tieferen Verständnis der mikroskopischen Welt geführt und uns Werkzeuge zur quantitativen Beschreibung ihrer rätselhaften Phänomene geliefert. Diese Werkzeuge wurden zur Herstellung elektronischer Geräte bzw. ganzer Netzwerke genutzt, welche radikale Veränderungen der modernen Gesellschaft herbeigeführt haben – oftmals wird in diesem Zusammenhang von einer "Quantenrevolution" gesprochen. Basierend auf den neuen Ideen der Quanteninformationsverarbeitung befinden wir uns heute am Rande einer "zweiten Quantenrevolution": Bisher ungenutzte Quantenphänomene könnten in

Quantencomputern Anwendung finden, mit deren Hilfe bis dato nicht lösbare Probleme gelöst werden und die darüber hinaus zur Entwicklung von Quantenkommunikationssystemen führen könnten, welche allerhöchste Sicherheit gewährleisten. Unter den möglichen Bausteinen dafür stellen Photonen – Lichtquanten – die natürliche Wahl für die Quantenkommunikation dar und sind auch geeignet für Anwendungen im Bereich der Quantencomputer. Eine der Hürden auf dem Weg zu diesen revolutionären Anwendungen war immer das Fehlen von Lichtquellen, die imstande sind, "auf Befehl" Einzel- und Mehrfachphotonen zu emittieren. Die Lösung dieses Problems könnten Strukturen von Halbleitermaterialien im Nanometerbereich liefern, welche bereits die Grundlage klassischer Rechen- und Kommunikationsarchitekturen bilden.

Im vorliegenden Projekt haben wir es uns zum Ziel gesetzt, eine weltweit führende photonische Plattform zu etablieren, die sich auf einen neuartigen Typ von Halbleiterphotonenquellen in Kombination mit innovativen photonischen Schaltkreisen stützt, und diese zur Demonstration von Multiphotonen-Quantenprotokollen zu benutzen. Um dieses Ziel zu erreichen, kombinieren wir die komplementären Expertisen der teilnehmenden ForscherInnen an den Universitäten Innsbruck, Linz und Wien.

Wir konzentrieren uns auf Halbleiter-Quantenpunkte aus Galliumarsenid, welche sehr vorteilhafte Eigenschaften zeigen, wie etwa die Fähigkeit, einzelne und verschränkte Photonen mit Emissionsraten im Gigahertzbereich zu erzeugen. Dabei passt die Farbe ihres Lichts zu dem Bereich in welchem Silizium-Detektoren sehr empfindlich sind. Es werden allerdings noch erhebliche Anstrengungen nötig sein, um die Helligkeit der Lichtquellen und die Qualität der Photonen zu erhöhen. Insbesondere bei der kombinierten Verwendung mehrerer solcher Quellen müssen die emittierten Photonen vollkommen identisch sein. Diesen Herausforderungen werden wir uns stellen, indem wir: (i) die Quantenpunkte in Mikrostrukturen integrieren, die eine effiziente Einspeisung des emittierten Lichts in die Photonenschaltkreise ermöglicht; (ii) die Farbe der emittierten Photonen mithilfe einer patentierten Technologie feinabstimmen und (iii) verschiedene Methoden der Anregung für die Quantenpunkte erforschen, um die "Reinheit" der emittierten Photonen zu erhöhen. Parallel zur Verbesserung der Photonenquellen werden wir immer komplexere Anwendungen realisieren und in photonische Hochleistungs-Bauelemente integrieren. Unter anderem ist ein Ziel die Erzeugung von "Clusterzuständen" einiger Photonen für sichere Quantencomputer. Passende Tests sollen entwickelt werden, um die Entstehung solcher Zustände im Experiment zu verifizieren und die Leistungsfähigkeit des Systems zu charakterisieren.

Die Kombination des Quantenlichts aus den neuartigen Quantenpunkten mit integrierten Photonenschaltungen machen dieses Forschungsvorhaben einzigartig. Auf lange Sicht erwarten wir, dass der hier skizzierte Ansatz es uns ermöglichen wird, uns den ultimativen Grenzen der photonischen Quanteninformationsverarbeitung anzunähern.

7.6. ASCENT+ - Access to European Infrastructure for Nanoelectronics

JKU PI: Armando Rastelli
Förderung: EU / RIA
Förderungszeitraum: 01.09.2020 - 31.08.2024
Webpage: https://www.ascent.network/
JKU Budget: 296.680 Euro

ASCENT+ wird das erste ASCENT-Programm vorantreiben und erweitern und zusätzliche wichtige europäische Infrastrukturen integrieren, um die aufkommenden Forschungsherausforderungen in der Nanoelektronik anzugehen und einen reibungslosen sowie konsistenten Übergang der europäischen Industrie in eine neue Ära zu ermöglichen. Gegenwärtig haben akademische ForscherInnen und Technologen Schwierigkeiten, branchenrelevante disruptive Technologien zu entwickeln, da der Zugang zu modernster Verarbeitung, Modellierung/Datensätze, Metrologie/Charakterisierung sowie Geräte/Teststrukturen für die Nanoelektronik begrenzt ist.

Über den Single Entry Point und eine benutzerorientierte Zugangsschnittstelle integriert ASCENT+ eine einzigartige Forschungsinfrastruktur mit einem Investitionsvolumen von mehr als 2,5 Mrd. Euro, um seinen Benutzern diese Funktionen zu bieten. ASCENT+ umfasst akademische Partner, um das Angebot während der Lebensdauer dieser zweiten Phase der Advanced Community voranzutreiben, sowie ein erweitertes Netzwerk von über 3.700 Mitgliedern durch Partnerforschungs- und Branchenclusterorganisationen. Auf diese Weise kann ASCENT+ eine kritische Masse an Menschen, Wissen und Investitionen mobilisieren, um eine beispiellose Integration in die Community zu etablieren. Dies wird eine viel breitere Anwenderbasis bedienen und Innovationen fördern, indem neue wissenschaftliche Erkenntnisse in der Nanoelektronik mit herausfordernder Forschung verknüpft werden.

Europäische und globale Foresight-Studien haben gezeigt, dass die nächste Ära von der Notwendigkeit getrieben wird, Folgendes zu erreichen: (i) Quantenvorteil unter Verwendung von Festkörperplattformen; (ii) energiesparendes Hochleistungsrechnen mit geringem Stromverbrauch auf der Basis von neuartigen Bauelementen sowie (iii) verbesserte Funktionalität durch fortschrittliche Integration einer Vielzahl von Materialien und innovativen Technologien. ASCENT+ wird es seiner Benutzergemeinschaft ermöglichen, die Lücke zwischen wissenschaftlicher Erforschung und Entwicklung von Proof-of-Concept-Technologien zu schließen, um die Innovationsfindung zu beschleunigen. ASCENT+ bietet Europa die einmalige Gelegenheit, in einer entscheidenden Zeit, in der die traditionelle Skalierung zu Ende geht, die weltweite Führungsrolle in der Nanoelektronik wiederzuerlangen.

7.7. Integration of Validation into a Refinement-based Rigorous Development Process

JKU PI: Alexander Egyed, Atif Mashkoor
Förderung: FWF
Förderungszeitraum: Oktober 2020 - Oktober 2023
Webpage: https://www.jku.at/en/institute-for-software-systems-engineering/research/research-projects/fwf-ivoire/
JKU Budget: 374.629,50 Euro

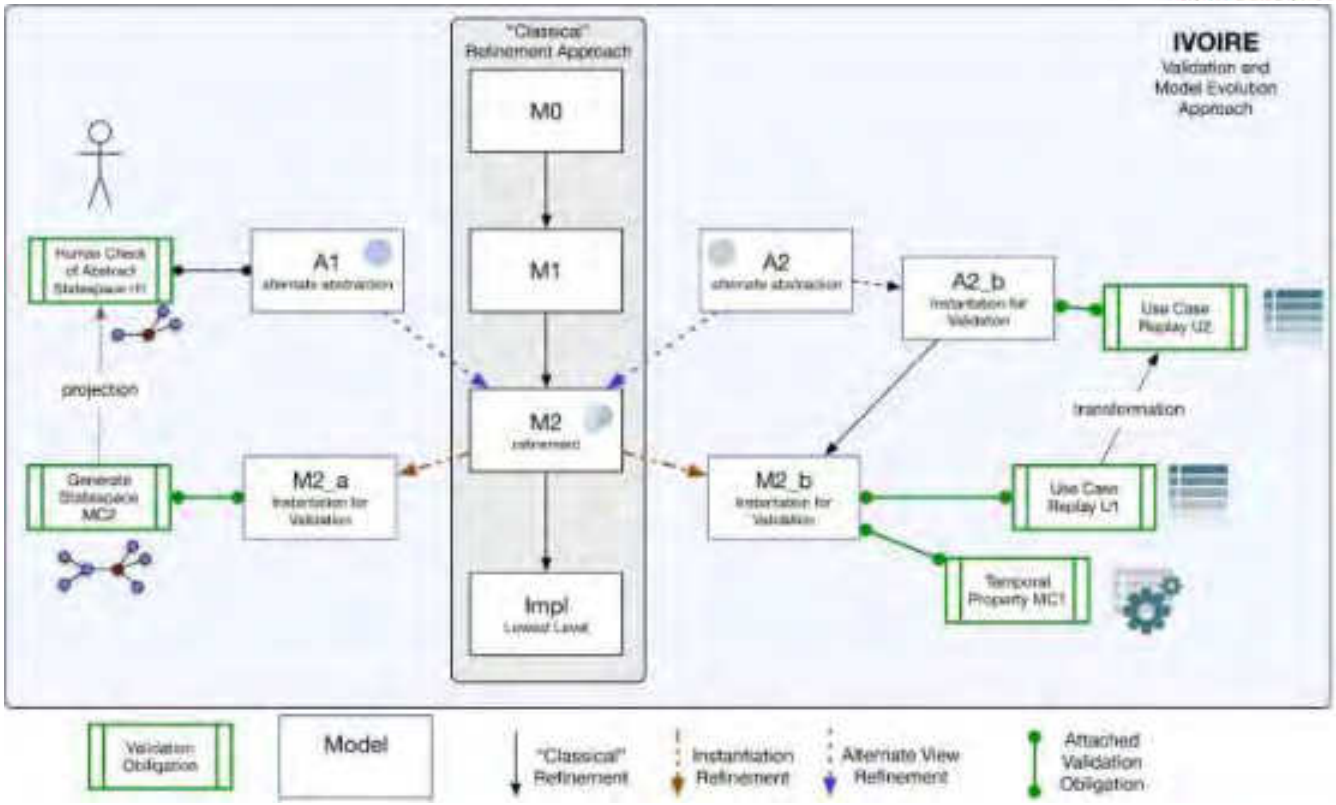
Trotz ihrer Wirksamkeit und jahrelanger Verfechtung ist der praktische Einsatz formaler Methoden immer noch sehr gering. Ein Grund ist, dass sich die aktuellen Methoden und Werkzeuge auf den Verifikationsprozess (wird die Software richtig entwickelt) konzentriert hat und den Validationsaspekt der Qualitätssicherung (wird die richtige Software entwickelt) im Vergleich dazu vernachlässigt hat.

Die Verifikation ist der Kern von Verfeinerungs-basierten Entwicklungsmethoden wie Event-B, wo jeder Verfeinerungsschritt die Eigenschaften des abstrakten Modells beibehalten muss. Die Validation findet oft erst statt, wenn die verfeinerten Modelle detailliert genug für eine Ausführung sind. Fehler in den Anforderungen oder deren Interpretation und Umsetzung werden deshalb viel zu spät im Entwicklungsprozess aufgedeckt.

Das IVOIRE Projekt wird es ermöglichen den Validierungsprozess kontinuierlich während der Entwicklung und Verfeinerung durchzuführen. Mit Hilfe von Event-B und Rodin, eine Methodik und eine Entwicklungsumgebung auf dem letzten Stand der Forschung, sollen Fortschritte auf drei Ebenen erzielt werden. Auf der formalen, wissenschaftlichen Ebene wird eine präzise Charakterisierung von Validierung im Rahmen von Verfeinerung entwickelt werden. Auf der Ebene der Methodik wird das klassische lineare Verfeinerungskonzept erweitert, um Validierungsobligationen und deren Prüfung darzustellen. Auf der praktischen Ebene wird die Rodin Werkzeugkette um neue Validationswerkzeuge erweitert und einer besseren Integration existierender Validationswerkzeuge ermöglicht. Anhand von verschiedenen Fallstudien wird der IVOIRE Ansatz mit Hilfe dieser Werkzeuge evaluiert.

Das IVOIRE Projekt wird folgende Ergebnisse liefern:

- Einen verbesserten formalen Entwicklungsprozess basierend auf einem erweiterten Verfeinerungskonzept mit Unterstützung für Validationsaktivitäten.
- Eine verbesserte Event-B Werkzeugkette, mit neuen Werkzeugen um Validierungsobligationen zu prüfen (zum Beispiel mit Animation oder Simulation) und um den gesamten Validierungsprozess zu verwalten.



7.8. ERC Consolidator Grant Project "Design Automation for Quantum Computing"

JKU PI: Robert Wille
Förderung: ERC
Förderungszeitraum: 01.07.2021 - 30.06.2026
JKU Budget: 1.979.552 Euro

In den 1970er Jahren begannen Forscher die Quantenmechanik zu nutzen, um Fragen der Informatik und der Informationstheorie zu beantworten und neue Forschungsrichtungen wie das Quantencomputing zu etablieren. Jetzt, fast fünf Jahrzehnte später, stehen wir am Beginn eines neuen "Computerzeitalters", in dem Quantencomputer tatsächlich Eingang in praktische Anwendungen finden. Während bei der physischen Realisierung von Quantencomputern beeindruckende Erfolge zu verzeichnen sind, besteht bei der Entwicklung von Softwaretools und automatisierten Methoden, die beim Entwurf und der Realisierung von Anwendungen für diese Geräte Unterstützung bieten, die Gefahr, dass sie mit dieser Entwicklung nicht Schritt halten können. Tatsächlich kann eine Situation eintreten, in der wir vielleicht leistungsstarke Quantencomputer haben, aber kaum geeignete Mittel, um sie tatsächlich zu nutzen.

In diesem Projekt wollen wir Methoden entwickeln, die helfen, eine solche Situation zu vermeiden. Der Schwerpunkt liegt auf der Entwicklung effizienter Methoden und Software für entsprechende Entwurfsaufgaben wie Simulation, Compilation, Verifikation und

andere. Zu diesem Zweck wollen wir das Potenzial und die Expertise der Entwurfsautomatisierung nutzen. Diese findet im Bereich des Quantum Computings bisher nur Anwendung. Dabei möchten wir sicherstellen, dass ForscherInnen aus dem Bereich der Entwurfsautomatisierung die "richtigen" Probleme angehen und die resultierende Software/Methode tatsächlich die Bedürfnisse von Stakeholdern berücksichtigt. Langfristiges Ziel ist es, eine Brücke zwischen Entwurfsautomatisierung und Quantum Computing zu schlagen und für Quantencomputer zu schaffen, was die "konventionelle" Entwurfsautomatisierung für klassische Schaltungen und Systeme realisiert hat.

7.9. Christian Doppler Labor "Private Digital Authentication in the Physical World"

JKU PI: René Mayrhofer
Förderung: CDG
Förderungszeitraum: 01.01.2020 - 31.12.2026
JKU Budget: > 2 Mio. Euro (Budgetplanung erfolgt pro Kalenderjahr)

Reisen ohne Pass, Türen öffnen ohne Schlüssel, U-Bahn-Fahren ohne physischen Identitätsnachweis – die Digitalisierung und die Speicherung biometrischer Daten könnte das möglich machen. Aber zentralisierte Datenbanken für biometrische Daten bergen ein großes Missbrauchspotential für anlass-unabhängige Massenüberwachung und sind anfällig für Fehler und Daten-Leaks. Damit trotzdem nicht auf die Vorteile der digitalen Authentifizierung verzichtet werden muss, forscht das CD-Labor für private digitale Authentifizierung in der physischen Welt an dezentralen Ansätzen, um allen NutzerInnen bessere Kontrolle über ihre Interaktionen in der digitalen sowie physischen Welt und damit den Datenspuren, die sie notwendigerweise hinterlassen, zu geben.

Wir assoziieren jeweils einen persönlichen digitalen Agenten mit individuellen NutzerInnen in der physischen Welt. Dieser ermöglicht als Stellvertreter die Nutzung digitaler und physischer Dienste für das jeweilige Individuum, unter dessen alleiniger Kontrolle der Agent steht. Jährliche Prototypen werden den Fortschritt demonstrieren und die Evaluierung anhand konkreter Anwendungsfälle ermöglichen.

7.10. Weitere Projekte und Kooperationen

Darüber hinaus konnten weitere Projekte und Kooperationen im LIT Lab etabliert werden. Konkret

- fördert Google mit einem Direktauftrag die Forschungen von Prof. Robert Wille am Lab zum Thema Quantencomputer,
- konnte Prof. Robert Wille zusammen mit der FH Hagenberg die Finanzierung einer gemeinsamen Doktoratsstelle zum Thema "Fast Quantum Simulation with consideration of hardware Noise" einwerben (ein weiteres Beispiel für die Kooperation mit Hagenberg),
- konnte ein LIT Projekt für eine PostDoc-Stelle zum Thema "Development of Design Automation Methods for Sample Preparation on Two-Phase Droplet Microfluidic

Labs-on-Chips" (d.h. dem Entwurf von korrekten "Lab-on-Chips"-Geräten) eingeworben werden,

- hat sich LIT Lab PostDoc Dr. Atif Mashkoor zusammen mit dem Software Competence Centrum Hagenberg (SCCH) federführend in der Initiative Pak Austria Fachhochschule eingebracht, in denen zusammen mit anderen österreichischen Hochschulen, wie der FH Joanneum oder dem MCI Innsbruck, eine langfristige Kooperation mit WissenschaftlerInnen aus Pakistan etabliert werden soll (in diesem Zuge erhält die JKU und das LIT Lab Finanzierungen für entsprechende PostDoc-Stellen für die kommenden zwei Jahre) und
- wurde ein speziell gefördertes Technik-Kunst-Projekt zum Thema Sicherheit von Schließsystemen durch Dr. Michael Roland am Ars Electronica Festival 2020 vorgestellt.
- wird gemeinsam mit der der Firma ENGEL in einer Kooperation daran geforscht, durch Bedrohungsmodellierung und Risikoanalysen systematisch mögliche Angriffe zu identifizieren, Risiken zu bewerten und entsprechende Gegenmaßnahmen einzuleiten.

8. Auszeichnungen und Erfolge

Die Exzellenz der am LIT Secure and Correct Systems Lab arbeitenden Personen zeichnet sich nicht nur die zahlreichen wissenschaftlichen Publikationen und Projekte aus, sondern wird von den Communities auch in Form verschiedener Preise und Auszeichnungen anerkannt.

So erhielt das Team um Prof. Armin Biere 2019 bei der SAT Competition zwei Medaillen (darunter einen ersten Platz), bei der SMT Competition insgesamt zehn Medaillen (darunter sieben erste Plätze) und bei der SAT Competition 2020 sieben Medaillen (darunter vier Goldmedaillen). Bei diesen Wettbewerben handelt es sich um die weltweit führenden Leistungsvergleiche im Bereich des SAT-Solving. Entsprechende SAT-Beweiser bilden bis heute die Grundlage für zahlreiche Methoden des Korrektheits- und Sicherheitsnachweises.

Weiters erhielt Prof. Armin Biere zusammen mit der LIT Lab Doktorandin Sibylle Möhle-Rotondi einen "Best Poster and Interaction Award" für die oben bereits genannte Arbeit mit dem Titel "Combining Conflict-Driven Clause Learning and Chronological Backtracking for Propositional Model Counting" (GCAI 2019).

Darüber hinaus wurde Sibylle Möhle-Rotondi im September 2020 mit einem "Best Student Contribution Award" für ihre Arbeit " (Dual) Projected Propositional Model Counting and Enumeration without Competition" ausgezeichnet.

Im Bereich Quantum Computing nahm das Team um Prof. Robert Wille und dem LIT Lab Doktoranden Lukas Burgholzer an der IBM Quantum Challenge 2019 teil. Aus über 700 TeilnehmerInnen hat sich das Team dabei für das Finale der verbliebenen 40 besten Teams qualifiziert und dort den dritten Platz errungen.

Eine der wegweisenden Arbeiten der Gruppe zur Übersetzung von Quantenprogrammen wurden zudem im Oktober 2020 mit einem Best Paper Award der IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems geehrt. Darüber hinaus schafften es mehrere Arbeiten der Gruppe (aus dem Bereich Quantum Computing aber auch Bereichen des Entwurfs von komplexen Schaltungen mit Hilfe von Machine Learning) in den engeren Kreis von Best Paper Award Kandidaten.

Weiters wurde 2019 Prof. Robert Wille mit einem Under-40 Innovators Award von der Design Automation Conference (DAC) geehrt, von JKU-Studenten zum besten Prof gewählt ("Vote your Prof") und erhielt im Dezember 2020 einen ERC Grant mit einer Fördersumme von 2 Millionen Euro. Zudem werden die Doktoranden von Prof. Robert Wille regelmäßig mit Nachwuchspreisen ausgezeichnet.

Hinsichtlich der Nachwuchsförderung freuen wir uns, dass das Team "UpperSec" (ein Verbund von Studierenden, der gemeinsam auf "Hacking"-Wettbewerben antritt und dabei vom LIT Lab unterstützt wird) ebenfalls sehr erfolgreich war. So hat sich "UpperSec" aus mehr als 1000 Mitbewerbern als bestes deutschsprachiges Team für das Finale des IT-Sicherheitswettbewerbs "VolgaCTF" qualifiziert. Dort konnten sie sich schließlich 2019 mit dem sechsten Platz (als bestes nicht-russisches Team) und 2020 mit dem 13. Platz bewähren. Darüber hinaus wurden sie beim CTF Time-Wettbewerb 2020 als bestes Team österreichweit gekürt.

Die Doktoranden Daniel Hofer und Philipp Schwarz hatten sich 2019 für das Finale des Adolf-Adam-Informatikpreises qualifiziert. Im Finale konnte sich hier schließlich Philipp Schwarz durchsetzen und erhielt den ersten Preis. Auch dies ist ein weiteres Beispiel dafür, dass das Lab mit überdurchschnittlich guten Personen besetzt ist.

9. Öffentlichkeitsarbeit

Als Repräsentanten der JKU und der "wissenschaftlichen Welt", die in hohem Maße von der Unterstützung der Öffentlichkeit abhängig ist, ist es uns natürlich auch ein besonderes Anliegen, unsere Arbeit einem breiteren Publikum (und nicht nur der Fachwelt) vorzustellen. Entsprechend versuchen wir die hierfür zur Verfügung stehenden Möglichkeiten (Pressearbeit, Veranstaltungen wie Lange Nacht der Forschung, Open House, etc. oder Schulbesuche) so gut wie möglich zu nutzen.

Ein besonderes Beispiel hierfür ist sicherlich die Eröffnung des LIT Secure and Correct Systems Lab am 17. Oktober 2019 im Open Innovation Center. Nach Grußworten des Wirtschaftslandesrats Achleitner und des Rektors Lukas konnte sich das Lab hier erstmalig im großen Rahmen circa 150 Gästen präsentieren (darunter auch KollegInnen aus Partnerinstitutionen, wie dem Software Competence Center Hagenberg und der Fachhochschule Hagenberg aber auch zahlreichen VertreterInnen aus der lokalen Industrie). Für großes Interesse sorgte die Veranstaltung auch bei der Presse, was sich in zahlreichen Artikeln in den darauffolgenden Tagen bemerkbar gemacht hat.

Darüber hinaus nutzen wir auch regelmäßig die oben genannten Erfolge und Aktivitäten als "Aufhänger", um mit der Presse (und damit mit der Öffentlichkeit) über unsere Arbeit ins Gespräch zu kommen. Auf diesen Weg wurden bereits knapp 50 Artikel über uns in der Presse veröffentlicht. Im Anhang findet sich hierzu ein entsprechender Auszug.

Auch Besuche, z.B. von Bundeskanzlerin Bierlein und der Ministerin Rauskala am 05.09.2019 oder des Finanzministers Eduard Müller am 22.10.2019, wurden von uns genutzt, um unsere Arbeit der Politik vorzustellen.

Und schließlich sind wir auch regelmäßig Redner bei öffentlichen Veranstaltungen, die z.B. vom Open Innovation Center der JKU, der Wirtschaftskammer Oberösterreich und weiteren veranstaltet werden.

Weiters haben wir Repräsentationsmaterial mit dem wir, z.B. auf Konferenzen, Messen oder in direkten Gesprächen, auf die Arbeit des Labs hinweisen bzw. das wir für die Akquise benutzen.

10. Schlussbemerkungen und Ausblick

Das LIT Secure and Correct System Lab hat sich in den vergangenen knapp zwei Jahren als Hub für exzellente Forschung und wissenschaftlichen Austausch etablieren können. Wie der Bericht zeigt, konnten trotz des harten Wettbewerbs um "die besten Köpfe" nicht nur alle Stellen mit herausragenden Persönlichkeiten besetzt werden (darunter viele WissenschaftlerInnen), sondern in sehr kurzer Zeit bereits zahlreiche wissenschaftliche Ergebnisse erzielt sowie Projekte und Kooperationen gestartet werden. Die Exzellenz zeigt sich in einer großen Anzahl an Publikationen, die in internationalen Foren veröffentlicht wurden und dort mittlerweile regelmäßig ausgezeichnet bzw. für Preise nominiert werden. Weiters zeigt sich die Relevanz der im Lab vertretenen Themen durch zahlreiche Projekte, die seit dem Start des Labs (oft mit industrieller Beteiligung) eingeworben wurden. Und schließlich positionieren wir über gezielte Öffentlichkeitsarbeit das Lab auch als "Leuchtturm" für die Region.

Für die Unterstützung des Landes Oberösterreichs und des Rektorats der JKU, ohne die diese Erfolge nicht möglich gewesen wären, möchten wir uns an dieser Stelle noch einmal herzlich bedanken! Für die Zukunft blicken wir angesichts dieser Ergebnisse sehr optimistisch nach vorn. Das Ziel der kommenden Monate wird es sein, die gelegten Grundlagen weiter auszubauen und perspektivisch eine Verstetigung des LIT Secure and Correct Systems Labs anzustreben. Die bisher erzielten Ergebnisse und Erfolge bilden dafür unserer Meinung nach eine solide Basis.

11. Anhang: Auszug aus der Forschungsdokumentation (FoDok)

11.1. Aufsatz / Paper in SCI-Expanded-Zeitschrift

Yuan X., Schwendtner M., Trotta R., Huo Y., Martin Sanchez J., Piredda G., Huang H., Edlinger J., Diskus C., Schmidt O., Jakoby B., Krenner H., Rastelli A.:
A frequency-tunable nanomembrane mechanical oscillator with embedded quantum dots, in AIP, in Appl. Phys. Lett., Serie 115, Seite(n) 181902, 2019

Liu J., Su R., Wei Y., Yao B., Covre da Silva S., Yu Y., Iles-Smith J., Srinivasan K., Rastelli A., Li J., Wang X.:
A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability, in Nature Nanotechnology, Vol. 14, Seite(n) 586-594, 2019

Schimpf C., Reindl M., Klenovsky P., Fromherz T., Covre da Silva S., Hofer J., Schneider C., Höfling S., Trotta R., Rastelli A.:
Resolving the temporal evolution of line broadening in single quantum emitters, in Optics Express, Vol. 27, Seite(n) 35290-35307, 2019

Huber D., Lehner B., Csontosova D., Reindl M., Schuler S., Covre da Silva S., Klenovsky P., Rastelli A.:
Single-particle-picture breakdown in laterally weakly confining GaAs quantum dots, in Phys. Rev. B, Vol. 100, Seite(n) 235425, 2019

Nysten E., Rastelli A., Krenner H.:
A hybrid (Al)GaAs-LiNbO3 surface acousticwave resonator for cavity quantum dot optomechanics, in Appl.Phys.Lett., Vol. 117, Seite(n) 121106, 2020

Servadei L., Mosca E., Zennaro E., Devarajegowda K., Werner M., Ecker W., Wille R.:
Accurate Cost Estimation of Memory Systems Utilizing Machine Learning and Solutions from Computer Vision for Design Automation, in IEEE Transactions on Computers (TC), Vol. 69, Nr. 6, Seite(n) 856-867, 2020

Niemann P., Wille R., Drechsler R.:
Advanced Exact Synthesis of Clifford+T Circuits, in Springer, in Quantum Information Processing, Springer NY, 2020

Fink G., Hamidovic M., Haselmayr W., Wille R.:
Automatic Design of Droplet-Based Microfluidic Ring Networks, in IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD), 2020

Fink G., Hamidovic M., Springer A., Wille R., Haselmayr W.:
Design and realization of flexible droplet-based lab-on-a-chip devices: From theory to practice, in e & i Elektrotechnik und Informationstechnik, Springer, Seite(n) 113 - 120, 2020

Kole A., Hillmich S., Datta K., Wille R., Sengupta I.:
Improved Mapping of Quantum Circuits to IBM QX Architectures, in IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD), 2020

Zhai L., Löbl M., Jahn J., Huo Y., Treutlein P., Schmidt O., Rastelli A., Warburton R.:
Large-range frequency tuning of a narrow-linewidth quantum emitter, in Appl. Phys. Lett., Vol. 117, Seite(n) 083106, 2020

Chekhovich E., Covre da Silva S., Rastelli A.:
Nuclear spin quantum register in an optically active semiconductor quantum dot, in Nature Nanotechnology, Vol. 15, Seite(n) 999-1004, 2020

Hanschke L., Schweickert L., Lopez Carreno J., Schöll E., Zeuner K., Lettner T., Casalengua E., Reindl M., Covre da Silva S., Trotta R., Finley J., Rastelli A., del Valle E., Laussy F., Zwiller V., Müller K., Jöns K.:
Origin of Antibunching in Resonance Fluorescence, in Phys. Rev. Lett., Vol. 125, Seite(n) 170402, 2020

Niemann P., Zulehner A., Drechsler R., Wille R.:
Overcoming the Trade-off Between Accuracy and Compactness in Decision Diagrams for Quantum Computation, in IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD), 2020

Hepp S., Hornung F., Bauer S., Hesselmeier E., Yuan X., Jetter M., Portalupi S., Rastelli A., Michler P.:
Purcell-enhanced single-photon emissionfrom a strain-tunable quantum dot in acavity-waveguide device, in Appl. Phys. Lett., Vol. 117, Seite(n) 254002, 2020

Vogele A., Sonner M., Mayer B., Yuan X., Weiß M., Nysten E., Covre da Silva S., Rastelli A., Krenner H.:
Quantum Dot Optomechanics in Suspended Nanophononic Strings, in Wiley, in Adv. Quantum Technol., Vol. 3, Seite(n) 1900102, 2020

Suárez-Forero D., Ardizzone V., Covre da Silva S., Reindl M., Fieramosca A., Polimeno L., De Giorgi M., Dominici L., Pfeiffer L., Gigli G., Ballarini D., Laussy F., Rastelli A., Sanvitto D.:
Quantum hydrodynamics of a single particle, in Light: Science &Applications, Vol. 9, Seite(n) 85, 2020

Manna S., Huang H., Covre da Silva S., Schimpf C., Rota M., Lehner B., Reindl M., Trotta R., Rastelli A.:
Surface passivation and oxide encapsulation to improve optical properties of a single GaAs quantum dot close to the surface, in Applied Surface Science, Vol. 532, Seite(n) 147360, 2020

11.2. Aufsatz / Paper in Tagungsband (referiert)

Tröls M., Mashkoor A., Egyed A.:
Collaboratively enhanced consistency checking in a cloud-based engineering environment, in Jose Ignacio Panach, Jean Vanderdonckt, Oscar Pastor: Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems, EICS 2019, Valencia, Spain, June 18-21, 2019, Nr. 15, ACM, Seite(n) 15:1-15:6, 2019

Möhle S., Biere A.:
Combining Conflict-Driven Clause Learning and Chronological Backtracking for Propositional Model Counting, in Diego Calvanese, Luca Iocchi: 5th Global Conference on Artificial Intelligence, Serie EasyChair EPiC series in Computing, 2019

Servadei L., Mosca E., Lee J., Yang J., Esen V., Wille R., Ecker W.:
Combining Evolutionary Algorithms and Deep Learning for Hardware/Software Interface Optimization, in ACM/IEEE: Workshop on Machine Learning for CAD (MLCAD), 2019

Pointner S., Wille R.:
Did we Test Enough? Functional Coverage for Post-Silicon Validation: International Test Conference in Asia (ITC-Asia), 2019

Berner F., Sametinger J.:
Dynamic Taint-Tracking: Directions for Future Research, in SECRYPT: SECRYPT 2019 - Proceedings of the International Conference on Security and Cryptography, Prague, Czech Republic, July 26-28, 2019, Vol. 2, Seite(n) 294-305, 2019

Zulehner A., Bauer H., Wille R.:
Evaluating the Flexibility of A* for Mapping Quantum Circuits: Conference on Reversible Computation (RC), 2019

Pointner S., Grimmer A., Wille R.:
Exact Stimuli Minimization for Simulation-Based Verification: International Symposium on circuits and Systems (IEEE), 2019

Serajeh-Hassani F., Sadrosadati M., Pointner S., Wille R., Sarbazi-Azad H.:
Focus on What is Needed: Area and Power Efficient FPGAs Using Turn-Restricted Switch Boxes: IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2019

Pointner S., Gonzalez de Aledo P., Wille R.:
Generic Error Localization for the Electronic System Level: DDECS 2019, 2019

Zulehner A., Hillmich S., Wille R.:
How to Efficiently Handle Complex Values? Implementing Decision Diagrams for Quantum Computation: International Conference on Computer Aided Design (ICCAD), 2019

Berner F., Sametinger J.:
Information Disclosure Detection in Cyber-Physical Systems: IWCFS 2019 - 3rd International Workshop onCyber-Security and Functional Safety in Cyber-Physical Systems,Linz, Austria, August 26-29, 2019, Vol. 1062, 2019

Auer D., Jäger M., Küng J.:
Linking Trust to Cyber-Physical Systems, in Kotsis, Gabriele; Tjoa, A. Min; Khalil, Ismail: Database and Expert Systems Applications, Serie Communications in Computer and Information Science, Nr. 1062, Springer International Publishing, Cham, Seite(n) 119-128, 2019

Wille R., Burgholzer L., Zulehner A.:
Mapping Quantum Circuits to IBM QX Architectures Using the Minimal Number of SWAP and H Operations: Design Automation Conference (DAC), 2019

Tröls M., Mashkoor A., Egyed A.:
Multifaceted Consistency Checking of Collaborative Engineering Artifacts, in Loli Burgueno, Alexander Pretschner, Sebastian Vosshel, Michel Chaudron, Jörg Kienzle, Markus Völter,Sebastien Gerard Mansooreh Zahedi Erwan Bousse Arend Rensink Fiona Polack Gregor EngelsGerti Kappel: 22nd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion, MODELS Companion 2019, Munich, Germany, September 15-20, 2019, IEEE, Seite(n) 278-287, 2019

Rao A., Carréon N., Lysecky R., Rozenblit J., Sametinger J.:
Resilient Security of Medical Cyber-Physical Systems: IWCFS 2019 - 3rd International Workshop on Cyber-Security and Functional Safety in Cyber-Physical Systems, Linz, Austria, August 26-29, 2019., 2019

Sametinger J.:
Securing Smart Homes: IWCFS 2019 - 3rd International Workshop on Cyber-Security and Functional Safety in Cyber-Physical Systems, Linz, Austria, August 26-29, 2019., 2019

Zahid M., Mashkoor A., Mehmood Z.:
Security Risk Mitigation of Cyber Physical Systems: A Case Study of a Flight Simulator, in Gabriele Anderst-Kotsis, A Min Tjoa, Ismail Khalil, Mourad Elloumi , Atif Mashkoor, Johannes Sametinger, Xabier Larrí ucea, Anna Fensel, Jorge Martinez Gil, B. Moser, C. Seifert, M. Ganitzer: Database and Expert Systems Applications - DEXA 2019 International Workshops BIOKDD, IWCFS, MLKgraphs and TIR, Linz, Austria, August 26-29, 2019, Proceedings, Serie Communications in Computer and Information Science, Vol. 1062, Springer, Seite(n) 129-138, 2019

Pointner S., Frank O., Hazott C., Wille R.:
Test Your Test Programs Pre-Silicon: A Virtual Test Methodology for Industrial Design Flows, in IEEE: Computer Society Annual Symposium on VLSI (ISVLSI), 2019

Wille R., Haghparast M., Adarsh S., M T.:
Towards HDL-based Synthesis of Reversible Circuits with No Additional Lines: International Conference on Computer Aided Design (ICCAD), 2019

Kreindl J., Bonetta D., Mössenböck H.:
Towards efficient, multi-language dynamic taint analysis: MPLR 2019: Proceedings of the 16th ACM SIGPLAN International Conference on Managed Programming Languages and Runtimes, ACM, Seite(n) 85-94, 2019

Zulehner A., Hillmich S., Markov I, Wille R.:
Approximation of Quantum States Using Decision Diagrams: Asia and South Pacific Design Automation Conference (ASP-DAC), 2020

Grurl T., Fuß J., Burgholzer L., Hillmich S., Wille R.:
Arrays vs. Decision Diagrams: A Case Study on Quantum Circuit Simulators: International Symposium on Multiple-Valued Logic (ISMVL), 2020

Mohamed A., Auer D., Hofer D., Küng J.:
Authorization Policy Extension for Graph Databases, in Tran Khanh Dang, Josef Küng, Makoto Takizawa, Tai M. Chung: Future Data and Security Engineering, Serie Lecture Notes in Computer Science series (LNCS), Vol. 12466, Springer Nature Switzerland, Seite(n) 47-66, 2020

Walter M., Wille R., Torres F., Drechsler R.:
Bail on Balancing: An Alternative Approach to the Physical Design of Field-coupled Nanocomputing Circuits: IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020

Hillmich S., Zulehner A., Wille R.:
Concurrency in DD-based Quantum Circuit Simulation: Asia and South Pacific Design Automation Conference (ASP-DAC), 2020

Grurl T., Fuß J., Wille R.:
Considering Decoherence Errors in the Simulation of Quantum Circuits Using Decision Diagrams: International Conference on Computer Aided Design (ICCAD), 2020

Servadei L., Mosca E., Devarajegowda K., Werner M., Ecker W., Wille R.:
Cost Estimation for Configurable Model-Driven SoC Designs Using Machine Learning: Great Lakes Symposium on VLSI (GLVLSI), 2020

Mir O., Mayrhofer R., Roland M.:
DAMFA: Decentralized Anonymous Multi-Factor Authentication, in ACM: BSCI: International Symposium on Blockchain and Secure Critical Infrastructure, 2020

Wille R., Hillmich S., Burgholzer L.:
Efficient and Correct Compilation of Quantum Circuits: IEEE International Symposium on Circuits and Systems, 2020

Mashkoor A., Egyed A.:
Evaluating the alignment of sequence diagrams with systembehavior: ISM 2020, 2020

Michelon G.:
Evolving System Families in Space and Time: Proceedings of the 24th ACM International Systems and Software Product Line Conference - Volume B, in ACM, Serie SPLC '20, Association for Computing Machinery, New York, NY, USA, Seite(n) 104-111, 2020

Hillmich S., Zulehner A., Wille R.:
Exploiting Quantum Teleportation in Quantum Circuit Mapping: International Workshop on Quantum Compilation (IWQC), 2020

Möhle S., Sebastiani R., Biere A.:
Four Flavors of Entailment, in Pulina L., Seidl M.: The 23rd International Conference on Theory and Applications of Satisfiability Testing, Serie Lecture Notes in Computer Science, Vol. 12178, Springer, Cham, 2020

Burgholzer L., Wille R.:
Improved DD-based Equivalence Checking of Quantum Circuits: Asia and South Pacific Design Automation Conference (ASP-DAC), 2020

Bornebusch F., Lüth C., Wille R., Drechsler R.:
Integer Overflow Detection in Hardware Designs at the Specification Level: Int'l Conf. on Model-Driven Engineering and Software Development (MODELSWARD), 2020

Hübscher G., Geist V., Auer D., Hübscher N., Küng J.:
Integration of Knowledge and Task Management in an Evolving, Communication-intensive Environment, in Maria Indrawan-Santiago, Eric Pardede, Ivan Luiz Salvadori, Matthias Steinbauer, Ismail Khalil, Gabriele Anderst-Kotsis: Proceedings of iiWAS 2020, Serie Proceedings of iiWAS, ACM, New York, Seite(n) 407-416, 2020

Suárez-Forero D., Ardizzone V., Pfeiffer L., Rastelli A., Sanvitto D.:
Interface of a deterministic single photons source with a 2D semiconductor microcavity: pushing polaritonic systems into the quantum regime, in B. Lee, C. Mazzali, K. Corwin, and R. Jason Jones: Frontiers in Optics / Laser Science, OSA Technical Digest (Optical Society of America, 2020), Seite(n) paper FTu2D.6, 2020

Wille R., Hillmich S., Burgholzer L.:
JKQ: JKU Tools for Quantum Computing: International Conference on Computer Aided Design (ICCAD), 2020

Hillmich S., Markov I., Wille R.:
Just Like the Real Thing: Fast Weak Simulation of Quantum Computation.: Design Automation Conference (DAC), 2020

Michelon G., Obermann D., Linsbauer L., Assunção W., Grünbacher P., Egyed A.:
Locating Feature Revisions in Software Systems Evolving in Space and Time: 24rd International Systems and Software Product Line Conference, 2020

Michelon G., Obermann D., Klewerton Guez Assunção W., Linsbauer L., Grünbacher P.:
Mining Feature Revisions in Highly-Configurable Software Systems: Proceedings of the 24th ACM International Systems and Software Product Line Conference - Volume B, Seite(n) 74-78, 2020

Riegler M., Sametinger J.:
Mode Switching from a Security Perspective: First Findings of a Systematic Literature Review: Database and Expert Systems Applications, in Database and Expert Systems Applications, Serie Communications in Computer and Information Science, Vol. 1285, Springer International Publishing, Cham, Seite(n) 63-73, 2020

Riegler M., Sametinger J.:
Multi-Mode Systems for Resilient Security in Industry 4.0: ISM 2020, International Conference on Industry 4.0 and Smart Manufacturing, Hagenberg, Austria November 23-25, 2020, virtual event., 2020

Almudever C., Lao L., Wille R., Guerreschi G.:
Realizing Quantum Algorithms on Real Quantum Computing Devices: Design, Automation and Test in Europe (DATE), 2020

Burgholzer L., Wille R.:
The Power of Simulation for Equivalence Checking in Quantum Computing: Design Automation Conference (DAC), 2020

Garlando U., Walter M., Wille R., Riente F., Torres F., Drechsler R.:
ToPoliNano and fiction: Design Tools for Field-coupled Nanocomputing: Euromicro Conference on Digital System Design (DSD), 2020

Bornebusch F., Wille R., Drechsler R.:
Towards Automatic Hardware Synthesis from Formal Specification to Implementation: Asia and South Pacific Design Automation Conference (ASP-DAC), 2020

Schober S., Carbonelli C., Roth A., Zoepfl A.:
Towards Drift Modeling of Graphene-Based Gas Sensors Using Stochastic Simulation Techniques: IEEE SENSORS, 2020

Deb A., Dueck G., Wille R.:
Towards Exploring the Potential of Alternative Quantum Computing Architectures: Design, Automation and Test in Europe (DATE), 2020

Shafiq S., Mayr-Dorn C., Mashkoor A., Egyed A.:
Towards Optimal Assembly Line Order Sequencing with Reinforcement Learning: A Case Study: 25th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2020, Vienna, Austria, September 8-11, 2020, in IEEE, IEEE, Seite(n) 982-989, 2020

Ring M., Bornebusch F., Lüth C., Wille R., Drechsler R.:
Verification Runtime Analysis: Get the Most Out of Partial Verification: Design, Automation and Test in Europe (DATE), 2020

Walter M., Wille R., Torres F., Große D., Drechsler R.:
Verification for Field-coupled Nanocomputing Circuits: Design Automation Conference (DAC), 2020

Burgholzer L., Raymond R., Wille R.:
Verifying Results of the IBM Qiskit Quantum Circuit Compilation Flow: IEEE International Conference on Quantum Computing (QCE), 2020

Pointner S., Gonzalez de Aledo P., Wille R.:
YASSi: Yet Another Symbolic Simulator: International Workshop on Cyber-Security and Functional Safety in Cyber-Physical Systems (IWCFS), 2020

Pekarek D.:
trcview: interactive architecture agnostic execution trace analysis: MPLR 2020: Proceedings of the 17th International Conference on Managed Programming Languages and Runtimes, ACM Digital Library, Seite(n) 89-97, 2020

11.3. Aufsatz / Paper in Sammelwerk (referiert)

Tröls M., Mashkoor A., Egyed A.:
Live and global consistency checking in a collaborative engineering environment, in Chih-Cheng Hung and George A. Papadopoulos: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC 2019, Limassol, Cyprus, April 8-12, 2019, in Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, ACM, Seite(n) 1776-1785, 2019

Keszöcze O., Keiner B., Richter M., Antpöhler G., Wille R.:
(Semi)automatic Translation of Legal Regulations to Formal Representations: Expanding the Horizon of EDA Applications: Natural Language Processing for Electronic Design Automation, Springer, Cham, Seite(n) 1-11, 2020

Zulehner A., Wille R.:
Simulation and Design of Quantum Circuits: Reversible Computation: Extending Horizons of Computing, Springer, Cham, Seite(n) 60-82, 2020

11.4. Tagungsband Mitherausgeberschaft (Erstauflage)

Dang K., Küng J., Takizawa M.:
Future Data and Security Engineering - 6th International Conference, FDSE 2019, Nha Trang City, Vietnam, November 27-29, 2019, Serie Lecture Notes in Computer Science, Vol. 11814, Springer, 2019

Dang K., Küng J., Takizawa M., Chung T.:
Future Data and Security Engineering - 7th International Conference, FDSE 2020, Quy Nhon, Vietnam, November 25-27, 2020, Proceedings, Serie Lecture Notes in Computer Science, Vol. 12466, Springer, 2020

Dang K., Küng J., Takizawa M., Chung T.:
TakizFuture Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications - 7th International Conference, FDSE 2020, Quy Nhon, Vietnam, November 25-27, 2020, Proceedings, Serie Communications in Computer and Information Science, Vol. 1306, Springer, 2020

11.5. Aufsatz / Paper in sonstiger referierter Fachzeitschrift

Fischer S., Michelon G., Ramler R., Linsbauer L., Egyed A.:
Automated test reuse for highly configurable software, in Empir. Softw. Eng., Vol. 25, Nr. 6, Seite(n) 5295-5332, 2020

Bonfanti S., Gargantini A., Mashkoor A.:
Design and validation of a C++ code generator from Abstract State Machines specifications, in J. Softw. Evol. Process., Vol. 32, Nr. 2, 2020

Mashkoor A., Arcaini P., Gargantini A.:
Intelligent Autonomous Systems, in Computer, Vol. 53, Nr. 12, Seite(n) 20-23, 2020

Shafiq S., Mashkoor A., Mayr-Dorn C., Egyed A.:
Machine Learning for Software Engineering: A Systematic Mapping, in CoRR, Vol. abs/2005.13299, 2020

Mashkoor A., Egyed A., Wille R.:
Model-driven Engineering of Safety and Security Systems: A Systematic Mapping Study, in CoRR, Vol. abs/2004.08471, 2020

Groza B., Berdich A., Jichici C., Mayrhofer R.:
Secure Accelerometer-based Pairing of Mobile Devices in Multi-modal Transport, in IEEE Xplore, in IEEE Access, Vol. 8, Nr. 1, Seite(n) 9246-9259, 2020

11.6. Aufsatz / Paper in Online-Archiv (nicht-referiert)

Mayrhofer R., Mohan V., Sigg S.:
Adversary Models for Mobile Device Authentication, in arXiv.org, in arXiv, e-Print archive, 2020

11.7. Sonstige

Mashkoor A., Sametinger J., Biró M., Egyed A.:
Security- and safety-critical cyber-physical systems (Editorial), in Journal of Software: Evolution and Process, 2020

12. Anhang: Ausgewählte Presseartikel

12.1. Eröffnung LIT Secure and Correct Systems Lab

JKU: "LIT Secure and Correct Systems Lab eröffnet", in *JKU News & Events*, 17.10.2019

LIT Secure and Correct Systems Lab eröffnet

Mit einem Live-Hack wurde gezeigt, warum das Secure and Correct Systems Lab der JKU so wichtig ist.

Im LIT OIC wurde das LIT Secure and Correct Systems Lab eröffnet.

Daniel Hofer hackt sich mit dem Zugang seines Professors ins Notensystem und gibt sich selbst ein „Sehr gut". Was für Erheiterung und überraschte Gesichter bei der Eröffnung des Secure and Correct Systems Lab der JKU Linz sorgt, zeigt auch, warum es ein solches Lab braucht.

„Sichere und korrekte Systeme wird es in der digitalisierten Welt nur geben, wenn wir deren Entwurf und Nutzung von allen Seiten betrachten. Mit dem LIT Secure and Correct System Lab schaffen wir eine internationale Plattform, die darin beteiligte TechnikerInnen, IngenieurInnen und ProgrammiererInnen zusammenbringt", erklärt Lab-Leiter, Professor Robert Wille. Denn manche Sicherheitsfragen sind

https://www.jku.at/news-events/news/detail/news/lit-secure-and-correct-systems-lab-eroeffnet/ 1/3

physikalischer Natur, andere Softwarefragen und wieder andere durch die Hardware bedingt. „Die digitale Welt ist komplex. Schon allein, weil es so viele Möglichkeiten gibt. Den KonsumentInnen zu sagen, „kümmert euch selbst um eure Sicherheit, das wird nicht ausreichen. Die Systeme müssen schon sicher gebaut werden."

Auch Lab-Leiter, Professor René Mayrhofer betont, dass die Komplexität die große Herausforderung in Sicherheitsfragen sei. „Gerade bei einem Wirtschaftsstandort wie Oberösterreich ist das auch eine Standortfrage. Hier gibt es sehr viel unterschiedliche Industrie mit sehr unterschiedlichen Anforderungen und Fragestellungen, und alle erwarten sich zu Recht, dass es Lösungen für ihre Probleme gibt."

Neben Daniel Hofer und seinem Live-Hack, stellten auch Barbara Lehner und Michael Riegler ihre Forschungsfragen und -ergebnisse vor. Lehner zeigte, dass die Herausforderung der Quantencomputer auch neue Antworten in der Sicherheit braucht und Riegler erklärte, welche Sicherheitsfragen sich durch Smart Homes ergeben können. Eröffnet wurde die Veranstaltung, bei der rund 150 Gäste anwesend waren, von Landesrat Markus Achleitner und Rektor Meinhard Lukas.

sgs: "Neun Institute für eine sichere IT", in *Stadt Rundschau* 43, 24./25.10.2019, S.49

Neun Institute für eine sichere IT

Die JKU treibt die Forschung an sicheren Computer-Systemen voran

LINZ (sgs). „Sichere und korrekte Systeme wird es in der digitalisierten Welt nur geben, wenn wir deren Entwurf und Nutzung von allen Seiten betrachten. Mit dem LIT Secure and Correct System Lab schaffen wir eine internationale Plattform, die darin beteiligte Techniker, Ingenieure und Programmierer zusammenbringt", so Leiter Robert Wille bei der Eröffnung des LIT Secure and Correct Systems Lab.

Rektor Meinhard Lukas (li.) mit Wirtschafts- und Forschungslandesrat Markus Achleitner bei der Eröffnung.

Sichere IT-Systeme

Der Fokus des neuen Labors liegt auf Forschung zu sicheren und korrekten IT-Systemen. Die Forschungsplattform bündelt deshalb die Expertisen verschiedener Disziplinen und steht der Industrie als zentraler Ansprechpartner für Kooperationen zur Verfügung. Durch eine Zusammenarbeit mit der Fachhochschule in Hagenberg wird das Know-how des Labors zusätzlich erweitert.

Von einer weiteren Stärkung des Wirtschaftsstandortes Oberösterreich sprach Wirtschaftslandesrat Markus Achleitner in seiner Eröffnungsrede und betonte die bereits bestehende enge und eingespielte Verzahnung von Wirtschaft und Forschung. Durch das LIT Secure and Correct Systems Lab würden die heimischen Unternehmen doppelt profitieren. Es würden neue marktfähige Dienstleistungen entstehen, die gleichzeitig die Sicherheit fördern.

Kapital für zwei Linzer Start-ups

LINZ (aba). Die Linzer Unternehmen 7lytix und Newsadoo erhalten in Summe zwei Millionen Euro Wachstumskapital von der Raiffeisenlandesbank OÖ. „Start-ups brauchen starke Finanzpartner, die offen sind, schnell entscheiden und sich auch für Visionäres begeistern können", so RLB OÖ-Generaldirektor Heinrich Schaller. Beide Start-ups setzen auf künstliche Intelligenz: Newsadoo bereitet Nachrichten basierend auf individuellen Interessen auf, 7lytix erstellt mit KI-Hilfe Absatzprognosen für Handel und Industrie.

Das Newsadoo-Gründerteam aus Linz.

sib: "Student hackt Laptop des Professors", in *Oberösterreichische Nachrichten*, 18.10.2019, S.8

Student hackt Laptop des Professors

LIT Labor: Bei der Eröffnung eines neuen Speziallabors für Datensicherheit an der Kepler-Uni demonstrieren mehrere Institute, was sie alles können

LINZ. Der Student Daniel will seinem Universitätsprofessor zwei Fragen stellen: Eine hat er ausformuliert und auf einem USB-Stick gespeichert, die zweite stellt er mündlich. – Und zwar in dem Moment, in dem der Professor den Datenträger in seinen Computer steckt. Derart abgelenkt, registriert der Lehrende nicht, dass sich innerhalb weniger Sekunden vom USB-Stick eine Schadsoftware auf seinen Laptop lädt.

Bei der gestrigen Eröffnung eines neuen interdisziplinären Labors an der Kepler Universität, das die Expertise um Datensicherheit und Hard- und Software zusammenführt, zeigt Daniel, dass er sich ab dem Zeitpunkt seine Zeugnisse selber ausdrucken könnte.

Diese Livepräsentation war einer der Programmpunkte bei der Eröffnung des LIT Secure and Correct Systems Lab. „Datensicherheit ist unser Thema. Wir stehen für Sicherheit von der Systementwicklung bis zum richtigen Vernichten von Daten", sagt Universitätsprofessor Robert Wille, der das Lab leitet.

Dazu haben sich neun Uni-Institute unter ein Dach zusammengeschlossen. „Durch die enge Kooperation können wir Techniker, Ingenieure und Programmierer mehr erreichen als die Summe der einzelnen Institute", erklärt Wille.

Neun Doktoranten erhalten unter diesem Dach eine breitere Ausbildung, als es in den Spezialfächern möglich wäre. Gefördert werden diese Jungforscher vom Land Oberösterreich.

Forscherin Barbara Lehner, Wille, Mayrhofer, Achleitner, Lukas, Lab-Assistentin Anja Hoffmann, stellvertretender Lab-Leiter Josef Küng (JKU)

Ein Partner für die Firmen

Wille und sein Stellvertreter Rene Mayerhofer betonen, dass die Kooperation mit heimischen Unternehmen nun einfacher funktionieren sollte. „Es gibt einen Ansprechpartner, der die verschiedenen Disziplinen zusammenbringt." Davon verspricht sich auch Wirtschaftslandesrat Markus Achleitner positive Effekte für die Unternehmen. „Es entstehen nicht nur marktfähige Dienstleistungen, wir erhöhen auch die Sicherheit in Oberösterreichs Wirtschaft."

Auch Rektor Meinhard Lukas ist überzeugt, dass diese Kooperation zu einer besseren Sichtbarkeit der Forschungsleistung führt. Denn auch im internationalen Vergleich sind die Linzer Forschungsleistungen auf diesem Gebiet tonangebend.

Kooperiert wird auch mit der Fachhochschule in Hagenberg und dem Labor für künstliche Intelligenz an der Kepler Uni. Bei der Eröffnung waren auch Banken- und Firmenvertreter dabei, etwa Oberbank-Vorstand Florian Hagenauer, Andreas Aichhorn von Sprecher Automation sowie Christian Altmann von der Business Upper Austria. *(sib)*

Kronen Zeitung

TECHNOLOGIE-INSTITUT

Von autonomen Autos bis hin zur Zahnbürste

(Bild: Sander Hons)

Noch sind die meisten Arbeitsplätze leer, bald wird sich das aber ändern. Am Donnerstag wurde das neue „Secure and Correct Systems Lab" im Linzer Technologie-Institut eröffnet. Im Zentrum der Forschung steht, Sicherheitsprobleme zu bekämpfen. Diese reichen von autonomen Autos bis zur elektronischen Zahnbürste.

Smartphone, selbstfahrende Staubsauger und Rasenmäher, Chipschlüssel oder ganze Smart Home-Anlagen sind in unseren Alltag integriert. Bereits jeder vierte Österreicher erleichtert sich seinen Haushalt mit zumindest einem „smarten" Angebot. Diese Geräte sind permanent online und vernetzt. Was natürlich auch Gefahren eines Hackerangriffs fördert. Bei einer Demo zeigten Experten, wie leicht man sich teilweise in solche Netze hacken und die Wohnungstüre per Klick öffnen kann. Durch das Zusammenspiel von Informatikern, Technikern und Physikern am neuen „Secure and Correct Systems Lab" auf der JKU sollen diese Sicherheitslücken erforscht und bekämpft werden.

Sicherheit für Oberösterreichs Wirtschaft

„Vom LIT ‚Secure and Correct Systems Lab' profitieren die heimischen Unternehmen aber gleich doppelt. Es entstehen dadurch nicht nur marktfähige Dienstleistungen im Land, sondern diese neuen Dienstleistungen schaffen vor allem auch Sicherheit für Oberösterreichs Wirtschaft", freut sich Wirtschafts-Landesrat Markus Achleitner.

„Keine Wunderdinge erwarten"

Die Experten im neuen Labor freuen sich endlich mit ihrer Forschung starten zu können, treten aber auf die Euphoriebremse. „Man darf sich keine Wunderdinge von uns erwarten. Security-Probleme bedürfen langer und harter Arbeit. Von manchen Problemen wissen wir bereits seit 30 Jahren Bescheid, machen die Fehler aber trotzdem noch immer", so Professor Robert Wille.

Philipp Zimmermann, Kronen Zeitung

krone.at

JOHANNES KEPLER UNIVERSITÄT

LIT Secure and Correct Systems Lab eröffnet

18. Oktober 2019, 12:00 Uhr • 61× gelesen • 0 • 0 •

Rektor Meinhard Lukas (links) mit Wirtschafs- und Forschungslandesrat Markus Achleitner bei der Eröffnung des neuen LIT Secure and Correct Systems Lab. • Foto: JKU • hochgeladen von Silvia Gschwandtner

Autor: Silvia Gschwandtner aus Linz

Die interdisziplinäre Forschungsplattform vereint neun Institute der Johannes Kepler Universität (JKU) und deckt damit von der Erstellung bis zur Wartung alle Aspekte von Sicherheitssystemen ab. Als zentraler Ansprechpartner steht sie für Kooperationen mit Unternehmen zur Verfügung.

LINZ. „Sichere und korrekte Systeme wird es in der digitalisierten Welt nur geben, wenn wir deren Entwurf und Nutzung von allen Seiten betrachten. Mit dem LIT Secure and Correct System Lab schaffen wir eine internationale Plattform, die darin beteiligte Techniker, Ingeneure und Programmierer zusammenbringt", erklärte Leiter Professor Robert Wille am Donnerstag bei der Eröffnung des LIT Secure and Correct Systems Lab.

Forschung zu sicheren IT-Systemen im Fokus

Der Fokus des neuen Labs liegt auf Forschung zu sicheren und korrekten IT-Systemen auf höchstem internationalen Niveau. Die institutsübergreifende, interdisziplinäre Forschungsplattform bündelt deshalb die Kompetenzen und Expertisen verschiedener Disziplinen, fördert Synergien und steht der Industrie als zentraler Ansprechpartner für Kooperationen zur Verfügung. Durch eine Kooperation mit dem der Fachhochschule Hagenberg wird das Know-how zusätzlich erweitert.

Heimische Unternehmen profitieren doppelt

Von einer weiteren Stärkung des Wirtschaftsstandortes Oberösterreich sprach Wirtschaftslandesrat Markus Achleitner in seiner Eröffnungsrede und betonte die bereits bestehende enge und eingespielte Verzahnung von Wirtschaft und Forschung. Durch das LIT Secure and Correct Systems Lab würden die heimischen Unternehmen doppelt profitieren. Es würden neue marktfähige Dienstleistungen entstehen, die gleichzeitig die Sicherheit fördern.

12.2. Synergien

JKU: "Superkomplexe Simulationen für die Rechner von Morgen':
ForscherInnen bereiten das Quantencomputing-Zeitalter vor", in *JKU News & Events*, 06.12.2019

Superkomplexe Simulationen für die Rechner von „Morgen": ForscherInnen bereiten das Quantencomputing-Zeitalter vor

Was lange wie Science Fiction klang, soll bald Realität sein: Quantencomputer, die schneller als Supercomputer hochkomplexe Berechnungen durchführen können.

von links: Doktor Jürgen Fuß (FH OÖ Campus Hagenberg), Dissertant Thomas Grurl und Prof. Robert Wille (JKU)

InformatikerInnen der FH Oberösterreich (FH OÖ), Campus Hagenberg, und der Johannes Kepler Universität Linz (JKU) setzen nun gemeinsam ihr Know-how ein, um auf die neue Technologie vorzubereiten.

Gemeinsam entwickeln und testen das JKU Institut für Integrierte Schaltungen und das FH OÖ Department Sichere Informationssysteme Algorithmen, die bei Quantencomputern zum Einsatz kommen – hochkomplexe Formeln, die diese Hochleistungsrechner quasi programmieren.

Diese Quantenalgorithmen können heute bereits auf den ersten kommerziell nutzbaren Quantenrechnern mit 20-30 Quantenbit (Qubit) Rechenleistung ausgeführt werden, wie sie Google oder IBM seit Kurzem über Cloud-basierte Lösungen zur Verfügung stellen. Und bald schon könnten den NutzerInnen noch leistungsfähigere Prozessoren zur Verfügung stehen, denn beide Unternehmen haben Rechner mit über 50 Quantenbits entwickelt.

Doch nicht jeder Quantenalgorithmus lässt sich sofort fehlerfrei auf Quantencomputern ausführen. Deswegen werden sie zunächst „in kleinem Maßstab" mit Hilfe von Simulatoren entwickelt und getestet, bevor sie schließlich auf der echten Maschine ausgeführt werden. Dabei kann nicht nur die Funktionalität des Algorithmus simuliert werden, sondern auch das konkrete physikalische Verhalten korrekt repräsentiert werden – inklusive möglicher Fehler, die bei Quantencomputern nicht vermeidbar sind.

Dieses hochkomplexe Unterfangen nennt sich „Quantensimulation", und in eben diesem Bereich besitzen das JKU Institut für Integrierte Schaltungen unter der Leitung von Prof. Robert Wille und das FH OÖ Department „Sichere Informationssysteme" mit dem Team von Dr. Jürgen Fuß mehrjährige Expertise.

„Wir haben festgestellt, dass sich unser Know-how perfekt ergänzt und beschlossen, unsere Kräfte zu bündeln, um die Entwicklung von Quantencomputern vorzutreiben und hier in Oberösterreich Pionierarbeit zu leisten", sagen Fuß und Wille, die mit ihren Teams seit dem Frühjahr 2019 eng zusammenarbeiten.

An der JKU wird unter der Leitung von Prof. Robert Wille bereits seit vier Jahren an Simulations- und Entwurfsmethoden für Quantencomputer geforscht, wofür sein Institut bereits mehrmals unter anderem von Google und IBM ausgezeichnet wurde. Die hier entwickelten Methoden erlauben es, Anwendungen „auf Knopfdruck" in Beschreibungen zu überführen, mit denen der Quantenrechner arbeiten kann.

Das vierköpfige Team von Dr. Jürgen Fuß am FH OÖ Campus Hagenberg arbeitet seit zwei Jahren an der Entwicklung von Werkzeugen zur Programmierung von Quantencomputern und testet sie auf der campus-eigenen Quantum Learning Machine der Firma Atos, einem der weltweit leistungsfähigsten kommerziell erhältlichen Quantensimulatoren.

Schon heute ist die Simulations-Expertise aus Oberösterreich international gefragt. So finden sich die hier entwickelten Methoden bereits in den offiziellen Entwurfswerkzeugen von IBM und Atos. Mit Unternehmen wie IBM, Google, Microsoft oder Atos, die sich in diesem Gebiet engagieren, steht die ExpertenInnen der FH OÖ und JKU in regelmäßigem Kontakt.

Die ForscherInnen der beiden oberösterreichischen Hochschulen sehen für ihre Arbeit vielfältige Anwendungsgebiete, nicht nur für Finanzdienstleister, die Logistik- und Transportbranche oder Automobilkonzerne, die bereits in die neue Technologie investieren. Mit Quantencomputing können enorme Fortschritte z. B. in der Verkehrsplanung und Stauvermeidung, der Medikamentenentwicklung, der Simulation von Klimaveränderungen und dem Schutz von Informationen durch neue Verschlüsselungsverfahren erzielt werden.

Autor unbekannt: "JKU und FH läuten gemeinsam ein neues Computer-Zeitalter ein",
in *Oberösterreichische Nachrichten*, 14.12.2019, S. 41.

JKU und FH läuten gemeinsam ein neues Computer-Zeitalter ein

Internationales Interesse an Forschungsergebnissen ist groß

LINZ. Ein Computer, der hochkomplexe Problemstellungen schneller als alle anderen Supercomputer weltweit lösen kann – was wie Science-Fiction klingt, soll in Oberösterreich bald Realität werden. Informatiker der FH Oberösterreich, Campus Hagenberg, und der Johannes Kepler Universität Linz arbeiten gemeinsam an der Entwicklung eines Quantencomputers.

„Wir haben festgestellt, dass sich unser Know-how perfekt ergänzt, und beschlossen, unsere Kräfte zu bündeln, um die Entwicklung von Quantencomputern voranzutreiben", sagt Robert Wille, Leiter des JKU-Instituts für Integrierte Schaltungen: „Hier in Oberösterreich wollen wir Pionierarbeit leisten." Gemeinsam entwickeln und testen das JKU-Institut und das Department „Sichere Informationssysteme" der FH Hagenberg seit dem Frühjahr Algorithmen, die beim Programmieren von Quantencomputern zum Einsatz kommen.

„Unser Know-how ergänzt sich perfekt. Darum haben wir beschlossen, unsere Kräfte zu bündeln."

Robert Wille, Leiter des JKU-Instituts für Integrierte Schaltungen

Erfolge der Vergangenheit geben den beiden Instituten recht und zeigen einen künftigen Weg vor. Schon heute ist die Expertise aus Oberösterreich international gefragt. Immerhin stehen die Experten der Fachhochschule und der Johannes Kepler Universität in regelmäßigem Kontakt mit Software-Unternehmen wie IBM, Google, Microsoft oder Atos.

DERSTANDARD

INNOVATIONEN

Neue Photonenquelle für bessere Quantennetzwerke

Von Forschern der Uni Linz mitentwickeltes System erzeugt Photonenpaare in bisher unerreichter Qualität und Rate

24. April 2019, 10:59

Für die abhörsichere Übertragung von Daten in zukünftigen Quantennetzwerken werden spezielle Lichtquellen benötigt, die quantenmechanisch verschränkte Photonenpaare produzieren. Eine internationale Kooperation unter Beteiligung der Universität Linz hat nun im Fachjournal "Nature Nanotechnology" [http://dx.doi.org/10.1038/s41565-019-0435-9] ein neues System vorgestellt, das Photonenpaare in bisher unerreichter Qualität und Rate erzeugen kann.

In Form von Fernsehgeräten halten sogenannte Quantenpunkte – das sind Nanostrukturen aus halbleitenden Materialien – gerade Einzug in den Alltag. An der Universität Linz dagegen wird versucht, solche winzigen Strukturen für die Quantenkommunikation nutzbar zu machen. "Das physikalische Grundprinzip ist durchaus mit dem der neuen Fernseher vergleichbar", sagte Armando Rastelli vom Institut für Halbleiter- und Festkörperphysik der Universität Linz, einer der Autoren der aktuellen Studie. "Beim Fernseher bestimmt die Größe der Quantenpunkte die Farbe des abgestrahlten Lichts. Wir dagegen verändern die Struktur der Punkte, um den Verschränkungsgrad der emittierten Photonenpaare zu optimieren."

Bessere Quantenkommunikation

Verschränkte Photonen stehen auch über beliebig große Distanzen hinweg in Wechselbeziehung zueinander – eine Eigenschaft, die für die Quantenkommunikation von größter Bedeutung ist. Die Erzeugung solcher Paare für technologische Anwendungen stellt aber nach wie vor eine große Herausforderung dar. Es muss sowohl die Qualität der Verschränkung möglichst hoch sein, was bedeutet, dass die erzeugten Photonenpaare mit einer möglichst hohen Wahrscheinlichkeit auch wirklich miteinander verschränkt sein sollen. Zum anderen müssen die erzeugten Paare möglichst ähnlich sein, damit sie sich nicht von einander unterscheiden lassen. In beiden Bereichen haben Forscher der Universität Linz in den letzten Jahren bereits internationale Bestmarken gesetzt.

Eine weitere Anforderung an die ideale Photonenquelle ist die Helligkeit, also die Rate, mit der verschränkte Photonen erzeugt werden. Hier haben chinesische Forscher ein Konzept entwickelt, das die in einem Quantenpunkt erzeugten Lichtteilchen zuverlässig in eine

bestimmte Richtung lenkt. Das minimiert die Verluste und erlaubt es, mehr der erzeugten Photonenpaare für die eigentliche Anwendung verfügbar zu machen. Dabei verhindert eine spezielle Gitterstruktur um den Punkt herum eine Ausbreitung der Photonen zur Seite, während ein Spiegel hinter dem Punkt diejenigen Photonen zurückwirft, die sonst verloren gehen würden.

Zukunftshoffnung

In den aktuellen Experimenten konnten nun die Expertisen aus Linz und China erfolgreich vereint werden. "Die Quantenpunkte beziehungsweise das Know-how für deren Herstellung stammt von uns, die Experimente haben schließlich die chinesischen Kollegen durchgeführt", sagte Rastelli.

So ist es gelungen, eine Quelle für verschränkte Photonen zu realisieren, die die unterschiedlichen Qualitätsmerkmale miteinander vereint. Zwar handelt es sich dabei noch um Grundlagenforschung und Rastelli zufolge sind noch einige Probleme auf dem Weg zur technologischen Anwendung zu lösen. Dennoch sind die Forscher zuversichtlich, dass ihr System einen wichtigen Schritt in der Weiterentwicklung aktueller Quantentechnologien darstellt. (APA, 24.04.2019)

12.3. Ehrungen

JKU: "Jung und innovativ: zwei JKU-Forscher ausgezeichnet",
in *JKU News & Events*, 06.06.2019

Jung und innovativ: zwei JKU-Forscher ausgezeichnet

JKU-Forscher erhielten Auszeichnung bei weltweit größter Tagung für Entwurfsautomatisierung.

Die weltweit größte Tagung für Entwurfsautomatisierung hat den JKU Professor Robert Wille heuer mit dem Under-40 Innovators Award ausgezeichnet. Auf der gleichen Tagung wurde zudem JKU-Doktorand Alwin Zulehner für sein Dissertationsprojekt ausgezeichnet.

Der Entwurf eines Smartphones, die Simulation von Quantencomputern, die Verbesserung von Suchmaschinen oder die automatische Interpretation von gesetzlichen Regularien – dies sind nur einige von zahlreichen Beispielen, mit denen sich Prof. Robert Wille in den letzten Jahren einen Namen gemacht hat. Ganz in der

Tradition der Linzer Ingenieurskunst hat der Informatiker dabei regelmäßig die Grenzen seines Faches überschritten und interdisziplinär mit Anknüpfungen an die Elektrotechnik, Quantenphysik, Medizin oder den Rechtswissenschaften gearbeitet. Seine Beiträge haben dabei nicht nur wissenschaftlich überzeugt, sondern wurden von namenhaften Firmen wie Infineon, IBM, Google oder AMD sowie verschiedenen mittelständigen Unternehmen aufgegriffen.

Das all diese Beiträge in vergleichsweise jungen Jahren erbracht wurden führte nun schließlich dazu, dass Robert Wille mit dem Under-40 Innovators Award ausgezeichnet wurde. Der Preis ehrt Personen, welche nicht älter als 40 Jahre sind und trotzdem bereits herausragende Innovationen im Bereich der Entwurfsautomatisierung erzielt haben. Die Preisträger zählen zum „Who's Who" der Branche und gelten als Personen, welche die Zukunft des Gebietes definieren und gestalten. Der Preis wurde im Rahmen der Design Automation Conference übergeben – der weltweit größten Tagung für Entwurfsautomatisierung, welche jährlich mehr als 1000 WissenschaftlerInnen zusammenbringt.

Doch damit nicht genug: Auf der gleichen Tagung wurde auch Alwin Zulehner für sein Dissertationsprojekt ausgezeichnet. Darin beschäftigt er sich mit Quantenrechnern – einer neuen Technologie, welche für bestimmte Anwendungen konventionellen Computern überlegen ist. Obwohl noch im Grundlagenstadium, entwickelt Alwin Zulehner hier Methoden, mit denen man bereits heute über Simulation mit diesen Rechnern der Zukunft arbeiten kann. Für seine Beiträge wurde er auf der Design Automation Conference mit einem Best Poster Award ausgezeichnet.

Zu den Personen:
Robert Wille ist seit Oktober 2015 Professor für Integrierten Schaltkreis- und Systementwurf und wurde im Alter von 32 Jahren als einer der jüngsten Professoren an die JKU berufen. Seitdem leitet er das Institut für Integrierte Schaltungen im Fachbereich Informatik. Kürzlich übernahm er zudem die Leitung des neu gegründeten LIT Secure and Correct Systems Lab der JKU. In seiner Karriere hat er über 200 wissenschaftliche Artikel in Zeitschriften und Tagungen sowie mehrere Bücher zum Entwurf von Schaltungen und Systemen veröffentlicht. Neben dem Under-40 Innovators Award wurde er in der Vergangenheit unter anderem auch mit einem Young Researcher Award, einem Google Faculty Research Award, Best Paper Awards und weiteren Ehrungen ausgezeichnet.

Alwin Zulehner hat 2015 an der JKU sein Masterstudium abgeschlossen und arbeitet seit Jänner 2016 am Institut für Integrierte Schaltungen. Seine Forschungsarbeiten umfassen die Entwicklung neuer Entwurfs- und Simulationsverfahren für neue Computertechnologien und insbesondere für Quantenrechner. Seine Arbeiten finden bereits Anwendung in offiziellen Tools von IBM. Seine Dissertationsarbeiten, für die er bereits in der Vergangenheit ausgezeichnet wurde, wird er im Sommer diesen Jahres an der JKU abschließen.

DESIGNLINES

Where IoT, AI & Quantum Computing Meet

LAS VEGAS — Where do IoT, AI and Quantum Computing intersect? The short answer is that they meet where data is growing exponentially. The long answer is... well, it's complicated.

Last week, a panel at the Design Automation Conference (DAC) drilled deep into this difficult topic. Participating were the winners of the "2019 Under 40 Innovation Awards" — young engineers and researchers working on next-generation technologies.

The panelists, all eager for the dawn of a new era in design automation, called upon the electronic design automation (EDA) industry for more sophisticated tools to help them advance the Internet of things (IoT), artificial intelligence (AI) and even quantum computing.

But given the slowdown of Moore's Law, what more can design automation contribute to electronic design? How exactly does EDA connect with AI?

Vijay Raghunathan, professor of electrical and computer engineering at Purdue University, explained: "One of the things EDA did for designs in general is to convert what was basically dark art [i.e. electronic design] into a very structured science."

Raghunathan continued: "If you talk to AI researchers today, you realize the design of these algorithms and neural networks is really a dark art. One of the most interesting things going forward is to see if EDA can bring the same level of rigorous structure to the design of neural networks and design of AI algorithms." He added, "To me, that is one of the most interesting aspects that connects the world of EDA with the world of AI."

2019 Under 40 Innovation Awards Panel at DAC

New-generation researchers also expect EDA tool vendors to jump into quantum computing — not in a few years, but today.

Robert Wille, a professor at Johannes Kepler University in Linz, Austria, said, "Everybody knows about Moore's Law and design gaps we've experienced in decades with conventional computing technology." Despite the widespread belief that the era of quantum computing is still far away, Wille stressed: "It makes absolutely sense for the design automation industry to start developing efficient and sophisticated EDA tool for Quantum Computing -- right now."

What is quantum computing for?

The panel, consisting of winners of this year's Under-40 Innovation Awards, included Huichu Liu, a staff research scientist at Intel, Rasit Onur Topaloglu, senior hardware developer and program manager at IBM, Wille, and Raghunathan.

Yunji Chen, professor at the Institute of Computing Technology, Chinese Academy of Sciences, was another honoree, but couldn't participate because he was not able to get a U.S. visa in time.

Recommended

IEEE, Tear Down This Wall

Given their diverse backgrounds, the panel covered a lot of ground, touched on diverse topics that ranged from IoT to AI and quantum computing.

For a layman, quantum computing is a mystery beyond solution. Asked why the world needs quantum computing, Wille said, "First, it's important to understand that the quantum computer is not replacing the conventional computer we know."

Instead, he said, it will be one of the many computing technologies of the future. The tech world has high hopes for quantum computers, which show promises, for example, in accelerating the exploitation of huge search bases.

"But the first killer app for quantum computing is what's known as Shor's algorithm — a quantum algorithm — developed years ago," Wille explained. "The algorithm will help make factorization much more efficient. This is still considered as the holy grail of quantum computing, as [many believe] this will change the entire world [in theory]." But in reality, "This is still the furthest away."

Robert Wille

In recent years, as big industry players such as IBM, Google and Microsoft Research jump into the fray, the quantum computing community is seeing the emergence of new commercial applications. For example, quantum computers can be used "for simulating climate change, solving optimization problems ... or... quantum chemistry is a huge topic," said Wille.

So, although the quantum computer's big goal of factorization is still far away, "We see today a variety of applications where [the use of] quantum computer may be beneficial," said Wille.

Vijay Raghunathan

As promising as this prospect might sound, Purdue's Raghunathan cautioned tha there are big challenges in quantum computing. "From an outsider's perspective see there is a class of very hard problems — computationally hard problems — where quantum computing holds a lot of promise." Solving optimization probler is one, by computing in the exponential space, for example, Raghunathan. "But t challenge is, how do you really extract true benefits [of quantum computing] for class of really wide-spread hard computational problems which seem to be all over the place?"

Infrastructure for quantum computing

Obviously, none of the young innovators expects the EDA industry to stand still. By stressing the need for automation tools for quantum computers, Wille said, "We need them to find out what's possible to fabricat and what's possible to design." He said, "We need to be prepared for the day when quantum computing becomes scalable."

IBM's Rasit Onur Topaloglu, another young innovation award winner, noted, "We also thought about this problem at IBM...we asked, when do we need automation tools to design quantum computing?"

He said, "We've concluded that up until 200 qubits, maybe we can still do it manually." He added, "I am not going to project when we will reach 200 qubits, but we already have an 80 qubits architecture." Although there is at least a seven year-gap from academic research to a product, he concluded that the research for design automation tools for quantum computing needs to start today. "When the idea [of quantum computing] takes off, we need those tools in the industry right away."

Rasit Onur Topaloglu

informatik austria

DER QUELLCODE DER ZUKUNFT

≡ Menü

Design Automation: Auszeichnung für Robert Wille

6. Juni 2019 von jkulinz

Die Design Automation Conference gilt als eine der wichtigsten Konferenzen in diesem Bereich und fand 2019 bereits zum 56. Mal statt. Insgesamt wurden fünf junge Top-Innovatoren im Rahmen der Eröffnungsveranstaltung am 3. Juni geehrt. Beim „Young

Under 40 Innovators Award Panel" diskutierten die Preisträger gemeinsam über die Themen Quantencomputer, Künstliche Intelligenz und Internet der Dinge.

Unter den Ausgezeichneten: Professor Robert Wille von der JKU Linz. Wille ist Experte für die Entwicklung von Methoden zur Entwurfsautomatisierung, die er nicht nur für den Entwurf konventioneller Schaltungen und Systeme, sondern auch für Zukunftstechnologien (einschließlich Quantencomputer, reversible Schaltungen, mikrofluidische Biochips usw.) sowie für ergänzende Bereiche wie die partikelbasierte Simulation einsetzt. Als interdisziplinärer Forscher überschreitet er dabei häufig die Grenzen zwischen Informatik, Elektrotechnik, Quantenphysik, Medizin oder auch Rechtswissenschaften. Die von ihm entwickelten Methoden wurden von namenhaften Unternehmen wie Infineon, IBM oder AMD aufgegriffen.

JKU: "SOKO JKU – KI zur besseren Fingerabdruckerkennung – JKU kürte Jung-Informatiker", in *JKU News & Events*, 20.12.2019

SOKO JKU - KI zur besseren Fingerabdruckerkennung – JKU kürte Jung-Informatiker

Auch heuer wurden vier Absolventinnen der JKU mit dem Adolf-Adam-Informatikpreis ausgezeichnet.

von links: Alfred Hiebl (Firma MIC), Philipp Schwarz

Für seine Masterarbeit „SOKO JKU - KI zur besseren Fingerabdruckerkennung" durfte sich Philipp Schwarz vom LIT Secure and Correct Systems Lab über den ersten Platz freuen. JurorInnen waren wie immer Oberstufen-SchülerInnen aus ganz Oberösterreich.

Zuschauerrekord: Zur Preisverleihung kamen mehr als 500 SchülerInnen. Sie kürten Philipp Schwarz für seine am Institut für Computational Perception verfasste Arbeit

zum Sieger. *„Meine Arbeit beschäftigt sich ganz allgemein mit dem Verarbeiten von Fingerabdrücken. Anders als herkömmliche Algorithmen schafft es mein Programm, aus Fingerabdrücken von besonders schlechter Qualität ein präzises Orientierungsfeld zu berechnen"*, so der Preisträger.

Auf den weiteren Plätzen landeten **Daniel Hofer** ((Un)sichtbare Wasserzeichen - Gestohlenen Webseiten auf der Spur), **Johannes Lehner** (PatchNet - Wie selbstfahrende Autos lernen, die Welt in 3D wahrzunehmen) und **Raphael Mosaner** (On-stack Replacement - Turbobeschleunigung von Programmschleifen).

Beeindruckende Qualität und Vielfalt

Für den Preis konnten sich AbsolventInnen der JKU-Masterstudien Computer Science und Bioinformatik bewerben, die ihr Masterstudium im vergangenen Studienjahr abgeschlossen haben und deren Arbeit mit „Sehr gut" beurteilt wurde. In einer Vorauswahl durch eine Fachjury wurden die besten vier ausgewählt. *„Die vier Finalisten zeigten nicht nur ihr IT-Know-how, sondern auch ein Talent, dieses Wissen einfach zu vermitteln. Wir freuen uns, dass sie diese Fähigkeiten heuer vor einem Rekordpublikum zeigen konnten"*, zeigte sich die Juryvorsitzende Univ.-Prof.in Gabriele Kotsis von der Qualität und Vielfalt der Arbeiten beeindruckt.

Über den Preis und seinen Namensgeber

Der mit 1.500 Euro dotierte Informatikpreis wurde gemeinsam mit Hauptsponsor MIC, der Österreichischen Computer Gesellschaft, der IT rocks Initiative und der Österreichischen Gesellschaft für Informatik vergeben. *Der Namensgeber* Univ.-Prof. Adolf Adam (1918-2004) war österreichischer Statistiker und Informatiker. Er wurde 1966 an die Hochschule für Sozial- und Wirtschaftswissenschaften nach Linz berufen und erstellte das Linzer Informationswissenschaftliche Programm (LIP), mit dem er den Weg zur Etablierung der Informatik als anerkannte Studienrichtung ebnete. Linz war 1969 die erste österreichische Universität, an der ein Informatikstudium eingerichtet wurde. Auf Adams Betreiben erfolgte 1971 auch die Umbenennung in Johannes Kepler Universität Linz.

Auf den Spuren des Sherlock Holmes

Philipp Schwarz gewann mit seiner Masterarbeit den Adolf-Adam-Preis

VON VALENTIN BAYER

SOKO JKU – KI zur besseren Fingerabdruckerkennung" – unter diesem Motto präsentierte Philipp Schwarz seine Masterarbeit vor 500 Oberstufenschülern aus ganz Oberösterreich. Er setzte sich damit gegen drei seiner Studienkollegen von der JKU durch und sicherte sich den Adolf-Adam-Preis. Der Trauner beschäftigte sich damit, wie selbst besonders schlechte oder schwache Fingerabdrücke digital verarbeitet werden können. Dazu trainierte der 26-Jährige ein neuronales Netzwerk, also eine lernfähige künstliche Intelligenz. „Mein Programm ist jetzt wesentlich besser als herkömmliche Algorithmen", sagt Schwarz.

Dass er nach der Matura am BRG Traun in der Informatik landen würde, war nicht von vornherein klar. „Ich habe mich einfach für Mathematik interessiert, wollte aber nicht nur das Fach an sich studieren", erzählt er. Nach einem Blick ins Studienangebot der Johannes-Kepler-Universität landete er im Studiengang Informatik. Damit scheint er sich wohlgefühlt zu haben, denn auch im Masterlehrgang „Networks and Security" widmete er sich dem Programmieren. Dort landete er auch bei der Disziplin der Biometrie, also der Vermessung von Lebewesen, in die auch Fingerabdruckerkennung fällt.

Seit September hat Schwarz den Master in der Tasche, jetzt macht er sich an seine Doktorarbeit. „Es wird wahrscheinlich in Richtung Gangerkennung gehen. Man kann Menschen ja nicht nur am Fingerabdruck, sondern zum Beispiel auch an der Gangart erkennen."

Mit dem neuen Gehalt macht sich Schwarz auf Wohnungssuche in Linz, er will näher am Arbeitsplatz wohnen. Nach Feierabend findet Schwarz im Sport einen Ausgleich. Seit zwei Jahren geht er regelmäßig zum Bouldern, eine Variation des Kletterns, bei der ohne Sicherung nur so hoch geklettert wird, dass der Absprung auf den gepolsterten Hallenboden ungefährlich bleibt. Außerdem liebt Schwarz Volleyball und Fußball. „Im Verein spiele ich zwar nicht mehr, aber für ein Match mit Freunden bin ich immer zu haben."

Foto: privat

„Ich habe mich einfach für Mathematik interessiert, wollte aber nicht nur das Fach an sich studieren."

Philipp Schwarz, Gewinner des Adolf-Adam-Preises

JKU
TNF / INF
FMV

team
contact
software
publications
teaching
jobs

GCAI'18 / BRAIN'19 Best Poster and Interaction Award

Best poster and interaction award

Sibylle Möhle, Armin Biere.
Combining Conflict-Driven Clause Learning and Chronological Backtracking for Propositional Model Counting.
In Proc. 5th Intl. Global Conf. on Artificial Intelligence (GCAI'19).
EPiC Series in Computing, 14 pages, EasyChair 2019, to appear.

[preprint] award]

SATALIA

15. November 2019

JKU-Informatiker unter den Top 3 bei internationalem Quantencomputer Wettbewerb

Als Titelverteidiger gestartet konnten sich die Linzer auch dieses Jahr wieder bei der IBM Quantum Challenge gegen Teams aus aller Welt durchsetzen.

Wissenschaftlerinnen und Wissenschaftler aber auch namhafte Firmen liefern sich ein Wettrennen um den ersten praktisch anwendbaren Quantencomputer. Nicht zuletzt Google und IBM dominieren die Diskussion darum, wer zuerst die Überlegenheit dieser neuen Computertechnologie im Vergleich zu unseren bisherigen Rechnern zeigen kann. Neben Fragen der physikalischen Machbarkeit rückt damit auch immer mehr die Informatik in den Fokus – Quantencomputer müssen ja auch korrekt „programmiert" werden.

Informatikerinnen und Informatiker der Johannes Kepler Universität sind hier bereits seit Jahren weltweit an der Spitze. Dies zeigte sich auch heuer wieder bei der IBM Quantum Challenge, in welcher Teams aus aller Welt ihr Können bei der Erstellung von Quantenalgorithmen unter Beweis gestellt haben. Da das Team um Prof. Robert Wille vom Institute for Integrated Circuits und dem LIT Secure and Correct Systems Lab letztes Jahr Platz 1 erreichte, war der Druck als Titelverteidiger heuer besonders groß.

Nachdem über 700 Teilnehmerinnen und Teilnehmer an insgesamt drei Vorrunden teilnahmen, fand nun schließlich das große Finale mit den verbliebenen 40 besten Teams statt. Die Aufgabe: Wie lassen sich in einem fiktiven Stadtteil von Tokio verschiedene Supermärkte so verteilen, dass benachbarte Viertel von unterschiedlichen Unternehmen versorgt werden – ein typisches Optimierungsproblem, das sich mit Quantencomputer perspektivisch schneller lösen lässt als mit konventionellen Rechnern.

Nun stehen die Ergebnisse fest: Die Lösung der JKU-Informatiker konnte das Problem mit am schnellsten lösen und beförderte das Team in die Top 3 des Wettbewerbs. Damit zeigt sich, dass die Linzer nicht nur heutige Computer beherrschen, sondern auch für zukünftige Computertechnologie bestens gewappnet sind.

Das JKU-Team (Lukas Burgholzer, Robert Wille, Hartwig Bauer, Stefan Hillmich) mit einem Ausdruck ihres Quantenalgorithmus (Foto: Daniel Hofer, Michael Riegler)

Quantencomputer "programmieren": Best Paper Award für JKU Informatiker

JKU Forscher*innen arbeiten an Algorithmen für Quantencomputer. Jetzt wurden sie dafür von einer führenden Fachzeitschrift ausgezeichnet.

von oben: Alwin Zulehner, Robert Wille, Alexandru Paler

Das JKU Institut für Integrierte Schaltungen und das LIT Correct and Secure System Lab ist seit einigen Jahren führend an der Entwicklung von Methoden zu „Programmierung" von Quantenrechnern beteiligt. Dafür gab's nun eine Auszeichnung.

Es wird immer deutlicher, dass Quantencomputer in naher Zukunft klassische Rechner für bestimmte Aufgaben ersetzen werden. Umso dringender notwendig sind die Grundlagen, wie solche Maschinen in Zukunft korrekt „programmiert" werden. Die JKU Informatik arbeitet hier schon seit vielen Jahren an entsprechenden Methoden, die auch direkt für Quantenrechner z.B. von IBM und Google genutzt werden können. Die entsprechenden Ergebnisse werden dabei regelmäßig in den führenden Fachzeitschriften und Konferenzen veröffentlicht, wo sich „JKQ" als JKU Plattform für den Entwurf von Quantencomputern mittlerweile etabliert hat.

Eine besondere Auszeichnung erreichte das Team unter Leitung von Prof. Robert Wille (Vorstand des Instituts für Integrierte Schaltungen/LIT Correct and Secure System Lab und Wissenschaftlicher Leiter am Software Competence Center Hagenberg) nun mit dem Erhalt des Donald O. Pederson Best Paper Award der IEEE Transactions on Computer-Aided Design. Damit zeichnet die führende Fachzeitschrift im Bereich des computergestützten Entwurfs einmal jährlich die beste Arbeit der vergangenen zwei Jahre aus. Aus knapp 500 Arbeiten, von denen es 14 in die engere Wahl geschafft haben, wurde schließlich die Arbeit aus Linz ausgewählt.

12.4. LIT Secure and Correct Systems Lab und LIT OIC

Popovsky, Julia: "Was sich hinter den Mauern des LIT verbirgt",
in *Oberösterreichische Nachrichten Campus* 68, 17.10.2019, S. 6

Was sich hinter den Mauern des LIT verbirgt

Dort werden nicht nur Bauteile gefertigt, sondern auch kreative Unternehmensideen und digitale Zwillinge kreiert

„In der Factory wird der gesamte Kreislauf von der Planung über die Produktion bis zur Wiederverwertung von Kunststoffen durchgedacht."

Das erste Start-up im LIT

Dominic Girardi verrät, was den Reiz ausmacht

DATEN UND FAKTEN

435 Tage lang ...

240 Arbeitsplätze ...

25 ...

Die neuen Gesichter der TNF

Gleich acht neue Professoren forschen und lehren an der TN-Fakultät der JKU. Hier stellen wir sie vor - heute Daniel Große.

Professor Daniel Große

Prof. Daniel Große ist 43 Jahre alt und stammt aus Weimar (Deutschland). Er ist Vorstand des Instituts für Complex Systems. Wie seine Arbeit die Welt verbessern kann und welches Kartenspiel er am liebsten spielt erzählt er im Interview.

In welchem Bereich forschen Sie?
Prof. Daniel Große: Ich beschäftige mich in der Forschung mit verlässlicher Elektronik. Diese prägt bereits jetzt unseren Alltag, wird aber immer komplexer, wenn man z.B. an autonome Fahrzeuge denkt. Mein Forschungsschwerpunkt liegt darin, das korrekte Zusammenspiel von Hardware und Software abzusichern.

Warum haben Sie sich für die JKU entschieden?
Prof. Daniel Große: Mich reizt besonders die Arbeit an einer forschungsstarken Universität mit engen Industriekooperationen. Das Linz Institute of Technology (LIT) bietet hier einen idealen Rahmen und ich habe schon erste Kontakte mit dem LIT Secure and Correct Systems Lab geknüpft.

Was begeistert Sie an diesem Bereich?
Prof. Daniel Große: Die enge Verknüpfung von Theorie und Praxis. So fließen

beispielsweise Forschungsergebnisse von mir in die IEEE-Standardisierung ein.

Wofür ist diese Forschung überhaupt notwendig bzw. wie verbessert sie unser Leben?
Prof. Daniel Große: Im Grunde geht es darum dafür zu sorgen, dass die Elektronik im Handy, Computer, Saugroboter und auch in wesentlich komplexeren Systemen korrekt und zuverlässig funktioniert. Ich will einen Beitrag leisten den Alltag für uns alle und vielleicht sogar auch die Welt insgesamt zu verbessern.

Warum sollten sich Studierende Sie als Lehrenden wünschen?
Prof. Daniel Große: In meinen Lehrveranstaltungen verknüpfe ich Grundlagenwissen mit aktuellen Forschungen. Die Studierenden können Elektronik auch hautnah erleben. Für meine Studierenden habe ich immer eine offene Tür und ein offenes Ohr.

An welchem Projekt arbeiten Sie momentan konkret?
Prof. Daniel Große: Ich entwickle neue skalierbare Methoden zur Verifikation von Software, die auf RISC-V Prozessoren abläuft. Hierfür verwende ich sogenannte virtuelle Prototypen. So kann die Software schon ein bis zwei Jahre vor der Fertigstellung der physikalischen Hardware entwickelt und verifiziert werden.

Welche Hobbys haben Sie?
Prof. Daniel Große: Ich spiele leidenschaftlich gerne Doppelkopf. Meine Frau und meine drei Kinder spielen Doppelkopf ebenfalls sehr gerne, so dass wir immer vier Spieler zusammen bekommen.

Was wollen Sie in Ihrem Leben unbedingt noch machen oder erreichen?
Prof. Daniel Große: Ein richtig gutes Lehrbuch schreiben.

NEWS 06.10.2020

JKU: "Das LIT OIC stellt vor: LIT Secure and Correct Systems Lab", in *JKU News & Events*, 05.08.2020

Das LIT OIC stellt vor: LIT Secure and Correct Systems Lab

Startseite

ARTIKEL TEILEN

Neun Institute arbeiten im LIT Secure and Correct Systems Lab daran, dass elektronische Systeme wirklich sicher und korrekt arbeiten.

Prof. Wille, Sie leiten das Lab. Warum ist das LIT Secure and Correct Systems Lab im LIT OIC angesiedelt?

Prof. Robert Wille: Einer der wesentlichen Ideen unseres Labs ist es, die Expertise von insgesamt neun Instituten unter einem Dach zu bündeln. Entsprechend besteht auch unser Team aus WissenschaftlerInnen unterschiedlicher Disziplinen. Das OIC ermöglicht es uns, diese auch im wörtlichen Sinn „unter einem Dach" zusammen zu bringen. Würden wir alle einzeln auf die Institute verteilen, würden wir viel der von uns gewünschten interdisziplinären Synergien verlieren.

Was macht das LIT Secure and Correct Systems Lab einzigartig?

Prof. Robert Wille: Elektronische Systeme (egal ob offensichtlich wie Smartphones oder eher "unsichtbar" wie z.B. die Bremsteuerung im Auto) bestimmen mittlerweile jeden Aspekt unseres Lebens. Damit diese aber wirklich sicher und korrekt arbeiten, muss eine ganze Menge berücksichtigt werden. Eine ungenaue Spezifikation kann bereits die Basis für zukünftige Sicherheitslücken bilden. Fehler in der Hardware oder Software können zu katastrophalen Konsequenzen führen. Nach Auslieferung des Systems sind Wartung und Updates relevant. Und selbst wenn das System außer Betrieb genommen wird, sollte man Sicherheitsfragen nicht komplett ignorieren, damit z.B. alte Daten nicht in falsche Hände kommen. Diese gesamte Bandbreite von Idee, Umsetzung, Nutzung und Außerbetriebnahme von Systemen können einzelne Personen oder Institute allein gar nicht mehr abbilden. Die Einzigartigkeit unseres Labs ist es, die verschiedenen notwendigen Expertisen zusammen zu bringen.

Was ist dein aktuelles Lieblingsprojekt?

Prof. Robert Wille: Unsere Arbeiten sind zu divers, was es nahezu unmöglich macht, einen Favoriten auszuwählen. Wir entwickeln wissensbasierte Business-Modelle, machen uns Gedanken zu digitalen Identitäten, garantieren eine sichere und korrekte Software- und Hardware-Entwicklung, machen Systeme sicher vor Hackern, etc.; und dann arbeiten wir auch noch an Zukunftsthemen wie Quantencomputer und Quantenverschlüsselung. Kurz: Alle unsere Projekte sind toll! ;o)

Was bringt das LIT OIC der Forschung?

Prof. Robert Wille: Forschung lebt von Innovation und Kreativität. Das lässt sich nicht "von oben verordnen", sondern benötigt Räume für Inspiration, Austausch und Entfaltung. Das OIC mit seinen Einrichtungen aber auch Veranstaltungen und Events bietet hierfür ideale Bedingungen. Hinzu kommt die Nähe zu den Firmen im OIC, die sicherstellen, dass wir nicht zum reinen akademischen Elfenbeinturm ohne praktischen Bezug werden.

12.5. Team SIGFLAG

JKU: "JKU-Studis qualifizieren sich für internationalen "Hacker"-Wettbewerb in Russland",
in *JKU News & Events*, 09.09.2019

JKU-Studis qualifizieren sich für internationalen „Hacker"-Wettbewerb in Russland

Informatik-Studierende der JKU und der FH Hagenberg qualifizierten sich für das Finale des internationalem „Hacker"-Wettbewerbs VolgaCTF.

Teilnehmer am HackerInnen-Wettbewerb: von links nach rechts: oben: Markus Vogl, Tobias Höller; unten: Mario Kahlhofer, Thomas Pointhuber

An der „Cyberfront" findet ein unerbittlicher Wettkampf statt. Meldungen über kritische Sicherheitsvorfälle und die Angst vor Cyberangriffen auf kritische Infrastruktur reißen nicht ab. Ein Umstand, der auch immer mehr junge Informatikerinnen und Informatiker motiviert, sich intensiver mit IT-Sicherheit zu beschäftigen. Das oberösterreichische Team UpperSec, ein Zusammenschluss von

Studierenden der JKU Linz (Team SIGFLAG) sowie der FH Hagenberg (Team HgbSec), ist hierbei besonders erfolgreich.

So konnte sich UpperSec beim internationalen IT-Sicherheitswettbewerb „VolgaCTF" als bestes deutschsprachiges Team durchsetzen und einen der begehrten Plätze für das Finale im russischen Samara sichern. Damit ließen sie über 1.000 andere HackerInnen-Teams aus aller Welt hinter sich und treten nun als bestes deutschsprachiges Team gegen 18 weitere Finalisten an. Für die Nominierung mussten die Studierenden Capture The Flag (CTF) Wettbewerbe bestreiten. Diese erlauben es, erlernte Kenntnisse in spannender Weise und einer kontrollierten Umgebung auszuprobieren. Im 20-köpfigen Team wurde hier im Frühjahr beim Qualifying 48 Stunden lang nach Sicherheitslücken in verschiedenen Programmen gesucht.

Beim Finale vom 17. bis 20. September wird das Szenario noch etwas verschärft. Hier wird ein Attack-Defense CTF gespielt, bei dem jedem Team ein zu schützender virtueller Computer zugewiesen wird. Punkte werden vergeben, wenn ein Team erfolgreich eine oder mehrere Schwachstellen in den Computern der anderen Teams findet bzw. den eigenen Rechner möglichst gut vor Angriffen schützt.

Das Team SIGFLAG wird durch das LIT Secure and Correct Systems Lab (Leitung: Prof. Robert Wille) unterstützt, welches sich der Forschung zu sicheren und korrekten IT-Systemen widmet und dabei insbesondere junge Talente fördert. Als Teil des Linz Institute of Technology (LIT) bündelt es die Expertise von neun Instituten verschiedener Fachbereiche.

NEWS 09.09.2019

Ruzmarinovic, Claudia: "Diese JKU-Studenten sind bei der "Hacker-WM "dabei", in *Heute*, 12.09.2019, Seite unbekannt

Diese JKU-Studenten sind bei der „Hacker-WM" dabei

Sie konnten sich gegen mehr als 1.000 andere „Hacker"-Teams aus der ganzen Welt durchsetzen: Sieben Informatik-Studenten der JKU Linz und der FH Hagenberg – darunter Markus Vogl, Tobias Höller und Thomas Pointhuber von der JKU – nehmen als bestes deutschsprachiges Team am Finale des „Hacker"-Wettbewerbs „VolgaCTF" in Samara (Russland) teil.

von Claudia Ruzmarinovic

Unter dem Team-Namen „UpperSec" treten die Oberösterreicher am 19. September gegen 18 weitere Finalisten an. In zehn Stunden (mit Pausen) müssen die IT-Cracks Punkte sammeln.

Die Aufgabe im Finale: „Es geht darum, den eigenen Computer vor Angriffen zu schützen bzw. den der anderen Teams anzugreifen. Dafür gibt's dann Punkte", so Mario Kahlhofer, der selbst nicht dabei ist, aber von daheim aus die Daumen drückt. Das Team, das die meisten Punkte hat, gewinnt.

Am 20. April ist dann die Preisverleihung. Und was gibt's zu gewinnen? „Das ist noch geheim", so Kahlhofer.

Die vier „Hacker-Cracks" der JKU sind im Finale dabei.

Herbert Schorn: "Linzer Studenten als Computer-Hacker in Russland",
in *Oberösterreichische Nachrichten*, 17.09.2019, S. 19

Linzer Studenten als Computer-Hacker in Russland

Unter 400 Teilnehmern aus aller Welt haben sich elf Studenten von JKU und FH für einen Hacker-Bewerb in Samara qualifiziert

VON HERBERT SCHORN

LINZ. Damit hatten die elf Informatik-Studenten selbst nicht gerechnet: Unter 400 Teilnehmern aus aller Welt hat sich die Truppe, die sich aus zwei Teams der Johannes Kepler Universität (JKU) Linz und der Fachhochschule (FH) in Hagenberg formierte, für einen internationalen Hacker-Wettbewerb im russischen Samara qualifiziert. „Unser Ziel war lediglich, besser als das Team der Uni in Wien zu sein", sagt Tobias Höller, einer der Teilnehmer, mit einem Augenzwinkern. Doch die Qualifikation lief deutlich besser als erwartet: Als einzes von nur fünf nicht russischen Teams wurden die Linzer zu dem Bewerb eingeladen.

„Da ergreift einen Panik"

Computer-Hacker gelten allgemein als kriminell. Sie suchen in Computersystemen nach Sicherheitslücken und nützen die Schwachstellen aus, um an Daten zu kommen, die eigentlich geheim bleiben sollen. Doch in den Hacker-Bewerben wird genau das trainiert: die Suchen nach Fehlern in IT-Systemen. „Wir nehmen die Dinge auseinander, um zu sehen, wie sie funktionieren und wo die Schwächen sind", sagt der 28-Jährige.

Gestern hat sich die elfköpfige Studentengruppe auf die Reise nach Russland gemacht. Samara ist eine Industriestadt an der Wolga mit 1,2 Millionen Einwohnern. Am Donnerstag wird's ernst für die Oberösterreicher: Von 9 bis 24 Uhr haben sie Zeit, sich im Kampf gegen 17 andere Teams aus Russland und aller Welt zu beweisen. Doch was müssen sie eigentlich tun? Genau weiß das Höller natürlich auch nicht: „Im Grunde geht es bei diesen Wettbewerben darum, im System verwertbare Informationen zu finden." Die Teilnehmer müssen etwa unbekannte Passwörter entdecken, Systeme entschlüsseln oder die eines Programm zugrunde liegenden Quellcodes herausgeben. „Da kann es schon sein, dass man in zwei Stunden eine neue Programmiersprache lernen muss", sagt Höller.

> „Wir nehmen Systeme auseinander, um zu sehen, wie sie funktionieren und wo die Schwachstellen sind."
>
> **Tobias Höller,** Informatikstudent an der Kepler-Uni

Zusätzlich wird der Adrenalinspiegel dadurch angehoben, dass jedes Team einen zugewiesenen virtuellen Computer schützen muss. Wer bei den anderen Schwachstellen findet oder deren Attacken gut abwehrt, erhält Punkte. Auch wenn alles nur ein Spiel ist: „Die Panik, die einen ergreift, wenn man gerade angegriffen wird, ist sehr real", sagt Höller. Er schreibt gerade an seiner Diplomarbeit und arbeitet als Uni-Assistent am Institut für Netzwerke und Sicherheit.

Und auch die Vorteile, die Teilnehmer solcher Bewerbe haben, sind durchaus real. Denn bei Firmen sind Informatik-Absolventen mit Wettkampferfahrung beliebt. „Teilnehmer eines solchen Wettbewerbes zu sein, ist in der Branche ein großer Vorteil."

Hacker unter sich: Tobias Höller (blaues Shirt) mit seinen Kollegen auf der Suche nach Computer-Sicherheitslücken

„Das Gefährdungspotenzial steigt"

René Mayrhofer über Hacker-Wettbewerbe und Computersicherheit

LINZ. Der Hackerangriff mit einem Wahlkampf auf die ÖVP hat gezeigt, wie schnell Sicherheitslücken im Netz gefunden werden können. René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit an der Kepler-Uni (JKU), unterrichtet genau deswegen die Teilnehmer seiner Studenten an Hacker-Wettbewerben.

JKU-Professor René Mayrhofer (privat)

OÖN: Herr Professor, was bringen solche Hacker-Bewerbe?

Mayrhofer: Die Studenten erwerben dabei Fertigkeiten, die im Berufsleben wichtig sind. Man kann nur jene Gefahren bekämpfen oder umgehen, die man selbst verstanden hat. Manche Produkthersteller veranstalten von sich aus solche Wettbewerbe und zahlen ziemlich hohe Preisgelder. Dort werden etwa Systeme in Smartphones oder Autos gezielt angegriffen. Dabei lernen die Entwickler, wo das System verbessert werden muss.

Wie ist es um die Cyber-Sicherheit in Oberösterreich bestellt?

Das ist von Bereich zu Bereich verschieden. So wie in anderen Regionen gibt es in Oberösterreich eine ge Bausteine. Aber ich denk nicht, dass einzelne Personen si sicher sind. Die die Vernetzun stärker wird, steigt aber auch d Gefährdungspotenzial.

Was kann jeder Einzelne tun, um sein Computersystem zu schützen?

Zum einen ist wichtig, dass d Software aktuell ist. Daher ist s ratsam, alle Updates durchzufü ren. Zum anderen sollte mit de Passwörtern verantwortungsvo wurde umgegangen werden. B sondere wichtige Informationen sollten mit einer Zweifaktoren identifizierung geschützt werde Das geht zum Beispiel mit speziellen USB-Tokens, bei denen ein Anmeldung extra bestätigt wir oder mit aktuellen Smartphones

12.6. Interviews und Expertenmeinungen

Sulzbacher, Markus: "Cyberwar", in *Keplertribüne*, Ausgabe 4, 13.12.2019, S.8 f.

Cyberwar

Die Anzahl der Cyberattacken steigt – auch in Österreich. Entscheiden in Zukunft nicht mehr Kampfjets, Granaten und Drohnen über das Kriegsgeschehen, sondern Viren und Würmer?

Von Markus Sulzbacher

(c) iStock

Für den Experten liegen die Vorteile auf der Hand. Die Kriegsführung und die Spionage im digitalen Raum „kostet wenig, braucht kaum Personal, die Akteure können anonym agieren und die Maßnahmen sukzessive steigern", erklärt Oberst Walter Unger vom Cyber-Verteidigungszentrum im Abwehramt des Bundesheeres. Es sind vor allem die vergleichsweise niedrigen Kosten, die diese Art der Auseinandersetzung attraktiv machen.

„Wir sind zum Schluss gekommen, dass ein gleichzeitiger Angriff auf die gesamte kritische Infrastruktur unseres Landes – von der Strom- und Wasserversorgung über Krankenhäuser, Behörden, die Flugsicherung bis hin zum Militär – mit relativ überschaubarem finanziellem Aufwand durchaus machbar wäre", erklärt Unger. Mit einem Budget von zehn Millionen Euro könnte man Österreich digital weitgehend lahmlegen, wobei die meisten Kosten für Programmierer und IT-Experten anfallen würden, rechnet er vor. Ein hochmoderner Panzer oder ein Kampfjet ist für dieses Geld nicht zu bekommen.

Im Verteidigungsministerium in Wien geht man davon aus, dass großflächige Angriffe nur mehr eine Frage der Zeit sind. Solche Attacken könnten etwa zu einem Black-out, einem mehrtägigen Stromausfall führen, der auch verheerende Auswirkungen bis hin zu Todesfällen mit sich bringen könnte.

Dass ein derartiges Szenario nicht weit hergeholt ist, zeigte sich 2015 in der Ukraine. Eine Woche vor Weihnachten ging in einem Teil der Hauptstadt Kiew der Strom für einige Stunden aus, nachdem ein Kraftwerk Ziel einer Cyberattacke geworden war. Den Angreifern gelang es, eine ausgefeilte Schadsoftware auf Rechner eines Energieversorgers einzuschleusen und die gesamte Steuerung des Kraftwerks zu übernehmen. Der Angriff wurde von westlichen Beobachtern Russland zugeordnet und als Machtdemonstration gewertet.

Wie verwundbar die IT-Infrastruktur auch in Österreich ist, zeigte Anfang dieses Jahres der junge Wiener IT-Experte Christian Haschek auf. Er hat ganz Österreich auf Sicherheitslücken gescannt. Konkret hat er jede der rund 11,2 Millionen IP-Adressen, die dem Land zugewiesen sind, untersucht. Das Ergebnis zeigte gravierende Sicherheitsprobleme auf. Denn neben einfachen Webseiten entdeckte er auch Industriesteuerungen, Überwachungskameras und längst veraltete Server, die mit wenigen Klicks zugänglich sind. In einigen Häusern könne jedermann das Licht ein- oder ausschalten oder Musik abspielen, da deren Smart-Home- Steuerung über das Netz zugänglich war. Aber auch die Steuerung einer Kläranlage war über das Netz erreichbar. Jeder, der auf dieser Seite landete, konnte den Betrieb gehörig stören.

Angegriffen wird, „was irgendwie erreichbar ist", betont Bundesheer-Experte Unger – auch das Bundesheer. Es gebe wöchentlich drei bis fünf Attacken, „die man ernst nehmen muss", sagt Unger. Weitere hunderttausende Attacken mit der Absicht, Computer zu sabotieren oder Daten zu stehlen, werden mit herkömmlichen Methoden wie Firewalls abgewehrt.

Tatsächlich toben im Netz also viele derartige Auseinandersetzungen, die als „Cyberwar" bezeichnet werden. Was die Kriegsführung im digitalen Raum von bisherigen Formen der Auseinandersetzung zwischen Staaten unterscheidet, ist, dass hier auch zu Friedenszeiten ständig „gekämpft" wird. Und es kommen weitere Dimensionen wie Cyberspionage, Desinformationskampagnen und Einflussoperationen hinzu. Zudem ist nicht immer klar, wer hinter einem Angriff steckt oder wer das wirkliche Ziel ist. Weiters ist bei derartigen Attacken auch die Schwelle hoch, darauf militärisch zu reagieren. Wenn der Mailserver einer Partei gehackt und die E-Mails gestohlen wurden, wird man kaum mit einem massiven Raketenangriff darauf antworten.

Derzeit sieht es so aus, als könnten Cyberangriffe eine Alternative zu einem Angriff mit traditionellen Mitteln werden. Unter Experten gelten sie als Weg zur Vergeltung, ohne den Gegner frontal anzugreifen. „Man kann Schaden verursachen, ohne Menschen zu töten oder Dinge in die Luft zu sprengen", sagte etwa James Lewis vom Zentrum für Strategische und Internationale Studien in Washington. Besonders die USA unter Präsident Donald Trump setzen derzeit auf diese Strategie, wie die aktuelle Krise am Persischen Golf zeigt.

Nach dem Abschuss einer US-Aufklärungsdrohne durch den Iran im Juni dieses Jahres führten die Vereinigten Staaten Cyberangriffe gegen iranische Ziele durch. Trump hatte zuerst einen militärischen Vergeltungsangriff erwogen, diesen dann aber kurzfristig abgebrochen. Wie die Zeitung „Washington Post" berichtete, wies er stattdessen das US-Cyber-Kommando an, zur Vergeltung Cyberattacken gegen den Iran zu starten.

Einer der Angriffe galt demnach iranischen Computern, mit denen Starts von Raketen und Lenkwaffen überwacht werden. Unter Berufung auf zwei ehemalige Geheimdienstvertreter hieß es, die US-Cyberangriffe hätten zudem ein Spionagenetzwerk getroffen, das Schiffe in der Seestraße von Hormus beobachtete.

Dort waren zuvor zwei Tanker aus Norwegen und Japan angegriffen worden, wofür Washington den Iran verantwortlich machte.

Im September folgte ein Drohnenangriff auf Erdölförderanlagen in Saudi-Arabien, dessen Urheberschaft nicht restlos geklärt ist. Als Reaktion griffen die USA im Oktober Rechner im Iran an, die für die Verbreitung von „Propaganda" verantwortlich waren, wie die Nachrichtenagentur Reuters meldete.

Der Iran wird von den USA seit Jahren immer wieder digital attackiert. So führte der US-Geheimdienst NSA, im Verbund mit israelischen Verbündeten, im Jahr 2010 einen „digitalen Angriff" durch, der das iranische Atomprogramm zeitweise völlig zum Erliegen brachte. Mit Hilfe des Computerwurms „Stuxnet" konnte der Betrieb tausender Zentrifugen in einer Urananreicherungsanlage gestoppt werden. Die Urananreicherung steht im Mittelpunkt des seit Jahren währenden Streits zwischen Teheran und der internationalen Gemeinschaft über das iranische Atomprogramm. Zwischen den USA und dem Iran haben sich die Spannungen auch deutlich zugespitzt, nachdem US-Präsident Trump das internationale Atomabkommen mit dem Iran 2018 einseitig aufgekündigt hatte.

Der erste Einsatz von Cyberwaffen soll aber weit länger zurückliegen. Vorbereitungen des US-Militärs für einen „Krieg durch Informationstechnologie" wurden bereits Mitte der 1990er getroffen. Im Kosovo-Krieg kam die Technik laut damaligen Medienberichten erstmals zum praktischen Einsatz: So sollen US-Hacker die Radaranlagen der Serben gestört haben, um ungehindert Bombeneinsätze auf Belgrad fliegen zu können. Der Luftkrieg galt in Militärkreisen als Erfolg: Die NATO meldete nur zwei abgeschossene Jets.

Cyberangriffe können aber auch Angriffe mit klassischen militärischen Waffen begleiten. So wurde die israelische „Operation Orchard" im September 2007 – damals wurde eine mutmaßliche Atomanlage in Syrien aus der Luft angegriffen – nach unbestätigten Berichten von einer digitalen Manipulation des Radarsystems begleitet, sodass auf dem Bildschirm nur ein leerer und friedlicher Luftraum zu sehen war. Die Syrer wurden von dem Angriff völlig überrascht.

Digital attackiert werden allerdings nicht nur Gegner der USA. Im Jahr 2007 kam es in dem kleinen baltischen Staat Estland zu Konfrontationen zwischen ethnischen Esten und der russischen Minderheit. In der Folge verübten Unbekannte von Russland aus massive Angriffe auf estnische Webseiten von Regierungsstellen, Parteien und Banken – für das digitale Vorzeigeland Estland ein besonderer Schock.

Die Angriffe auf Websites in Estland im April 2007 waren für sich genommen vergleichsweise harmlos, hatten aber weitreichende Konsequenzen. Die Attacken führten maßgeblich dazu, dass sich die NATO verstärkt mit dem Thema Cyberwar beschäftigte und weitere Staaten für den Krieg im Netz massiv aufrüsten. Die USA, Großbritannien, die Niederlande, Israel, China, Russland, Pakistan und Indien verfügen mittlerweile über enorme Kapazitäten und gelten in Sachen elektronischer Kriegsführung als Supermächte.

Auch das österreichische Bundesheer will seine diesbezüglichen Fähigkeiten in den kommenden Jahren massiv erweitern. So sollen defensive und offensive Cyberwaffen entwickelt und beschafft und ein „Trainingszentrum für den Kampf im Cyberspace" errichtet werden. Zusätzlich soll Gerätschaft zur „Befähigung zur effektiven Störung der Waffen- und Kommunikationssysteme des Gegners" angeschafft werden.

Im September 2018 beschuldigten NATO- Staaten Russland, hinter zahlreichen Hackerangriffen der letzten Jahre zu stecken – etwa dem Diebstahl von E-Mails der

US-Demokraten, deren Inhalte von Trump während des Präsidentschaftswahlkampfes geschickt genutzt wurden und dessen Wahl zum 45. US-Präsidenten vielleicht erst möglich gemacht haben. Zusätzlich drohte die NATO unverhohlen mit Gegenschlägen in Richtung Russland. Dafür stellten Großbritannien, Dänemark und die Vereinigten Staaten dem Bündnis offensive Cyberwaffen zur Verfügung.

Diese Aufrüstung wird von Netzaktivisten kritisiert. Die beste Verteidigung liege darin, sichere Systeme zu schaffen, Datenschutz auf allen Ebenen ernst zu nehmen und rigoros gegen Datenmissbrauch vorzugehen, sagt Thomas Lohninger von der Netz-NGO epicenter.works.

Obendrein begeben sich die Staaten in eine Zwickmühle: Um Angriffswerkzeuge zu bekommen, müssen sie Schwachstellen und Verwundbarkeiten von Betriebssystemen oder Programmen im Geheimen horten. Diese Sicherheitslücken werden von Dritten, meist Firmen mit zweifelhaftem Ruf, gekauft. Deren Geschäftsmodell verbietet es, die Öffentlichkeit über Lecks zu informieren, und eben diese geheim gehaltenen Lücken könnten von Kriminellen oder staatlichen Hackern entdeckt und für Angriffe ausgenutzt werden, was in der Vergangenheit bereits passiert ist.

So stammt die Schadsoftware „Wanna Cry" ursprünglich von der NSA. Die Software nutzte eine Schwachstelle im Microsoft- Betriebssystem Windows aus, die der US-Geheimdienst entdeckt und jahrelang für eigene Spionageangriffe genutzt hatte. Die Cyberwaffe mit dem Namen „EternalBlue" geriet 2016 in die Hände einer Hackergruppe, danach schwappten Angriffswellen mit der Software durch das Netz, die weltweit Millionen Rechner trafen. Kriminelle hatten „EternalBlue" zu einem Verschlüsselungstrojaner weiterentwickelt. Dieser soll die Anwender mit manipulierten E-Mails dazu animieren, auf einen infizierten Dateianhang zu klicken und damit eine flächendeckende Verschlüsselung aller Daten auf den Computern im Netzwerk auszulösen. Für das Passwort, mit dem die Daten wieder entschlüsselt werden können, wird Lösegeld in Form von Bitcoins verlangt. Neben Privatpersonen und Banken wurden auch Krankenhäuser Opfer dieser Erpressung.

Auch Spionagesoftware für Smartphones benötigt Sicherheitslücken, um das Gerät in Echtzeit zu überwachen. Derartige Programme können unter anderem Standortdaten, Chat-Verläufe, Fotos oder Gespräche übertragen. Dass derartige Software auch von staatlichen Behörden eingesetzt wird, sieht René Mayrhofer, Institutsvorstand für Netzwerke und Sicherheit der Johannes Kepler Universität Linz, äußerst kritisch. Die Risiken sind höher als deren Nutzen, sagt der Sicherheitsexperte. Dass Sicherheitslücken bewusst verheimlicht werden, damit sie von Strafverfolgern genutzt werden können, sieht er als fahrlässig an. Das Risiko, dass derartige Schwachstellen auch von Kriminellen gefunden und ausgenutzt werden, ist hoch. Er wirft die Frage auf, ob derartige Software, die darauf baut, mit Steuergeld gekauft werden soll. Immerhin beliefern große Anbieter derartiger Programme auch Diktaturen oder Autokraten, die damit Journalisten oder Oppositionelle überwachen.

Mayrhofer hält diese Form der polizeilichen Ermittlungen nicht für besonders zukunftsträchtig. Mobile Betriebssysteme wie Googles Android werden immer mehr mit starken Schutzmechanismen ausgestattet, die Angriffe und Manipulationen von Handys enorm erschweren sollen. Mit jedem Android-Update werden Lücken geschlossen und so die Möglichkeit zu absoluter Kontrolle über ein Smartphone verhindert.

Johannes Sametinger vom JKU-Institut für Wirtschaftsinformatik streicht heraus, dass kritische Infrastrukturen künftig so entworfen und gebaut werden müssen, dass

US-Demokraten, deren Inhalte von Trump während des Präsidentschaftswahlkampfes geschickt genutzt wurden und dessen Wahl zum 45. US-Präsidenten vielleicht erst möglich gemacht haben. Zusätzlich drohte die NATO unverhohlen mit Gegenschlägen in Richtung Russland. Dafür stellten Großbritannien, Dänemark und die Vereinigten Staaten dem Bündnis offensive Cyberwaffen zur Verfügung.

Diese Aufrüstung wird von Netzaktivisten kritisiert. Die beste Verteidigung liege darin, sichere Systeme zu schaffen, Datenschutz auf allen Ebenen ernst zu nehmen und rigoros gegen Datenmissbrauch vorzugehen, sagt Thomas Lohninger von der Netz-NGO epicenter.works.

Obendrein begeben sich die Staaten in eine Zwickmühle: Um Angriffswerkzeuge zu bekommen, müssen sie Schwachstellen und Verwundbarkeiten von Betriebssystemen oder Programmen im Geheimen horten. Diese Sicherheitslücken werden von Dritten, meist Firmen mit zweifelhaftem Ruf, gekauft. Deren Geschäftsmodell verbietet es, die Öffentlichkeit über Lecks zu informieren, und eben diese geheim gehaltenen Lücken könnten von Kriminellen oder staatlichen Hackern entdeckt und für Angriffe ausgenutzt werden, was in der Vergangenheit bereits passiert ist.

So stammt die Schadsoftware „Wanna Cry" ursprünglich von der NSA. Die Software nutzte eine Schwachstelle im Microsoft- Betriebssystem Windows aus, die der US-Geheimdienst entdeckt und jahrelang für eigene Spionageangriffe genutzt hatte. Die Cyberwaffe mit dem Namen „EternalBlue" geriet 2016 in die Hände einer Hackergruppe, danach schwappten Angriffswellen mit der Software durch das Netz, die weltweit Millionen Rechner trafen. Kriminelle hatten „EternalBlue" zu einem Verschlüsselungstrojaner weiterentwickelt. Dieser soll die Anwender mit manipulierten E-Mails dazu animieren, auf einen infizierten Dateianhang zu klicken und damit eine flächendeckende Verschlüsselung aller Daten auf den Computern im Netzwerk auszulösen. Für das Passwort, mit dem die Daten wieder entschlüsselt werden können, wird Lösegeld in Form von Bitcoins verlangt. Neben Privatpersonen und Banken wurden auch Krankenhäuser Opfer dieser Erpressung.

Auch Spionagesoftware für Smartphones benötigt Sicherheitslücken, um das Gerät in Echtzeit zu überwachen. Derartige Programme können unter anderem Standortdaten, Chat-Verläufe, Fotos oder Gespräche übertragen. Dass derartige Software auch von staatlichen Behörden eingesetzt wird, sieht René Mayrhofer, Institutsvorstand für Netzwerke und Sicherheit der Johannes Kepler Universität Linz, äußerst kritisch. Die Risiken sind höher als deren Nutzen, sagt der Sicherheitsexperte. Dass Sicherheitslücken bewusst verheimlicht werden, damit sie von Strafverfolgern genutzt werden können, sieht er als fahrlässig an. Das Risiko, dass derartige Schwachstellen auch von Kriminellen gefunden und ausgenutzt werden, ist hoch. Er wirft die Frage auf, ob derartige Software, die darauf baut, mit Steuergeld gekauft werden soll. Immerhin beliefern große Anbieter derartiger Programme auch Diktaturen oder Autokraten, die damit Journalisten oder Oppositionelle überwachen.

Mayrhofer hält diese Form der polizeilichen Ermittlungen nicht für besonders zukunftsträchtig. Mobile Betriebssysteme wie Googles Android werden immer mehr mit starken Schutzmechanismen ausgestattet, die Angriffe und Manipulationen von Handys enorm erschweren sollen. Mit jedem Android-Update werden Lücken geschlossen und so die Möglichkeit zu absoluter Kontrolle über ein Smartphone verhindert.

Johannes Sametinger vom JKU-Institut für Wirtschaftsinformatik streicht heraus, dass kritische Infrastrukturen künftig so entworfen und gebaut werden müssen, dass

sie Angriffen nicht nur besser standhalten, sondern im Ernstfall auch Fallback-Strategien zur Verfügung haben. „Gut vorstellbar ist das beispielsweise anhand eines Herzschrittmachers", erklärt Sametinger. „Kein Patient, der ein solches Gerät implantiert hat, kann ruhig schlafen, wenn er jederzeit potentiell damit rechnen muss, dass Unberechtigte die Kontrolle über das Gerät übernehmen können. Wenn also Schwachstellen solcher Geräte bekannt werden oder es sogar zu Angriffen kommen sollte, dann ist es besser, auf Komfort zu verzichten und beispielsweise durch Abdrehen von Kommunikationskanälen die Sicherheit zu erhöhen, weil dadurch Angriffe verhindert werden können." Auch in Flugzeugen sollte das Netz der Passagiere physisch vom Netz der Flugzeugsteuerung getrennt sein. Eine weitere Maßnahme, um Angriffspunkte in einem möglichen Cyberwar zu entschärfen, wäre es, im Ernstfall kritische Infrastrukturen wie das Stromnetz physisch vom Internet zu trennen.

Dzugan, Franziska: "Digitaler Führerschein: "Massenüberwachung muss man ausschließen"", in *Profil. Shortlist*, 25.11.2019

Digitaler Führerschein: "Massenüberwachung muss man ausschließen"

© ÖAW/ELIA ZILBERBERG

2020 werden die ersten Staaten den digitalen Führerschein auf dem Smartphone einführen – Österreich könnte bald folgen. Es sei nur eine Frage der Zeit, bis der elektronische Ausweis auch den Pass ersetzt, sagt der Informatiker René Mayrhofer.

Von Franziska Dzugan (25. 11. 2019)

profil: Wie wird der elektronische Führerschein funktionieren?
Mayrhofer: Die internationale Norm sieht zwei Varianten vor, zwischen denen eine Behörde wählen kann. Zum einen soll es einen Führerschein geben, der direkt von der Behörde auf das Smartphone zugestellt wird. Bei einer Fahrzeugkontrolle hat die Polizei ein Endgerät, das beim Zusammenführen der beiden Geräte den Führerschein auslesen kann, ähnlich wie beim Zahlen im Supermarkt.

Dieser Artikel stammt aus profil 47/2019. *Das aktuelle Heft können Sie im Handel oder als E-Paper erwerben.*

profil: Wie sieht Variante zwei aus?
Mayrhofer: Dabei werden die Daten auf einem Server gespeichert; das Handy weiß lediglich, wo die Daten liegen. Will die Polizei sie abfragen, muss sie eine Verbindung zur Cloud herstellen.

profil: Schreit das nicht förmlich nach Datenmissbrauch?
Mayrhofer: Die Risiken sind wegen der Zentralisierung größer als bei der ersten Variante, die wir Forscher empfehlen.

profil: Wann wird der digitale Führerschein in Österreich kommen?
Mayrhofer: Das ist eine politische Entscheidung. Die Staatsdruckerei hat aber bereits erste Prototypen in Arbeit.

profil: Und wenn das Handy gestohlen wird?
Mayrhofer: Man kann den Ausweis aus der Ferne sperren lassen, wie eine verlorene Bankomatkarte. Das kann auch die Behörde beim Führerscheinentzug.

profil: Der Plan ist, auch den Pass, sämtliche Fahrscheine, die Supermarktkarte und die meisten Passwörter durch eine digitale Identität zu ersetzen. Wie sicher ist so ein digitales Ich?
Mayrhofer: Seit 2014 erforschen wir, wie wir gefährliche Verknüpfungen von digitalen Ausweisen verhindern können. Fazit: Man kann sicherstellen, dass meine digitale Supermarktkarte auf dem Handy mich nicht zuordnen kann, wenn ich mit demselben Handy im selben Supermarkt mein Alter nachweise, um Alkohol zu kaufen.

„

Wir Wissenschafter empfehlen Systeme mit möglichst wenig externen Abhängigkeiten.

“

profil: Welche Vorteile bringt das?
Mayrhofer: Bei digitalen Ausweisen kann ich auswählen, welche Daten ich herzeige. Bei der Anmeldung einer SIM-Karte wird häufig der Ausweis kopiert. Damit werden unnötige Daten gesammelt.

profil: Wie kann man verhindern, dass der Staat eine Sammelleidenschaft entwickelt wie in China, wo Sozialleistungen bereits vom Verhalten der Bürger abhängen?
Mayrhofer: Massenüberwachung muss man von vornherein ausschließen, weil niemand weiß, was künftige Regierungen im Sinn haben. Eine Möglichkeit, Cloud-Lösungen in Zukunft besser zu schützen, besteht darin, dem Bürger seine Daten selbst in die Hand zu geben. Er soll entscheiden können, ob er sie einem staatlichen Server, seiner Hausbank oder einem privaten Anbieter anvertraut – oder sie auf verschiedene Server verteilt. Auch Wechseln muss einfach möglich sein.

profil: Sie waren von 2017 bis Mitte 2019 Sicherheitschef bei Googles Betriebssystem Android. Google fällt immer wieder durch Datenlecks auf, zuletzt mit der Cloud G-Suite, die Passwörter seit 2005 unverschlüsselt speicherte. Wie erklären Sie das Menschen, die Angst um ihre Daten haben?
Mayrhofer: Ich war für die Sicherheit des Endgeräts zuständig, mit der Cloud hatte ich kaum zu tun. Aber es stimmt, dass wir vielen Anbietern großes Vertrauen entgegenbringen müssen. Wir Wissenschafter empfehlen deshalb Systeme mit möglichst wenig externen Abhängigkeiten.

profil: Quantenkryptografie gilt als abhörsicher. Kann sie unsere Daten sicherer machen?
Mayrhofer: Die Kommunikation zwischen zwei Computern wird dadurch abhörsicher. Das schützt aber die Daten auf den Endgeräten in keiner Weise. Die Quantentechnologie birgt sogar eine Gefahr, mit der sich bereits ein eigener Forschungszweig befasst: Quantencomputer werden es mit ihrer extrem hohen Rechenleistung schaffen, manche heutige Algorithmen zu knacken. Das gilt es zu verhindern.

Zur Person

René Mayrhofer leitet seit 2014 das Institut für Netzwerke und Sicherheit der Johannes Kepler Universität Linz und arbeitet in der Internationalen Organisation für Normung (ISO) am neuen Standard für digitale Ausweise mit. Vergangene Woche sprach er in der Österreichischen Akademie der Wissenschaften (ÖAW) in Wien über die Zukunft der digitalen Identität.

Prof. Robert Wille entwickelt neue Computer-Technologien an der Johannes Kepler Universität Linz.

Computer von morgen

Eine neue Technologie soll die Rechenzeit von Jahren auf wenige Sekunden verringern

Strom aus" und „Strom an" – auf diesem einfachen Konzept basierten über Jahrzehnte unsere heutigen Computertechnologien. Elektrische Schaltungen – im Notebook, Smartphone etc. – bilden die Grundlage heutiger Computer, die mittlerweile jeden Aspekt unseres Alltags erfasst haben. „Was vor 60 Jahren ganze Räume füllte, passt heute in jede Hosentasche. Diese Miniaturisierung elektrischer Schaltungen erreicht mittlerweile bereits die atomare Ebene", so Univ.-Prof. Robert Wille von der Johannes Kepler Universität Linz. Dies sei ein großes Problem, denn kleiner als einzelne Atome lassen sich Computer-Komponenten nicht bauen.

Daher sind Alternativen nötig, an denen derzeit auch eifrig gearbeitet wird. „Zum Beispiel Quantencomputer. Diese verarbeiten Informationen nicht nur mithilfe zweier möglicher Zustände, also ‚Strom aus' und ‚Strom an', sondern ermöglichen durch Ausnutzung quantenmechanischer Eigenschaften auch Berechnungen von beiden Zuständen gleichzeitig. Dieses für Nicht-Experten nicht verständliche Phänomen kann von uns Quantenphysikern trotzdem zur Konstruktion neuartiger Computer verwendet werden", erläutert Wille. Dadurch ließen sich Probleme, für die die Forscher bisher Jahre Rechenzeit benötigten, in wenigen Sekunden lösen.

Diese Technologien stehen jedoch noch am Anfang ihrer Entwicklung. Für Informatiker wie Wille ist das eine große Herausforderung: „Wir meistern das, indem wir zukünftige Computertechnologien erst einmal nur simulieren. Dafür nutzen wir mathematische Beschreibungen der physikalischen Phänomene, die zusätzlich noch mit cleveren schematischen Methoden der Berechnung, sogenannten Algorithmen, und Datenstrukturen so aufbereitet werden, dass sie auch auf bisherigen Computern einigermaßen effizient berechnet werden können." So gaukeln sich die Forscher selbst vor, an einem Quantencomputer zu arbeiten.

> *Was vor 60 Jahren noch ganze Räume füllte, passt heute in jede Hosentasche. Diese Miniaturisierung elektrischer Schaltungen erreicht mittlerweile bereits die atomare Ebene.*
>
> Prof. Robert Wille

„Natürlich ist man damit nie so effizient wie die neue Computertechnologie selbst", sagt Wille. „Aber immerhin lassen sich mit Simulationen schon neue Anwendungen für die Forschung testen und auch zukünftige Informatikerinnen und Informatiker auf diese Technologie vorbereiten." Dies sei auch dringend nötig, denn so wie sich bisherige Computer in unserem Alltag etabliert haben, würden sich auch neue Technologien durchsetzen.

ZUR PERSON

Prof. Robert Wille, geboren in Gera (D), studierte Informatik an der Universität Bremen. Nach seinem Doktorat arbeitete er unter anderem am Deutschen Forschungszentrum für Künstliche Intelligenz sowie an den Universitäten in Dresden und Potsdam, bevor er mit nur 32 Jahren als einer der jüngsten Professoren an die JKU Linz berufen wurde.

In dieser Serie stellen wir Projekte von Spitzenforscherinnen und -forschern in Österreich vor. Ausgewählt werden sie von Prof. Dr. Georg Wick vom Biozentrum der Medizinischen Universität Innsbruck.

SAMSTAG, 12. OKTOBER 2019 OÖNachrichten

MENSCHEN & MÄRKTE
VON DIETMAR MASCHER

„Das Thema Sicherheit im Netz gewinnt an der JKU an Bedeutung: kommende Woche öffnet das LIT Secure & Correct Lab"

Die Fragen für die Zeit nach dem Handy

René Mayrhofer: Nach seiner Zeit bei Google will der JKU-Professor nun gewährleisten, dass der Staat und Großkonzerne nicht über alle Daten zentral verfügen können.

Wenn es um Sicherheit im Internet geht, gilt der Linzer Universitäts-Professor **René Mayrhofer** international als einer der renommiertesten Experten. Nächste Woche übernimmt er am **LIT** (Linz Institute of Technology) gemeinsam mit seinen Kollegen **Robert Wille** und **Josef Küng** die Leitung des neuen **Secure & Correct Systems Lab**. Es soll Antworten auf die Frage finden, wie Sicherheit im Internet erhöht werden kann – auch nach der Hoch-Zeit des Smartphones. „Ziel muss sein, persönliche Daten möglichst dezentral abzulegen, um die digitale Identität zu schützen", sagt Mayrhofer im Gespräch mit den OÖNachrichten. Vor allem die vollständige Erfassung des Menschen durch den Staat oder internationale Konzerne solle dadurch vermieden werden.

Die Ära des klassischen Handys werde in etwa zehn Jahren vorbei sein. „Das Smartphone ist wie ein Schweizer Messer. Man kann damit alles ein bisschen machen. Aber wenn man in der Küche steht, will man mit einem richtigen Kochmesser arbeiten", sagt der 40-jährige Wissenschafter. Es sei davon auszugehen, dass nach der Zeit des Smartphones die Zeit der Clouds komme.

Mittels biometrischer Daten wie Iris- oder Fingerabdruckkennung werde man sich in Infrastruktur einklinken können, die praktisch überall verfügbar und eng vernetzt sein werde.

Die zentrale Überlegung dabei ist, dass möglichst viel dezentral gespeichert wird. Laufen alle Daten an einer zentralen Stelle zusammen, geht es in die Richtung von China, wo der einzelne Bürger nicht nur umfassend erfasst, sondern auch sozial bewertet wird, was sich letztlich auf die Zukunftschancen und die persönliche Sicherheit der Betroffenen unterschiedlich auswirkt. „Je dezentraler, desto schwieriger wird für den Staat oder einen Konzern, die Skalierung (also die Verhaltensweisen und Daten) einzustufen", sagt Mayrhofer.

„Geben schon zu viel preis"

Schon jetzt würden im Grunde viel zu viele Daten preisgegeben. Wer einen Führerschein herzeige und scannen lasse, nur um zu beweisen, dass er volljährig sei, verschenke seine Daten. Das lasse sich diskreter gestalten, sagt Mayrhofer. Derzeit laufen in vier Bundesstaaten Versuche, den Führerschein am Handy abzuspeichern und dabei auch die Datenfreigabe zu steuern. „Wichtig ist dabei, dass dies auch offline funktioniert", sagt Mayrhofer.

Der Wissenschafter arbeitete zwischenzeitlich bei **Google** als Direktor für Android Platform Security. Als er die Zentrale in Mountain View nach zwei Jahren wieder verließ, war seine Abteilung von zehn auf 30 Mitarbeiter gewachsen. Die JKU hat einiges in Bewegung gesetzt, um Mayrhofer wieder nach Linz zu holen. Besser vom Google ist er nach wie vor, und die Zeit in Kalifornien möchte er nicht missen. An der Universität freue man sich über bescheidene Zahlen an Publikationen und Zitierungen. Bei einem Konzern wie Google sei man plötzlich für mehr als zwei Milliarden Smartphones mitverantwortlich und sehe, wie sich Herausforderungen bei Problemen in großer Zahl potenzieren können. Entsprechend möchte Mayrhofer auch die Schnittstelle zwischen Wirtschaft und akademischer Forschung stärken.

> **Je dezentraler die persönlichen Daten gespeichert sind, desto schwieriger wird es für den Staat und Großkonzerne, diese zu skalieren."**
>
> **René Mayrhofer**, Professor an der Johannes Kepler Universität, Leiter des Instituts für Netzwerksicherheit und ab nächster Woche auch mitverantwortlich für das LIT Secure & Correct Lab an der Linzer Uni

Ein Schritt könnte ein Christian Doppler Labor sein, das beantragt ist und möglicherweise noch heuer von der Politik bewilligt wird. In Kooperation mit der **3-Banken-IT**, dem **Kepler Uni-Klinikum (KUK)**, **NXP Semiconductors** und der **Staatsdruckerei** soll in diesem CD-Labor die Software für den Datenaustausch in der neuen Infrastruktur nach dem Handy entwickelt werden.

Leben ohne Alexa

Und wie hält es der Professor, der aus Graz stammt, aber in Linz studiert hat und zunächst an der Fachhochschule Hagenberg tätig war, zu Hause mit der IT-Sicherheit? Mayrhofer räumt ein, dass er kein ähnliches Sprachsteuerungssystem wie Alexa zu Hause nutze – er habe eine eigene Variante gebaut. Auch eine allumfassende Vernetzung via Internet vermeidet der Professor. Bestimmte Dinge seien nur über spezielle sichere Netzwerke zugänglich. Und auch sonst stelle er – auch in Alltagsdingen – für manche Menschen eher ungewöhnliche Fragen. „Ich möchte ein Elektrogerät, das man auch auf Flugmodus stellen kann. Bisher konnte mir noch kein Verkäufer erklären, ob das auch funktioniert."

DAS VIRTUELLE ICH

Digitale Identitäten sind eine Voraussetzung für zahlreiche Apps & Services und gewinnen auch als elektronische Ausweise an Bedeutung. Welche Trends in diesem Bereich auf uns zukommen und warum die Sicherheit nicht auf der Strecke bleiben darf, berichtete René Mayrhofer, Informatiker und ehemaliger Android Sicherheitschef, im Rahmen einer Akademievorlesung an der ÖAW.

© Antoine Beauvillain/Unsplash

Von der E-Banking-App über Web-Shoppings bis hin zum elektronischen Führerschein: Ohne Log-Ins und eine elektronische Identifikation kommt man in der digitalisierten Welt vielfach nicht mehr weit. Der Wunsch der digitalen Identität eröffnet dabei neue Fragen über die Möglichkeiten und Grenzen des virtuellen Ichs.

René Mayrhofer vom Institut für Netzwerke und Sicherheit der Johannes Kepler Universität (JKU) Linz kennt diese sehr genau. Als ehemaliger Android Sicherheitschef war der Informatiker bei Google für die Absicherung dieses weltweit verbreiteten Smartphone-Systems zuständig. Am 11. November 2019 referierte er an der Österreichischen Akademie der Wissenschaften (ÖAW) in der Reihe der Akademievorlesungen, welche Entwicklungen und Perspektiven in diesem Bereich zu beobachten sind.

Herr Mayrhofer, was ist eine digitale Identität?

René Mayrhofer: Darunter verstehen wir heute oft ein ganzes Sammelsurium von Log-In Daten, die wir im Netz verwenden, vom E-Banking bis zu Social Media-Webseiten. Allgemeiner gesprochen sind digitale Identitäten aber Mengen von Attributen, die Eigenschaften natürlicher Personen beschreiben, wie zum Beispiel Namen, Alter, Wohnort und so weiter.

Wie weit ist die Digitalisierung der Identität schon vorangeschritten?

Mayrhofer: Derzeit werden ganz verschiedene Attribute einer Identität von Plastik- oder Papierdokumenten auf das Smartphone verschoben, sei Führerscheinen über E-Cards bis zu Reisepässen. Das erfordert, dass wir uns Gedanken darüber machen, wie solche sensiblen Informationen sicher auf unseren Geräten genutzt werden können. Wir arbeiten an der JKU etwa daran mit, einen internationalen Standard für elektronische Führerscheine zu entwickeln. Das ist aber nur der erste Schritt der Digitalisierung.

Wie geht die Entwicklung weiter?

Mayrhofer: Ich denke, dass wir in den nächsten zehn Jahren sehen werden, dass weitere Identifikationsapplikationen auf unseren Smartphones landen. Danach rechne ich damit, dass diese Systeme in die Cloud wandern werden. Vom Öffnen von Türen in Gebäuden bis zur Grenzkontrolle werden die erforderlichen persönlichen Informationen und Berechtigungen dann in Nutzerprofilen gespeichert werden, die nicht mehr auf ein spezifisches Gerät angewiesen sind.

Wie ein digitaler Schatten, der mir überall hin folgt und verschiedenste Türen öffnen kann?

Mayrhofer: Ja, dahin geht der Trend, aber das passiert nicht über Nacht. Wir wissen heute, wie wir diverse Ausweisdokumente und Nutzerkonten auf Smartphones bringen können, es wird aber trotzdem noch Jahre dauern, bis eine breite Bevölkerungsschicht von dieser Möglichkeit Gebrauch macht.

Was sind die Vorteile einer Cloud-Lösung?

Mayrhofer: Das wäre vor allem bequem. Der Fingerabdruck oder ander biometrische Merkmale könnten dann sämtliche Ausweise und Log-Ins ersetzen. Die Sicherheit wird auch erhöht, weil Identitäten nicht mehr durch den Diebstahl eines Smartphones kompromittiert werden können.

Wie sieht es mit den Schattenseiten aus?

Mayrhofer: Wenn wir eine zentrale Datenbank mit allen nötigen Informationen haben, ist das natürlich ein Problem für den Datenschutz und die Privatsphäre. In Indien und China kann man derzeit sehen, dass der Aufbau solcher Datensammlungen demokratiepolitisch bedenklich ist. Wir sehen als Wissenschaftler, wohin die Reise geht, aber wir kennen auch die Risiken. Systeme wie sie in Indien und China entstehen, sind nicht kompatibel mit europäischen Werten.

Das heißt, es geht nicht nur um technische Fragen, sondern auch darum, wie viel Macht wir unseren politischen Verantwortlichen geben wollen.

Wirtschaft Oberösterreich

BUSINESS AKTUELL

Doppelspitze
Elke Gornik und Stefan Sunzenauer leiten nun das „Center of Lifelong Learning" an der FH OÖ.

Neue Marke
Die Hotelgruppe Mayer gründete die Marke Familux-Resorts, zu der auch das Hotel Dachsteinkönig in Gosau gehört.

Robert Wille (r.) rührt die Werbetrommel fürs Informatik-Studium. Die Begeisterung versucht er auch damit zu wecken, komplexe Themen im Biomedical-Science-Journal kindergerecht aufzubereiten.

Fotos: Markus Wenzel

Bedarf an IT-Spezialisten groß **JKU-Professor über Wunsch der Studenten:**

„Die meisten wollen hacken"

Sein Smartphone liegt vor ihm, dazu eine Broschüre über das Angebot am Linz Institute of Technology. „Ich bin für mein Leben gern Professor", sagt Robert Wille. Der Informatiker leitet das neue Labor für Secure und Correct-Systems an der Kepler-Universität. „Ich schaue mir gerne Ideen an, die nicht so Schema F sind", sagt er.

Sonntagabend steigt er in Bremen in den Zug, um Montagfrüh in Linz zu sein. Donnerstagabend tritt er die gleiche Route wieder an, diesmal umgekehrt. „Freitag arbeite ich von zu Hause", sagt Robert Wille, der an der Kepler-Uni das Institut für integrierte Schaltungen und das Labor für Secure und Correct-Systems leitet, aber auch am Deutschen Forschungszentrum für Künstliche Intelligenz in Bremen als Berater tätig ist.

Wille, leidenschaftlicher Querdenker, rührt die Werbetrommel für die Technik – vor allem für die Informatik. Das Interesse an einem Studium in diese Richtung ist zwar gestiegen, doch der Bedarf an IT-Spezialisten ist riesig: „Wir sind am Vorabend eines neuen, technologischen Zeitalters. Als Informatiker muss man sich existenziell keine Sorgen machen." Wille verbringt viel Zeit im Open-Innovation-Center in Linz, hält aber auch Vorlesungen zum Thema Hardware-Entwurf. „Ich will den Studierenden vermitteln, wie cool es ist, Hardware zu entwickeln, den Zauber übertragen", so Wille, dem bewusst ist: „Die meisten wollen hacken."

Um die Leidenschaft für die Informatik anzukurbeln, veröffentlicht der 37-Jährige mit Uni-Kollegen kindergerecht aufbereitete Texte im Biomedical-Science-Journal, das an Schulen verteilt werden soll: „Wir haben keine Fußball spielenden Roboter, müssen daher einfach andere Wege gehen, um zu begeistern." B. Kneidinger

Leider gibt es viel Technologiefeindlichkeit. Dabei umgibt uns Informatik überall. Wir sind so abhängig davon.

Robert Wille, IT-Professor an der JKU

Privat oder bequem?

Von Klaus Buttinger 02. November 2019 00:04 Uhr

René Mayrhofer
Bild: JKU/König

Der Umgang mit unserer Privatsphäre verändert sich – je nach Technologie und Zeitgeist.

LESEDAUER ETWA 2 MIN

Er leitet mit Robert Wille und Josef Küng das Secure & Correct Systems Lab am LIT (Linz Institute of Technology): René Mayrhofer (40). Ihm geht es um die Sicherheit im Netz, um den Schutz der digitalen Identität.

OÖN: Wenn wir die Grenzen unserer Privatsphäre mit den Mauern unseres Heims definieren, stellt sich die Frage: Wie löchrig sind die schon?

Mayrhofer: Wenn wir Privatsphäre so sehen, wie wir sie als Kind gelernt haben – Zimmertür zu und darin tut man, was man will –, dann darf man sich heute schon fragen, ob da nicht Löcher entstanden sind.

Welche Technik bohrte die?
Sehr viele, die alle mit Bequemlichkeit zu tun haben. Das fängt an mit Websurfen. Wenn man Dienste verwendet, wie z. B. Snap Chat, um Fotos hin- und herzuschicken, muss man sich darauf verlassen, dass auf der anderen Seite auch die Tür zu bleibt und dass nichts

weitergezeigt wird. Wenn man miteinander redet, sehe ich genau, was mein Gegenüber tut. Diese Reziprozität bricht weg, wann man remote kommuniziert.

Sprachassistenten stehen auf dem Wohnzimmertisch, warten im Handy und rapportieren das Gehörte an ihre Hersteller ...

Dass sämtliche Sprachschnipsel, inklusive dem, was im Hintergrund zu hören ist, erfasst und übermittelt werden, damit die Systeme lernen können, ist zwar in den Geschäftsbedingungen beschrieben, aber ob das den Benutzern soweit bewusst ist, ist nicht sicher.

Der smarte Kühlschrank bestellt automatisch Milch beim Supermarkt. Bezahlen wir unsere Bequemlichkeit mit Daten?

Der smarte Kühlschrank wird zwar seit Jahrzehnten als Technologie ausgerufen, hat aber unser Leben noch nicht verbessert ...

... Aber Amazon weiß wahrscheinlich mehr über das Private vieler Menschen als deren Verwandtschaft. Ist das den Menschen bewusst?

Ich vermute nicht, dass die gesamten Implikationen bewusst sind. Denn da geht es um Datenanalysen und Statistiken. Dass sich aus Büchern eine gewisse politische Einstellung ableiten lässt, werden die meisten Erwachsenen wissen. Dass man aus der Zusammensetzung verschiedenster Produkte, die man kauft, vielleicht noch ganz andere Charakteristika einer Person ableiten kann, wenn man große Datenbasen hat, ist vermutlich nur mehr den Datenanalysten bewusst.

Was wäre ein No-Go, damit auch das moderne Haus weiter eine Burg bleibt, oder wie die Briten sagen: "My home is my castle"?

Was ein No-Go ist im Zwiespalt von Sicherheit, Privatsphäre und Bequemlichkeit muss jeder für sich entscheiden. Auf der Ebene der Produkte geht es eher in Richtung Bequemlichkeit, zu leichterer Erreichbarkeit von Services, und dafür nimmt man bewusst oder weniger bewusst Abstriche in der Privatsphäre in Kauf. Dass sich Kameras in Schlafräumlichkeiten befinden, wäre wahrscheinlich vor 20 Jahren undenkbar gewesen. Jetzt, da man dadurch vielleicht eine individualisierte Stilberatung fürs morgendliche Anziehen bekommt, ist das für manche kein No-Go mehr. Wenn man an den Social Score (Sozialkredit-System, Anm.) in China denkt, wäre das für unser europäisches demokratiepolitisches Verständnis ein No-Go. Dort wird das aber schon gelebt.

Die menschliche Identität in der virtuellen Welt

Ein digitaler Identitätsausweis für Führerscheinkontrollen und Grenzübertritte könnte bald Alltag sein. Wie sich ein „virtuelles Ich" sicher umsetzen lässt und zukünftige digitale Identitäten erörtert der ehemalige Google-Manager René Mayrhofer am heutigen 12. November an der Akademie der Wissenschaften.

© Bildbericht.com

(red/czaak) Im analogen Leben bestätigt etwa ein Personalausweis die jeweilige Identität. Im Internet braucht es eine große Menge an IDs und Passwörtern, um sich auf den diversen elektronischen Medien und Geräten einzuloggen. In naher Zukunft könnten diese Identitäten und Authentifizierungen einheitlich funktionieren.

Über Smartphone oder sogenannte Clouds ist die Ausweisung mit „nur" einer einzigen digitalen Identität möglich, in virtuellen wie in physischen „Welten". Als Ersatz für sämtliche Ausweise und Log-Ins soll es damit darin etwa möglich sein, Staatsgrenzen zu überschreiten, das erforderliche Alter beim Kinobesuch nachzuweisen, Eingänge zu öffnen oder auch seine Stimme bei einer politischen Wahl abzugeben.

Demokratiepolitische Risiken

Das Internet bringt für den Umgang mit der eigenen Identität aber auch Risiken. René Mayrhofer, Professor für Netzwerke und Sicherheit an der Johannes Kepler Universität Linz, wird bei seinem Vortrag „Aktuelle Entwicklungen zu digitalen Identitäten" im Rahmen seiner Vorlesungen am 12. November 2019 an der Österreichischen Akademie der Wissenschaften über die Möglichkeiten und Grenzen des digitalen Ichs sprechen.

„Wenn wir eine zentrale Datenbank mit allen nötigen Informationen haben, ist das natürlich ein Problem für den Datenschutz und die Privatsphäre. In Indien und China kann man derzeit sehen, dass der Aufbau solcher Datensammlungen demokratiepolitisch bedenklich ist. Wir sehen als Wissenschaftler, wohin die Reise geht, aber wir kennen auch die Risiken", sagt Mayrhofer.

Globaler Android-Sicherheitschef

René Mayrhofer leitet seit 2014 das angeführte Uni-Institut in Linz. Als ehemaliger Android-Sicherheitschef war der Informatiker bei Google für die Absicherung dieses globalen Smartphone-Systems zuständig. Sein aktuelles Forschungsgebiet betrifft die Bereiche Sicherheit und Privatsphäre an der Schnittstelle zu Netzwerkkommunikation, mobilen Systemen und maschinellem Lernen. Ein zentraler Fokus betrifft dabei das Thema digitale Identitäten.

René Mayrhofer: „Aktuelle Entwicklungen zu digitalen Identitäten" am Dienstag, den 12.11.2019 um 18.00 Uhr im Festsaal der Österreichischen Akademie der Wissenschaften am Dr. Ignaz-Seipel-Platz 2 in 1010 Wien.

Support eingestellt

Darum wird Windows 7 zum Sicherheitsrisiko

Wer noch Windows 7 nutzt, sollte sich nach einer Alternative umsehen. Foto: PC Dron/Fotolia hochgeladen von Christian Diabl

Am 14. Jänner hat Microsoft den Support für Windows 7 eingestellt. Wer das veraltete Betriebssystem noch immer nutzt, sollte daher rasch auf Windows 10 upgraden, rät JKU-Datensicherheitsexperte René Mayrhofer.

LINZ. Wer auf seinem PC immer noch das veraltete Windows 7 verwendet, könnte schon bald Probleme bekommen. Der Grund: Wie bei allen großen Betriebssystemen wurden bis vor kurzem auch bei Windows 7 laufend Sicherheitslücken entdeckt und durch kostenlose System-Updates geschlossen. Doch damit ist es nun vorbei. Wie schon länger angekündigt, hat Microsoft nämlich den Support für Windows 7 am 14. Jänner eingestellt. Und Sicherheitslücken gibt es mehr als man glaubt.

Offene Türen für Cyberkriminelle

Fast jede Woche werden solche Lücken gefunden und geschlossen, erklärt der Datensicherheits-Experte René Mayrhofer von der Johannes Kepler Universität gegenüber der StadtRundschau. Bleiben diese Updates aus, riskiert der Nutzer Opfer von Schadsoftware und ähnlichem zu werden. Im Extremfall können Cyberkriminelle in das System eindringen, um beispielsweise Daten zu stehlen oder gar die Kontrolle über den Computer zu übernehmen.

Ein Drittel nutzt noch Windows 7

Wie viele Nutzer davon betroffen sein könnten, zeigt ein Blick nach Deutschland. Laut der Münchner "Abendzeitung" hat das Sicherheitsunternehmens ESET berechnet, dass rund ein Drittel aller PC-Anwender noch Windows 7 nutzen. Grund zur Panik besteht für Mayrhofer trotzdem nicht. "Nur weil der Support ausgelaufen ist, bedeutet das nicht, dass Windows 7 von einem Tag auf den anderen unsicherer ist", so Mayrhofer. Allerdings werde das System mit der Zeit immer unsicherer. Der Experte empfiehlt deshalb eher früher als später auf Windows 10 upzugraden. Im Moment könne man das als Inhaber einer gültigen Windows 7-Lizenz noch kostenlos tun.

Buttinger, Klaus: "Wie sicher ist mein Handy?", in *Oberösterreichische Nachrichten*, 08.02.2020

OÖNachrichten

LINZ 2°

OBERÖSTERREICH POLITIK WIRTSCHAFT PANORAMA SPORT MEINUNG KULTUR MEINE WELT THEMENSPECIALS AKTIONEN

WEB

Wie sicher ist mein Handy?

Von Klaus Buttinger, 08. Februar 2020 00:04 Uhr

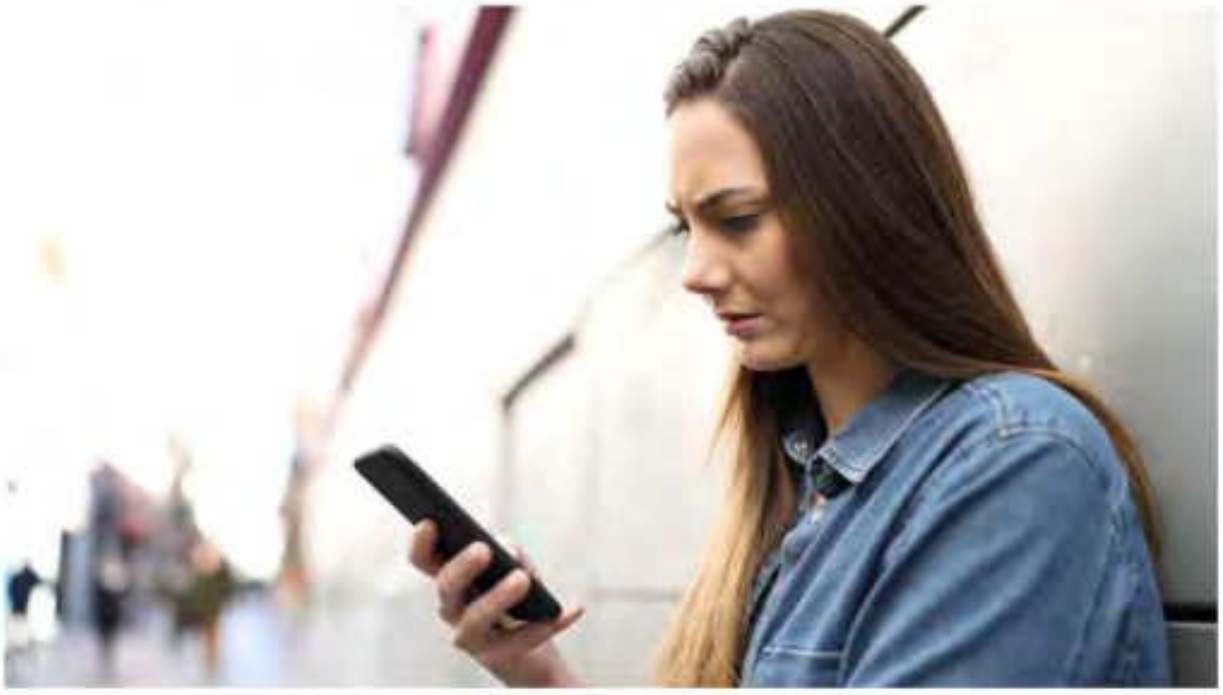


Bild: colourbox.de

Wenn seltsame Seiten nach Bankdaten fragen oder das Handy vor Werbung übergeht, hat man sich wohl einen Virus eingefangen.

Smartphones können immer mehr, folglich werden die Angriffe von Cyberkriminellen intensiver. Ein Gespräch mit Univ.-Prof. Rene Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit an der Johannes Kepler Universität, über die Sicherheit von mobilen Endgeräten.

Holz-Pellets: Sehr Gut! Heizöl: Nicht Genügend!

OÖNachrichten: Wie sicher ist ein Smartphone?

Mayrhofer: Ein Smartphone mit aktuellem Software- und Patchstand lässt sich als sehr sicher bezeichnen. Sogar sicherer als aktuelle Desktop- oder Laptopsysteme.

Wenn man liest, dass selbst das Handy von einem der reichsten Menschen der Welt, nämlich Amazon-Gründer Jeff Bezos, gehackt wurde, wie kann man da so sicher sein? Oder war das eine andere Liga des Ausspionierens?

Ich würde sagen Letzteres. Eine perfekte Sicherheit gibt es bei keinem System, ob mobil oder daheim. Bei entsprechendem Aufwand und entsprechender Motivation dahinter wird man fast jedes System, vor allem, wenn es am Netz hängt, angreifen können. Beim Angriff auf Bezos' Handy war höchstwahrscheinlich ein sogenannter Zero Day Exploit im Einsatz (eine Schwachstelle wird ausgenutzt, bevor sie der Softwarehersteller bemerken und schließen kann, Anm.). Solche Exploits gibt es immer wieder, aber sie sind sehr teuer. Man kann sie nur einmal verwenden, dann wird die Lücke geschlossen. Das zahlt sich vielleicht beim Handy von Bezos aus, unsere Handys wird das nicht betreffen.

Was tun gegen Malware auf dem Handy?

Da gibt es nur zwei Möglichkeiten. Der größte Anteil von Malware ist Adware, die Spam-Pop-ups erzeugt, oder Malware, die Daten aus dem Handy ausliest und an Dritte schickt. Dann muss man die App, die das im Hintergrund macht, finden und deinstallieren. Dann ist der Spuk vorbei. Denn die Sicherheitsmaßnahmen sind so designt, dass sich Apps nur in ihren eigenen Sandboxen (abgeschottete Bereiche, Anm.) bewegen dürfen. Um dort herauszukommen, muss eine App eine Berechtigung bekommen, z. B. das Adressbuch zu lesen oder eine SMS zu verschicken.

Die zweite Möglichkeit?

Es gibt Malware, die versucht, diese schützenden Sandbox-Mechanismen auszuschalten. Indem sie ein Rooting oder Jailbreak durchführt, dadurch Rechte bekommt und sich tiefer im System verankert. Es gibt Medienberichte von Malware, die selbst nach einem Factory-Reset (Zurücksetzen auf die Werkseinstellungen, Anm.) immer noch da ist. Ich kann mir theoretisch vorstellen, wie das geht, habe aber noch keines dieser Programme gesehen.

Es wird geraten, ausschließlich Apps aus den offiziellen Kanälen der Handyhersteller herunterzuladen. Trotzdem kann man sich beim Download aus dem Google Play Store etwas holen?

Ich habe gerade den Android-Transparency-Report vor mir. Hier wird die Wahrscheinlichkeit, sich eine App herunterzuladen, die ein unerwünschtes Verhalten zeigt, mit 0,094 Prozent angegeben. Das heißt: Es gibt etwas, das bei den App-Scans durchrutscht, obwohl die immer besser werden. Wollte man diese Rate verbessern, müsste man manuell jede Zeile des Quellcodes lesen. Selbst dann könnte noch jemand irgendetwas verstecken. Das tut weder Apple noch Google. Das Risiko, sich infizierte Apps aus anderen Quellen einzufangen, liegt achtmal höher.

Hier passiert also ein permanentes Aufrüsten der Cyberkriminellen und der App-Stores?

Richtig. Die Autoren von Malware werden wieder neue Sachen probieren, die dann wieder erkannt werden. Man bekämpft das durch die Kombination von Scans in den Stores mit zusätzlichen Sicherheitsvorkehrungen in den neuen Versionen der Betriebssysteme.

Definitionen

Malware: Kofferwort aus eng. malicious (dt. bösartig) und Software. Computerprogramme, die unerwünschte und gegebenenfalls schädliche Funktionen ausführen.

Adware: Kofferwort aus engl. advertisement (dt. Reklame, Werbung) und Software. Bringt unverlangte Werbung aufs Smartphone.

Randomware: verschlüsselt Dateien und erpresst Geld.

Banking-Trojaner: spioniert Bankzugangsdaten aus

KEPLER TRIBUNE
Wissen in Gesellschaft

Die Angst vorm Abhören

Wissen

ARTIKEL TEILEN

Der chinesische Konzern Huawei will in Europa das schnelle 5G-Mobilnetz aufbauen. Doch nicht alle fühlen sich damit besonders wohl. Vielleicht sogar aus gutem Grund.

VON CLAUDIA ZETTEL

Ein Gespenst geht um in der Mobilfunkwelt: Es trägt den Namen Huawei. Im Zuge des Auf- und Ausbaus der 5G-Netze ist auch eine Diskussion darüber entbrannt, wie sehr man dem chinesischen Konzern vertrauen kann. Huawei ist einer der weltweit führenden Anbieter für die benötigte Netzwerkinfrastruktur. Doch insbesondere die USA werfen dem Konzern eine große Nähe zur chinesischen Regierung vor und fürchten Spionageaktivitäten und Sabotage. Infolge sind auch in der EU Zweifel aufgekommen, ob man ausgerechnet auf Huawei setzen sollte, wenn es um die nächste Mobilfunkgeneration geht. Doch endgültige und klar ausformulierte Standpunkte gibt es bislang nicht.

Im Herbst vergangenen Jahres warnte die EU-Kommission vor Gefahren durch 5G-Anbieter außerhalb der Europäischen Union. Unternehmen könnten versuchen, durch den Diebstahl geistigen Eigentums Wettbewerbsvorteile zu erlangen, hieß es in einem Bericht, den die Brüsseler Behörde im Oktober vorstellte. Die Gefahr könne von Staaten sowie von staatlich unterstützten Akteuren ausgehen, so die Sorge. Vor allem Letztere könnten die „Motivation, Absicht und Fähigkeit haben, anhaltende und ausgefeilte Angriffe" auf 5G-Netze durchzuführen, las man in dem Bericht. Die Motivation solcher Angriffe sei hauptsächlich politisch. Die EU-Kommission nannte den chinesischen Anbieter Huawei in diesem Zusammenhang zwar nicht namentlich, spielte aber durchaus indirekt auf ihn an.

An einer anderen Stelle des Berichts hieß es weiter: Huawei, Ericsson, und Nokia seien im Hinblick auf den Marktanteil die Hauptakteure im 5GBereich, weitere seien ZTE, Samsung und Cisco. Ericsson und Nokia hätten ihre Hauptquartiere in der EU, die anderen jedoch nicht. „Ihre Unternehmensführung weist erhebliche Unterschiede auf, etwa mit Blick auf das Level an Transparenz und die Eigentumsverhältnisse der Unternehmen." Auch der EU-Rat warnte indirekt vor Huawei. So wurde im November vergangenen Jahres ein Beschluss vorgelegt, der bestimmte Regelungen für den 5G-Ausbau vorschlägt. Darin wird vor den „rechtlichen und politischen" Rahmenbedingungen für Anbieter aus Drittstaaten gewarnt. Es müsse in besonderem Maße auf die Risikoprofile einzelner Anbieter geachtet werden. Befürchtet wird seitens EU-Vertreterinnen und -Vertretern außerdem, dass man sich von einzelnen Anbietern abhängig machen könnte.

Die Politik hält sich zurück – aus gutem Grund

Auf politischer Ebene ging auch zu Beginn des neuen Jahres der Seiltanz um die Positionierung zu Huawei weiter. Deutschland beispielsweise hat sich bisher ebenso wenig festgelegt, ob es Huawei vom Netzausbau ausschließen wird oder nicht, wie Österreich. Einerseits teilt man die weit verbreiteten Bedenken bezüglich der Vertrauenswürdigkeit des chinesischen Konzerns, andererseits weiß man auch um die möglichen Folgen, käme es tatsächlich so weit. So hat China bereits angedeutet, dass es Konsequenzen für Deutschland haben werde, sollte Huawei vom deutschen Markt ausgeschlossen werden. Die Drohgebärde kam zum Beispiel seitens der chinesischen Botschaft in Berlin und ging dabei in Richtung der deutschen Autoindustrie in China.

Zuletzt zögerte auch die deutsche Bundeskanzlerin Angela Merkel eine klare Aussage erneut hinaus. Vor März 2020 ist nun jedenfalls keine Entscheidung in der Huawei-Frage zu erwarten. Auch die österreichische Landwirtschaftsministerin Elisabeth Köstinger, zu deren Agenden nun auch 5G und Breitband gewandert sind, legte sich bislang nicht fest. Der Status quo lautet: Man werde sich alles ganz genau anschauen. Österreichs Bundeskanzler Sebastian Kurz betonte unlängst, dass man technologieneutral agieren und gleichzeitig ein Maximum an Sicherheit haben wolle. Bei der Frage, ob man Huawei akzeptieren oder ausschließen soll, hofft Kurz auf eine einheitliche europäische Vorgehensweise.

Dass man sich seitens der Politik nur schrittweise an eine Entscheidung herantastet, ist aus Sicht von Expertinnen und Experten nicht ganz unbegründet. „Nach der derzeitigen Rechtslage steht es einzelnen Mitgliedstaaten der EU bzw. der EU als solcher frei, Unternehmen aus Drittstaaten von öffentlichen Auftragsvergaben auszuschließen", sagt Franz Leidenmühler, Institutsvorstand am Institut für Europarecht an der Johannes Kepler Universität Linz. Die Regelungen für das Auftragswesen würden nur innerhalb der EU gelten, in der Praxis würden oft auch Aufträge nur für EU-Unternehmen ausgeschrieben. „Aus rechts- und vor allem wirtschaftspolitischer Sicht ist aber natürlich bei dem deklarierten Ausschluss eines Unternehmens aus einem Drittstaat mit entsprechenden Gegenmaßnahmen des Herkunftsstaates dieses Unternehmens zu rechnen", sagt Leidenmühler. „Etwa, dass China als sogenannte Retorsion auch EU-Unternehmen von Auftragsvergaben ausschließt." Die Einschätzung des Experten bestätigt also genau das, was die chinesische Botschaft in Berlin bereits angedeutet hat.

Huawei auf Angriffe vorbereitet

Eine eindeutige Positionierung in der Huawei-Frage fällt deswegen schwer, weil bislang zwar starke Vermutungen bezüglich möglicher Abhöraktionen im Raum stehen, eindeutige Belege dafür jedoch fehlen. Huawei seinerseits bestreitet naturgemäß sämtliche Vorwürfe, geht aber gleichzeitig davon aus, dass sich der Streit, befeuert durch weitere Eskalationen mit US-Präsident Donald Trump, auch 2020 fortsetzen wird.

Auf dem Weltwirtschaftsforum in Davos ließ Huawei-Chef Ren Zhengfei verlauten, dass man sich mittlerweile besser auf die „Angriffe" vorbereitet sehe. Einerseits spielte Ren Zhengfei wirtschaftliche Auswirkungen herunter, gleichzeitig sagte er, man habe im vergangenen Jahr einiges an Erfahrungen gesammelt, nun ein stärkeres Team zusammengestellt und sei optimistisch, dass man im Konzern auch mit weiteren Vorwurfswellen gut zurechtkommen werde.

Die US-Regierung hatte US-Firmen die Zusammenarbeit mit Huawei im vergangenen Jahr tatsächlich verboten. Die Behörden begründeten den Schritt mit der „nationalen Sicher- heit". Weiters übt man seitens der USA auch Druck auf Staaten in der EU aus.

Wie die Spionage funktionieren könnte

Aber wie würde das Szenario eigentlich aussehen, sollten die Befürchtungen zutreff en und Huawei tatsächlich einen Lauschangriff auf andere Nationen starten? Rene Mayrhofer und Andreas Springer, beide ebenfalls Professoren an der Johannes Kepler Universität Linz, erläutern die technischen Vorgänge: „Die Daten kommen über die Basisstationen (Funkmasten) vom Mobiltelefon bzw. zum Mobiltelefon. In der Basisstation, oder auch in anderen Knoten im Netzwerk, könnte dann – unbemerkt von der Benutzerin oder dem Benutzer – mitgehört werden", sagt Andreas Springer. Damit könne nicht nur spioniert werden, wer welche Daten überträgt, sondern auch, wer sich wann wo aufh ält und wer wie lange mit wem kommuniziert bzw. auf welche Daten oder Dienste zugreift. „Allerdings ist anzumerken, dass so eine extrem große Datenmenge zu verarbeiten und auch zum sogenannten „Spion" weiter zu übertragen wäre, was technisch eine große Herausforderung darstellt", so Springer. „Aber auch aufgrund der notwendigen Datenübertragung, etwa zu einem Rechenzentrum des „Spions", wäre das nicht so einfach zu verschleiern.

Man müsse außerdem unterscheiden zwischen Geräten im sogenannten Backend, also in der Infrastruktur für Netzbetreiber (wie zum Beispiel im Mobilfunknetzwerk) und Endgeräten wie Smartphones. „Die möglichen Szenarien sind sehr unterschiedlich", ergänzt Rene Mayrhofer, der an der JKU das Institut für Netzwerke und Sicherheit leitet.

Bei Backend-Geräten könnten Datenströme, die über diese Geräte laufen, abgehört oder manipuliert werden, so Mayrhofer. „Dazu müssten solche Geräte aber direkten Kontakt mit Servern der möglicherweise abhörenden Organisationen haben oder diese Organisationen den Datentransfer generell abgreifen können." Ein Abhören könne dann entweder durch Fehler in der Software – die dem Hersteller nicht bekannt sind, aber von Angreifern gefunden wurden – ermöglicht werden. „Oder durch bewusst eingebaute Hintertüren. Jedes komplexe System hat Fehler, und ich halte die Gefahr schlechter Produkte für deutlich größer als die, dass Hintertüren bewusst eingebaut werden", sagt der Experte.

„Netzbetreiber sollten ohnehin Netzwerkarchitekturen pfl egen, die sich nicht auf die vollständige Sicherheit einzelner Komponenten verlassen", meint Mayrhofer. Das bedeutet laut dem Experten konkret, dass sich Backend-Geräte nicht unkontrolliert direkt mit Servern anderer Organisationen verbinden dürfen, sondern nur durch entsprechend kontrollierte Kanäle. „Kommunikation über Hintertüren sollte damit zumindest nach gewisser Zeit auff allen", so Mayrhofer.

Wenn Hersteller zu viele unbeabsichtigte Fehler in den eigenen Produkten haben, die nicht zeitnah durch Updates geschlossen werden, seien jedenfalls alle Kundinnen und Kunden dieser Produkte betroff en und möglichen Angriff en ausgesetzt, erklärt der Experte. Das treff e auf beides – Backend und Endgeräte – zu. „Die Frage nach dem Ablauf möglicher Spionageaktivitäten ist daher eine der Produktqualität: Gute Produkte und gute Netzwerkarchitekturen erschweren es, schlechte Produkte bieten viel Potenzial", sagt Mayrhofer. „Sichere Hintertüren, die nur der Hersteller oder ein Land nützen kann, andere aber nicht fi nden werden, sind mir keine bekannt", betont der Experte. „Wenn jemand in der Lage ist, solch perfekte Hintertüren zu bauen, sollte auch der Rest des komplexen Systems komplett fehlerfrei sein – und das habe ich in Jahrzehnten noch nicht in der Praxis gesehen."

Eine Frage des Preises

Noch ist schwer abzuschätzen, ob man sich in den EU-Ländern darauf einlassen wird, Huawei den Netzausbau zu überlassen, oder sich doch lieber auf europäische Alternativen wie Ericsson oder Nokia festlegt. Das grundlegende Problem beim 5G-Aufbau ist wohl auch, dass es nicht besonders viele Anbieter gibt, schon gar nicht, die bei der Technologie mit Huawei mithalten können. Das chinesische Unternehmen besticht vor allem auch mit seinen Preisen, die – wie man in der Branche vernimmt – gegenüber der Konkurrenz wohl niedrig sind.

„Ich nehme an, dass man Komponenten von Huawei sehr wohl einsetzen wird", so die Einschätzung Mayrhofers. „Allerdings sollten alle Produkte solcher Komplexität immer überwacht werden, und man sollte sich nicht auf ein einzelnes Gerät für die Sicherheit des gesamten Systems verlassen." Vielleicht könne es künftig auch sinnvoll sein, Backend-Geräte von Huawei im eigenen Netzwerk besonders isoliert zu betreiben, um Erfahrungen mit dem Betrieb und Verhalten zu sammeln, so der Experte. „Vertrauen wird immer nur langsam aufgebaut und kann bei erkanntem Fehlverhalten auch schnell verloren sein. Wenn man vorsichtig vorgeht, sollte kein Grund zu Panik-Entscheidungen bestehen."

Was bringt 5G?

5G ist die nächste bzw. 5. Mobilfunkgeneration, die die aktuell im Einsatz befi ndliche LTETechnik ablösen soll. Versprochen werden mehr Bandbreite und kürzere Latenzzeiten – also weniger Verzögerung zwischen Sender und Empfänger. LTE (oder auch 4G) schaff t derzeit eine Datenrate von maximal 300 Megabit pro Sekunde und eine Latenzzeit von unter zehn Millisekunden. 5G jedoch soll es künftig auf eine Datenrate von bis zu 20 Gigabit pro Sekunde und weniger als eine Millisekunde Latenzzeit bringen.

Die Einsatzszenarien sind vielfältig, und 5G fällt als Begriff oft in Zusammenhang mit einem anderen Schlagwort: Internet der Dinge. Egal, ob man von vernetztem oder autonomem Fahren spricht, von Sensoren generell, die in Echtzeit miteinander kommunizieren, von Multiplayer Games am Handy, Filmen in 4K-Auflösung oder Drohnen, die via Mobilfunk gesteuert werden – 5G ist derzeit in aller Munde.

Laut Schätzungen des Informationsdienstleisters IHS soll es bis zum Jahr 2030 30 Milliarden vernetzte Dinge Ganz besonders interessant könnte es auch für Unternehmen werden, gleich ganze Teile des Mobilfunknetzes sichere, interne Kommunikation zu reservieren. Auch für die Industrie, wenn es etwa um ferngesteuerte Rob wird 5G ein Thema sein. Generell wird das neue, schnellere Netz zunächst einmal vor allem im Businessbereic Rolle spielen. Denn beim Privatgebrauch von WhatsApp, Smartphone Games und Social Media wird man erst keine grofsen Unterschiede bemerken.

Für Debatten sorgt 5G auch immer wieder in Sachen Gesundheit. Viele fürchten sich vor schädlichen Strahlen gibt es jedoch keine konkreten Hinweise darauf, dass 5G oder Mobilfunktechnologien generell krebserregende haben könnten. Hinzu kommt, dass die Strahlengrenzwerte für den 5G-Standard gemeinsam mit der Weltgesundheitsorganisation (WHO) und weiteren Expertinnen und Experten erarbeitet und festgelegt wurde

12.7. Forschungserfolge

Uru: "Linzer Forscher arbeiten an EU_Corona-App mit",
in *Oberösterreichische Nachrichten*, S. 22., 04.04.2020

22 Land & Leute

Linzer Forscher arbeiten an EU-Corona-App mit

60 Prozent der Bevölkerung müssten mitmachen

LINZ. Die Nutzung von Handydaten zur Bekämpfung der Verbreitung des Coronavirus wird derzeit heftig diskutiert. Das JKU-Institut für Künstliche Intelligenz unter der Leitung von Sepp Hochreiter würde als einzige österreichische Institution eingeladen, an dieser länderübergreifenden App mitzuarbeiten, teilte JKU-Rektor Meinhard Lukas beim nachmittäglichen Corona-Livestream mit.

Bereits rund 140.000 Österreicher haben sich die Tracking-App des Roten Kreuzes zur Nachvollziehbarkeit der persönlichen Kontakte (mit ein bis zwei Meter Abstand) heruntergeladen. Es müssten jedoch laut Manuel Wimmer, Institut für Wirtschaftsinformatik, „60 bis 70 Prozent der Bevölkerung" die App verwenden, damit die Neuinfektionen stark eingedämmt und die Betroffenen schnell getestet werden können.

Sepp Hochreiter ist überzeugt davon, dass die App durch künstliche Intelligenz präziser werden kann, ohne dass man die Daten zusammenführen muss. Das nämlich fürchten Datenschützer, dass die heiklen personenbezogenen Daten missbräuchlich verwendet werden könnten. Hochreiter: „Jeder behält dabei seine Daten."

Derzeit ist die Nutzung der App freiwillig. Aufgrund des massiven öffentlichen Interesses zur Erhaltung des Gesundheitssystems wird eine „App-Pflicht" diskutiert, weil

Die Rotkreuz-App Foto: ORF

sie nur bei einer entsprechenden Bevölkerungsabdeckung greife. Rechtsprofessor Andreas Janko sagt, das wäre zwar ein sehr schwerer Eingriff in die Grundrechte, sei jedoch aus seiner Sicht mit dem EU-Recht vereinbar. Das öffentliche Interesse wiege im Fall Corona mindestens so schwer.

Technisch gesehen kommunizieren zwei Smartphones auf Bluetooth-Basis miteinander. Es sei möglich, die pseudonymisierten Daten nur lokal am Handy zu speichern, so Wimmer, und sie nur bei konkreter Infektion zentral auf einem Server mit anderen Daten zu verknüpfen. Weder personenbezogene noch Ortsdaten sollten gespeichert werden, sondern nur ein daraus generierter „Schlüssel".

Uni-Professor Rene Mayrhofer vom Institute of Networks and Security plädiert dafür, dass bei so heiklen Gesundheits-Apps der Quellcode öffentlich zugänglich gemacht wird, um nachvollziehen zu können, was genau mit den Daten geschieht. (uru)

Christian-Doppler-Labor für private digitale Authentifizierung in der physischen Welt in Linz eröffnet

Das Christian-Doppler-Labor für private digitale Authentifizierung in der physischen Welt (DIGIDOW) wurde wegen Corona virtuell eröffnet.

Professor René Mayrhofer, Credit: Florian Kölig

Unter digitaler Anwesenheit von Wirtschaftsministerin Margarete Schramböck, Wirtschaftslandesrat Markus Achleitner und dem Linzer Bürgermeister Klaus Luger erklärten der Rektor der Johannes Kepler Universität Linz Meinhard Lukas, der Präsident der Christian Doppler Forschungsgesellschaft Martin Gerzabek und der Leiter des Labors, Prof. René Mayrhofer, die wissenschaftliche und gesellschaftliche Bedeutung der Forschungseinrichtung.

"Die Digitalisierung bietet uns viele Chancen und Möglichkeiten - vom elektronischen Bezahlen bis hin zum Reisepass. Damit es aber auch sicher ist, muss noch viel geforscht werden, zum Beispiel an dezentralen Lösungen wie in diesem CD-Labor. Mehr Wissen bringt mehr Möglichkeiten und größere Entscheidungsfreiheit im privaten Bereich ebenso wie für kommende politische Entscheidungen", betont Ministerin Schramböck die konkreten Fragestellungen, mit denen sich das Labor beschäftigen werde. Markus Achleitner und Klaus Luger gingen auf die Bedeutung des Labors für den Standort Linz und Oberösterreich ein.

„Daten sind das neue Gold. Die Achillesferse dabei sind jedoch der Schutz der Daten und die Datensicherheit. Daher will sich Oberösterreich auch als international sichtbares Kompetenzzentrum für IT-Sicherheit etablieren. Das neue Christian-Doppler-Labor leistet mit seinen Forschungen hier einen wichtigen Beitrag und stärkt so die Wettbewerbsfähigkeit des Wirtschaftsstandortes Oberösterreich", erklärte Wirtschafts- und Forschungs-Landesrat Markus Achleitner.

Bürgermeister Klaus Luger: „Es freut mich außerordentlich, dass der Standort Linz um eine wesentliche Forschungseinrichtung reicher geworden ist. Das Christian-Doppler-Labor stellt für mich eine gelungene Kooperation von Wissenschaft und Wirtschaft dar, die für beide zahlreiche Vorteile bringt. Die derzeitigen Entwicklungen machen es notwendig, dass wir sowohl die Innovationskraft wie auch die Wirtschaftsleistung stärken. Die Forschungsbeiträge des Labors, wie etwa die zukünftige Entwicklung des 5G-Netzes, tragen hier sicherlich dazu bei."

Wirtschaftsministerium fördert CD-Labor mit über 1 Million Euro

Neben der öffentlichen Hand sind auch eine Reihe privater Unternehmen am Labor beteiligt. Darunter die Firma NXP: „NXP ist bestrebt, seinen Kunden sichere, zuverlässige und flexible Smart City-Lösungen anzubieten ", sagt Paul Hubmer, CTO von NXP Semiconductors Austria. „Durch die Unterstützung des CDL DIGIDOW-Projekts werden wir nicht nur neue Technologien für bequeme und sichere benutzerzentrierte Lösungen nutzen, sondern uns auch auf die Herausforderungen vorbereiten, die mit kontobasierten und Cloud-Identifikations-basierten Systemen verbunden sind. In einer zunehmend vernetzten Welt setzen wir uns dafür ein, dass kommende Technologien auf einfache, sichere und zuverlässige Weise eingesetzt werden."

"Technologie wird der bestimmende Faktor für das vor uns liegende Jahrzehnt sein", so Stefan Vogl, Experte der Österreichischen Staatsdruckerei. „Der Fokus kann jedoch nicht nur auf Technologie und damit auf Kosten des Datenschutzes liegen, wir wollen auch zeigen, dass es Möglichkeiten gibt, innovative technische Lösungen unter voller Wahrung des Datenschutzes zu liefern. Deshalb ist es für uns sehr wichtig, Teil des DIGIDOW-Projekts zu sein."

Karl Stöbich von 3-Banken-IT unterstrich: „Gerade für uns – als IT-Dienstleister der Finanzindustrie – ist eine sichere digitale Authentifizierung eine notwendige Voraussetzung für die weitere Digitalisierung von Bankprozessen. Insofern hat dieses Thema bzw. unsere Teilnahme an DIGIDOW einen sehr hohen Stellenwert."

Lukas: Aufgabe der Wissenschaft ist es, Sicherheit und Freiheit zu verbinden

Rektor Meinhard Lukas unterstrich in seinen einleitenden Worten, dass es die Aufgabe der Wissenschaft sei, Sicherheit und Freiheit zu vereinen. „Wir haben eine Verantwortung der Gesellschaft und dem Einzelnen gegenüber. Wir haben die Verantwortung, umfassend und folgenabschätzend nachzudenken. Gerade die aktuelle Corona-Krise zeigt uns, wie verlockend es manchmal scheint, Grundrechte zumindest für eine kleine Weile nicht für so wichtig zu erachten. Aber diese Verlockung ist eine gefährliche, denn wer einmal eine solche Entscheidung getroffen hat, kann sie wieder treffen. Deshalb es ist von größter Bedeutung, dass die moralische Dimension schon bei der Entwicklung solcher Anwendungen implementiert ist. Ich wünsche allen Beteiligten viel Erfolg für die kommenden Jahre und die vor ihnen liegenden Forschungstätigkeiten."

„Um zum Beispiel öffentliche Verkehrsmittel benutzen oder Staatsgrenzen übertreten zu können, müssen wir Tickets bzw. einen Reisepass vorweisen. Solche physischen Objekte zur Authentifizierung können verloren, gestohlen, gefälscht, oder beschädigt werden und unterliegen daher einem Sicherheitsrisiko. Bereits in naher Zukunft wäre es technisch möglich, diese Authentifizierung auf Basis biometrischer Daten durchzuführen – Verlust oder Diebstahl physischer Elemente wären ausgeschlossen und Authentifizierung noch möglich, solange die Daten vorliegen", betonte Martin Gerzabek von der Christian Doppler Forschungsgesellschaft. Solche digitalen Identitätsnachweise könnten leicht durch zentralisierte Datenbanken, welche sämtliche biometrischen Daten von Nutzer*innen speichern, realisiert werden. Allerdings berge eine zentrale Überwachung und Speicherung aller Nutzerbewegungen und -interaktionen massives Missbrauchspotential, bis hin zur Fälschung und Löschung digitaler Identitäten.

Eine dadurch mögliche vollständige Überwachung und Kontrolle aller Nutzer*innen sei aktuell nicht mit den universellen Grundrechten auf Privatsphäre vereinbar und mit europäischen Konzepten des Datenschutzes unverträglich, erläuterte René Mayrhofer, der auch deutlich unterstrich, dass die Kombination von Wissenschaft und Ethik ein entscheidender Antrieb des Labors sein werde. So werde die interdisziplinäre Forschungsarbeit Bereiche der Kryptographie, der Netzwerke, der verteilten Systeme, der biometrischen Authentifizierung, des maschinellen Lernens und der Sicherheit von Programmcode sowie der zugehörigen sozialen, rechtlichen und ethischen Aspekte umfassen.

CHRONIK OBERÖSTERREICH 26.05.2020

Reisen ohne Pass bald möglich

Neues Labor in Linz erforscht Anwendungsmöglichkeiten biometrischer Daten.

Digitale Authentifizierung mittels biometrischen Daten könnte Vorteile bieten, etwa Reisen ohne Pass. Doch die Methode öffnet auch Missbrauch Tür und Tor und ist anfällig für Fehler. Wie es dennoch möglich ist, die Vorteile der Technologie zu nutzen, will das neue, am Dienstag an der Uni Linz eröffnete „CD-Labor für private digitale Authentifizierung in der physischen Welt" (DIGIDOW) erforschen.

Authentifizierung aufgrund biometrischer Daten

Schon in naher Zukunft wäre es technisch möglich, Authentifizierung etwa beim Übertritt einer Staatsgrenze oder der Nutzung öffentlicher Verkehrsmittel auf Basis biometrischer Daten durchzuführen, betonte der Präsident der Christian Doppler Forschungsgesellschaft (CDG), Martin Gerzabek, in einer Aussendung. Notwendig für solche digitalen Identitätsnachweise wären zentralisierte Datenbanken, wo sämtliche biometrische Daten von Nutzern gespeichert werden. Eine zentrale Überwachung und Speicherung dieser Daten sowie aller Nutzerbewegungen und -interaktionen birgt allerdings „massives Missbrauchspotenzial, bis hin zur Fälschung und Löschung digitaler Identitäten".

Die dadurch mögliche vollständige Überwachung und Kontrolle aller Nutzer sei aktuell nicht mit den universellen Grundrechten auf Privatsphäre vereinbar und mit europäischen Konzepten des Datenschutzes unverträglich, erklärte der Leiter des neuen CD-Labors, René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit der Universität Linz. Die zentrale Frage, um die sich die Forschung in dem neuen Labor dreht, ist daher, wie man die digitale Identität zur Authentifizierung in der physischen Welt nutzen kann, ohne die Privatsphäre der Nutzer zu gefährden.

Sicherheit und ethische Aspekte

Ziel sei es, mittels dezentralen Ansätzen allen Nutzern bessere Kontrolle über ihre Interaktionen in der digitalen und physischen Welt und damit über die Datenspuren, die sie notwendigerweise hinterlassen, zu geben. In der interdisziplinären Forschungsarbeit sollen auch Wissenschaft und Ethik kombiniert werden, gearbeitet wird in den Bereichen Kryptographie, Netzwerke, verteilte Systeme, biometrische Authentifizierung, maschinelles Lernen und Sicherheit von Programmcodes sowie an den zugehörigen sozialen, rechtlichen und ethischen Aspekte.

Kooperationen

In den von der CDG für jeweils sieben Jahre genehmigten CD-Laboren kooperieren Wissenschafter mit Unternehmen im Bereich der anwendungsorientierten Grundlagenforschung. Das Budget - im Fall des neuen CD-Labors mehr als eine Million Euro - kommt dabei jeweils zur Hälfte von der öffentlichen Hand und den Industriepartnern. Bei diesen handelt es sich um die NXP Semiconductors Austria GmbH, die Österreichische Staatsdruckerei, das Kepler Universitätsklinikum und die 3 Banken IT GmbH.

Autor unbekannt: "CD-Labor für private digitale Authentifizierung an Uni Linz eröffnet", in *studium.at*, 26.05.2020

STUDIUM.AT

CD-Labor für private digitale Authentifizierung an Uni Linz eröffnet

26. Mai 2020 - 12:23

Digitale Authentifizierung mittels biometrischen Daten könnte Vorteile bieten, etwa Reisen ohne Pass. Doch die Methode öffnet auch Missbrauch Tür und Tor und ist anfällig für Fehler. Wie es dennoch möglich ist, die Vorteile der Technologie zu nutzen, will das neue, an der Uni Linz eröffnete "CD-Labor für private digitale Authentifizierung in der physischen Welt" (DIGIDOW) erforschen.

Zentrale Überwachung der Daten birgt "massives Missbrauchspotenzial

Schon in naher Zukunft wäre es technisch möglich, Authentifizierung etwa beim Übertritt einer Staatsgrenze oder der Nutzung öffentlicher Verkehrsmittel auf Basis biometrischer Daten durchzuführen, betonte der Präsident der Christian Doppler Forschungsgesellschaft (CDG), Martin Gerzabek, in einer Aussendung. Notwendig für solche digitalen Identitätsnachweise wären zentralisierte Datenbanken, wo sämtliche biometrische Daten von Nutzern gespeichert werden. Eine zentrale Überwachung und Speicherung dieser Daten sowie aller Nutzerbewegungen und -interaktionen birgt allerdings "massives Missbrauchspotenzial, bis hin zur Fälschung und Löschung digitaler Identitäten".

Überwachung nicht mit Grundrechten vereinbar

Die dadurch mögliche vollständige Überwachung und Kontrolle aller Nutzer sei aktuell nicht mit den universellen Grundrechten auf Privatsphäre vereinbar und mit europäischen Konzepten des Datenschutzes unverträglich, erklärte der Leiter des neuen CD-Labors, René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit der Universität Linz. Die zentrale Frage, um die sich die Forschung in dem neuen Labor dreht, ist daher, wie man die digitale Identität zur Authentifizierung in der physischen Welt nutzen kann, ohne die Privatsphäre der Nutzer zu gefährden.

Ziel sei es, mittels dezentralen Ansätzen allen Nutzern bessere Kontrolle über ihre Interaktionen in der digitalen und physischen Welt und damit über die Datenspuren, die sie notwendigerweise hinterlassen, zu geben. In der interdisziplinären Forschungsarbeit sollen auch Wissenschaft und Ethik kombiniert werden, gearbeitet wird in den Bereichen Kryptographie, Netzwerke, verteilte Systeme, biometrische Authentifizierung, maschinelles Lernen und Sicherheit von Programmcodes sowie an den zugehörigen sozialen, rechtlichen und ethischen Aspekte.

In den von der CDG für jeweils sieben Jahre genehmigten CD-Laboren kooperieren Wissenschafter mit Unternehmen im Bereich der anwendungsorientierten Grundlagenforschung. Das Budget - im Fall des neuen CD-Labors mehr als eine Million Euro - kommt dabei jeweils zur Hälfte von der öffentlichen Hand und den Industriepartnern. Bei diesen handelt es sich um die NXP Semiconductors Austria GmbH, die Österreichische Staatsdruckerei, das Kepler Universitätsklinikum und die 3 Banken IT GmbH.

Autor unbekannt: "Neues Institut forscht zu sicherer Datennutzung", in *Science ORF*, 26.05.2020

Schon in naher Zukunft wäre es technisch möglich, Authentifizierung etwa beim Übertritt einer Staatsgrenze oder der Nutzung öffentlicher Verkehrsmittel auf Basis biometrischer Daten durchzuführen, betonte der Präsident der Christian Doppler Forschungsgesellschaft (CDG), Martin Gerzabek, in einer Aussendung. Notwendig für solche digitalen Identitätsnachweise wären zentralisierte Datenbanken, wo sämtliche biometrische Daten von Nutzern gespeichert werden. Eine zentrale Überwachung und Speicherung dieser Daten sowie aller Nutzerbewegungen und -interaktionen birgt allerdings „massives Missbrauchspotenzial, bis hin zur Fälschung und Löschung digitaler Identitäten".

Die dadurch mögliche vollständige Überwachung und Kontrolle aller Nutzer sei aktuell nicht mit den universellen Grundrechten auf Privatsphäre vereinbar und mit europäischen Konzepten des Datenschutzes unverträglich, erklärte der Leiter des neuen „CD-Labors für private digitale Authentifizierung in der physischen Welt" (DIGIDOW), René Mayrhofer, Vorstand des Instituts für Netzwerke und Sicherheit der Universität Linz. Die zentrale Frage, um die sich die Forschung in dem neuen Labor dreht, ist daher, wie man die digitale Identität zur Authentifizierung in der physischen Welt nutzen kann, ohne die Privatsphäre der Nutzer zu gefährden.

Daten besser kontrollieren

Ziel sei es, mittels dezentraler Ansätze allen Nutzern bessere Kontrolle über ihre Interaktionen in der digitalen und physischen Welt und damit über die Datenspuren, die sie notwendigerweise hinterlassen, zu geben. In der interdisziplinären Forschungsarbeit sollen auch Wissenschaft und Ethik kombiniert werden, gearbeitet wird in den Bereichen Kryptographie, Netzwerke, verteilte Systeme, biometrische Authentifizierung, maschinelles Lernen und Sicherheit von Programmcodes sowie an den zugehörigen sozialen, rechtlichen und ethischen Aspekte.

In den von der CDG für jeweils sieben Jahre genehmigten CD-Laboren kooperieren Wissenschafter mit Unternehmen im Bereich der anwendungsorientierten Grundlagenforschung. Das Budget - im Fall des neuen CD-Labors mehr als eine Million Euro - kommt dabei jeweils zur Hälfte von der öffentlichen Hand und den Industriepartnern. Bei diesen handelt es sich um die NXP Semiconductors Austria GmbH, die Österreichische Staatsdruckerei, das Kepler Universitätsklinikum und die 3 Banken IT GmbH.

OÖNachrichten

WIRTSCHAFTSRAUM OÖ

Grenzübertritt bald überall ohne Reisepass?

Laborleiter René Mayrhofer

LINZ. Digitaler Identitätsnachweis: Christian-Doppler-Labor forscht an dezentraler Speicherung von Daten.

Ohne Pass in ein anderes Land reisen, eine Tür öffnen, ohne vorher einen Schlüssel ins Schloss zu stecken, oder Straßenbahn fahren, ohne dem Kontrolleur ein gültiges Ticket vorweisen zu müssen: An der Linzer Kepler Uni (JKU) forscht ein Team daran, um all diese Dinge in Zukunft möglich zu machen und gleichzeitig den Schutz unserer Daten zu gewährleisten.

In (digitaler) Anwesenheit von Rektor Meinhard Lukas und Wirtschaftsministerin Margarete Schramböck wurde gestern an der JKU das "Christian-Doppler-Labor für private digitale Authentifizierung in der physischen Welt" (Digidow) eröffnet, das von René Mayrhofer geleitet wird. Den Verzicht auf Dokumente ermöglichen die Digitalisierung und die Speicherung sogenannter biometrischer Daten, sagt Mayrhofer: "Der Kreativität sind hier keine Grenzen gesetzt. Auch der Führerschein oder ein Bonusprogramm im Supermarkt kann auf diese Weise abgewickelt werden."

Der große Vorteil bestehe in der Bequemlichkeit. Ein physisches Objekt könne außerdem gestohlen werden. In einem ersten Schritt würden Dokumente und Tickets auf dem Smartphone gespeichert werden. Die Vision sei aber, dass Personen in Zukunft beim Grenzübertritt identifiziert werden können, ohne ein Smartphone oder einen Pass mitzuführen. Das Problem besteht laut Mayrhofer darin, dass die zentrale Speicherung biometrischer Daten, also etwa eines Fingerabdrucks, Tür und Tor für Missbrauch öffne, etwa für anlassunabhängige Überwachung. Am Linzer Doppler-Labor wird daher geforscht, wie die Daten dezentral gespeichert werden können.

Seyringer, Karin: "Reisen ohne Pass, Türen ohne Schlüssel öffnen:
Neues Doppler Labor an der JKU forscht an der Zukunft der digitalen Identität", in *Tips*, 27.05.2020

Tips

Reisen ohne Pass, Türen ohne Schlüssel öffnen: Neues Doppler Labor an der JKU forscht an der Zukunft der digitalen Identität

LINZ. Die JKU und damit Linz ist um eine bemerkenswerte neue Forschungseinrichtung reicher: Das neue „Christian Doppler Labor für private digitale Authentifizierung in der physischen Welt" (DIGIDOW) wurde mit einer virtuellen Feier eröffnet. Unter der Leitung von Professor René Mayrhofer wird der Frage nachgegangen, wie digitale Identität für die Authentifizierung in der physischen Welt genutzt werden kann, ohne die Privatsphäre der Nutzer zu gefährden.

Reisen ohne Pass, Türen öffnen ohne Schlüssel, Straßenbahn-Fahren ohne physisches Ticket – die Digitalisierung und die Speicherung biometrischer Daten könnte das möglich machen. Aber: zentralisierte Datenbanken für biometrische Daten können auch eine große Gefahr darstellen, wie Missbrauch bei Massenüberwachung, sie sind auch anfällig für Fehler und Daten-Leaks.

An der Linzer Kepler Uni (JKU) forscht das neue Labor nun daran, um all diese Dinge in Zukunft möglich zu machen und gleichzeitig den Schutz der Daten zu gewährleisten.

„Was jetzt zum Beispiel im zentralen Melderegister vorliegt, sind eher statische Daten, Stammdaten, die sich nicht so schnell ändern. Jedes Mal aber wenn ich in eine Straßenbahn steige, eine Bürotüre aufmache, dann fallen ungleich viel mehr Daten an. Das ist etwas, vor dem wir etwas Angst haben, und ist einer der Ausgangspunkte, warum dieses Labor gegründet wurde", so Mayrhofer.

Geforscht wird an dezentralen Lösungen, um alle Nutzern bessere Kontrolle über ihre Interaktionen in der digitalen sowie physischen Welt und damit den Datenspuren, die sie notwendigerweise hinterlassen, zu geben.

Jährliche Prototypen werden den Fortschritt demonstrieren und die Evaluierung anhand konkreter Anwendungsfälle ermöglichen.

Virtuelle Eröffnungsfeier

Unter digitaler Anwesenheit von Wirtschaftsministerin Margarete Schramböck, Wirtschaftslandesrat Markus Achleitner und dem Linzer Bürgermeister Klaus Luger erklärten JKU-Rektor Meinhard Lukas, der Präsident der Christian Doppler Forschungsgesellschaft Martin Gerzabek und der Leiter des Labors René Mayrhofer bei der Eröffnungsfeier die wissenschaftliche und gesellschaftliche Bedeutung der Forschungseinrichtung.

„Die Digitalisierung bietet uns viele Chancen und Möglichkeiten – vom elektronischen Bezahlen bis hin zum Reisepass. Damit es aber auch sicher ist, muss noch viel geforscht werden", betonte Ministerin Schramböck. Das Wirtschaftsministerium fördert das neue Labor mit über einer Million Euro, dazu kommt Unterstützung privater Unternehmer.

Landesrat Achleitner und Bürgermeister Luger gingen auf die Bedeutung des Labors für den Standort Linz und Oberösterreich ein. „Daten sind das neue Gold. Die Achillesferse dabei sind jedoch der Schutz der Daten und die Datensicherheit. Daher will sich Oberösterreich auch als international sichtbares Kompetenzzentrum für IT-Sicherheit etablieren", so Achleitner. Luger pflichtet bei: „Es freut mich außerordentlich, dass der Standort Linz um eine wesentliche Forschungseinrichtung reicher geworden ist. Das Christian-Doppler-Labor stellt für mich eine gelungene Kooperation von Wissenschaft und Wirtschaft dar, die für beide zahlreiche Vorteile bringt."

„Sicherheit und Freiheit verbinden"

„Aufgabe der Wissenschaft ist es, Sicherheit und Freiheit zu verbinden", unterstreicht Rektor Lukas. „Wir haben eine Verantwortung der Gesellschaft und dem Einzelnen gegenüber. Wir haben die Verantwortung, umfassend und folgenabschätzend nachzudenken. Gerade die aktuelle Corona-Krise zeigt uns, wie verlockend es manchmal scheint, Grundrechte zumindest für eine kleine Weile nicht für so wichtig zu erachten. Aber diese Verlockung ist eine gefährliche, denn wer einmal eine solche Entscheidung getroffen hat, kann sie wieder treffen. Deshalb es ist von größter Bedeutung, dass die moralische Dimension schon bei der Entwicklung solcher Anwendungen implementiert ist. Ich wünsche allen Beteiligten viel Erfolg für die kommenden Jahre und die vor ihnen liegenden Forschungstätigkeiten."

„Ambitionierter Projektplan"

Der Projektplan des neuen Labors sei ambitioniert, so Mayrhofer, im zweiten Jahr könne man vielleicht schon beim Partner Kepler Universitäts Klinikum Probleme im medizinischen Alltag angehen, etwa Türen nicht mehr händisch zu öffnen (Stichwort Einweghandschuhe), sondern mit Gesichtserkennung.

Kronen Zeitung

NACHRICHTEN BUNDESLÄNDER SPORT ADABEI DIGITAL FREIZEIT AUTO TR

Wien NÖ / Bgld. Oberösterreich Steiermark Kärnten Salzburg Tirol / Vbg.

FORSCHUNG IN OÖ

Daten sind „neues Gold", Sicherheit bleibt Thema

Margarete Schramböck ist Bundesministerin für Digitalisierung und Wirtschaftsstandort

Die Linzer JKU bekommt ein neues Forschungslabor. Es wird sich mit Digitalisierung beschäftigen, konkret mit Regeln und Lösungen für mehr Datensicherheit. Das Wirtschaftsministerium fördert das neue Christian-Doppler-Labor mit mehr als 1 Million Euro.

Die Corona-Krise bringt Apps zur Verfolgung von Kontakten hervor, aber auch die Verarbeitung von Gesundheitsdaten und biometrischen Daten nimmt zu. „Damit Digitalisierung sicher ist, muss viel geforscht werden", umreißt Ministerin Margarete Schramböck die Aufgaben des neuen JKU-Labors. Es wurde gestern per Videokonferenz eröffnet.

René Mayrhofer, Professor an der JKU, wird das neue Labor für Datensicherheit leiten.

Impuls für Wirtschaft

„Daten sind das neue Gold. Die Achillesferse dabei sind jedoch der Schutz der Daten und die Datensicherheit. Daher will sich Oberösterreich auch als international sichtbares Kompetenzzentrum für IT-Sicherheit etablieren", erklärte Wirtschafts- und Forschungs-Landesrat Markus Achleitner. Das neue Christian-Doppler-Labor leistet mit seinen Forschungen hier einen wichtigen Beitrag und stärkt so die Wettbewerbsfähigkeit des Wirtschaftsstandortes. Uni-Professor René Mayrhofer, Experte für Datensicherheit hat die Leitung inne. In OÖ gibt es bereits mehr als 20 Doppler-Labore und Ressel-Zentren.

APA: "Physiker schreiben Quanteninformation in Nano-Halbleiter ein", in *Der Standard*, 09.10.2020

DERSTANDARD · Wissenschaft

COMPUTER-EVOLUTION

Physiker schreiben Quanteninformation in Nano-Halbleiter ein

Forscher aus Linz und Großbritannien konnten zwei kontrollierbare Quantenbits in Galliumarsenid-Gitter herstellen

9. Oktober 2020, 15:38, 6 Postings

Linz – Damit Quantencomputer oder -internet funktionieren können, muss die flüchtige Quanteninformation in kontrollierbare Systeme eingeschrieben werden. Das sind zum Beispiel Ionen oder Photonen. In Kooperation mit Kollegen aus Großbritannien haben nun Linzer Physiker zwei Quanteninformationseinheiten (Qubits) in einer einzelnen Halbleiter-Nanostruktur realisiert, wie sie im Fachblatt "Nature Nanotechnology" berichten. Aus technischer Sicht könnte sich das als nützlich erweisen.

Information in Halbleiter-Quantenpunkte zu packen könnte nach Ansicht der Forscher einen Entwicklungssprung in der Entwicklung leistungsfähiger Computer darstellen.

Das Team um Armando Rastelli vom Institut für Halbleiter- und Festkörperphysik der Universität Linz beschäftigt sich mit der Herstellung von Halbleiter-Nanostrukturen und im speziellen mit sogenannten Quantenpunkten. Dabei handelt es sich um Objekte bestehend aus einigen Tausend Atomen, die sich gemeinschaftlich wie ein künstliches "Makroatom" verhalten, so Rastelli. Im vergangenen Jahr hat der Forscher mit Kollegen bereits gezeigt, dass sich damit unter bestimmten Bedingungen sehr effizient quantenphysikalisch verschränkte Lichteilchen (Photonen) erzeugen lassen, die aber beliebig große Distanzen hinweg in Wechselbeziehung zueinander stehen. Eine Eigenschaft, die für technische Anwendungen der Quantenmechanik zentral ist.

KURIER

Ihr Kind will Friseur oder Friseurin werden?

Perfekt, denn KURIER sucht genau(!) SO

System aus zwei Qubits

Zusammen mit Evgeny Chekhovich von der University of Sheffield (Großbritannien) haben die Wissenschafter nun versucht, Quantenpunkte aus Galliumarsenid nicht nur als Lichtquelle, sondern als Quantenregister zu nutzen. Dabei handelt es sich um ein ebenfalls verbundenes System aus einzeln manipulierbaren Quantenbits (Qubits). Diese bilden die kleinste Informationseinheit im Quantencomputer und haben den Vorteil, dass sie nicht nur die Zustände "0" und "1", sondern auch beide Zustände gleichzeitig annehmen können. Physiker sprechen hier von "Superposition".

So ist es gelungen "ein System aufzubauen, das zwei Qubits enthält", sagte Rastelli. Als Träger der Information fungieren hier rund einhunderttausend Arsen-75-Atomkerne in dem Galliumarsenid-Gitter. Gesteuert werden deren Eigenschaften mittels Licht und Radiofrequenz-Signalen. Um die so eingeschriebene Information wieder auszulesen, verwenden die Physiker wieder Laserlicht. Im Rahmen der Arbeit konnte man zeigen, dass die Qubits rund 20 Millisekunden stabil bleiben. Das sei lange genug, um bis zu 100 Operationen durchzuführen, was eine erkleckliche Anzahl an Rechenmöglichkeiten eröffnet.

Natürliche Computetr-Evolution

Die Idee, Information in Halbleiter-Quantenpunkte zu packen, ist interessant, weil "die ganze Elektronik auf Basis von Halbleitern funktioniert. Würde man es schaffen, auf dieser Basis einen Quantencomputer zu bauen, wäre das die natürliche Evolution herkömmlicher Computer", so Rastelli. Dazu brauchte es freilich deutlich mehr verschränkte Qubits als die bisher realisierten zwei. "Wie man das hochskalieren könnte, ist noch nicht klar", räumte der Physiker ein. Der Gedanke sei aber durchaus verlockend, für Quantencomputer-Hardware nicht in eine völlig andere Materialumgebung oder Plattformen wechseln zu müssen.

"Wir wollen in Zukunft schauen, wie weit wir mit Halbleitern alleine kommen", sagte Rastelli. Gleichzeitig koordiniert der Physiker auch eine Forschungsgruppe, in die Wissenschafter der traditionell starken Quantenphysik-Standorte an der Uni Innsbruck und Uni Wien eingebunden sind, die auf andere Quantensysteme wie Photonen oder Ionen setzen. "Die gängige Meinung ist, dass wahrscheinlich mehrere Plattformen für unterschiedliche Zwecke kombiniert werden müssen." (APA, 9.10.2020)

11/2020: "Willkommen in der Zukunft – wie Digitalisierung unser Leben verändert", in *Die Oberösterreicherin*, Ausgabe November, S. 155

Willkommen in der Zukunft – wie Digitalisierung unser Leben verändert

Wo ein Wille, da ein Weg: Informatiker Robert Wille erhält renommierten ERC Consolidator Grant für Forschung zu Quantencomputern

Einer der begehrten Grants geht heuer an Prof. Robert Wille vom LIT der JKU. Er entwickelt Methoden, mit denen die Arbeit von Quantencomputern verbessert wird.

Professor Robert Wille

Der Consolidator Grant des Europäischen Forschungsrats (European Research Council) zählt zu den renommiertesten Wissenschaftsauszeichnungen Europas. Einer der begehrten Grants geht heuer an ein Forschungsteam, das der Zukunft vorgreifen will: Prof. Robert Wille vom LIT der Johannes Kepler Universität Linz entwickelt Methoden, mit denen die Arbeit von Quantencomputern verbessert wird. Die Fördersumme: Zwei Millionen Euro.

Es ist eine (ober-)österreichische Erfolgsgeschichte: Vor fünf Jahren wurde Prof. Robert Wille im Alter von 32 Jahren als einer der jüngsten Professoren an die JKU berufen. Hier leitet er heute das Institute for Integrated Circuits und das Secure and Correct Systems Lab des Linz Institute of Technology (LIT). Seit Mai ist Wille zudem wissenschaftlicher Leiter des Software Competence Centers Hagenberg (SCCH). Seine internationale hoch geschätzte Arbeit wird nun mit einen der renommiertesten Wissenschaftsauszeichnungen Europas gewürdigt: Robert Wille erhält den ERC Consolidator Grant.

Neue Phase der Informatik

Das hat seinen Grund: Quantencomputer werden – so die Meinung der Expert*innen – in absehbarer Zeit die Informatik revolutionieren. Entsprechend gibt es einen weltweiten Wettlauf um die Entwicklung dieser Computer. Momentan gibt es erste Modelle von Quantencomputern, die bereits für einige ausgewählte Probleme vielversprechende Lösungen anbieten. Es wird erwartet, dass diese in wenigen Jahren ein gewisse „Marktreife" erreichen. Diese „Quantencomputer" können dann in kurzer Zeit speziell entworfene Aufgaben lösen, für die sogar die schnellsten aktuell existierenden Supercomputer Jahrtausende brauchen würden.

Konzentration auf Software

Der beste Computer nutzt allerdings nichts ohne entsprechende Programmierung und Entwurfswerkzeuge. Hier sind aber im Vergleich zu aktuellen Computern völlig neue Ansätze und Problemstellungen zu bewältigen. Und dafür sind Prof. Wille und sein Team weltweit anerkannte Expert*innen. *„Für konventionelle Rechner haben wir hocheffiziente Verfahren und Werkzeuge, um entsprechende Programme zu entwickeln. Diese fehlen uns bisher für Quantencomputer. Wir laufen Gefahr, dass wir am Ende hoch leistungsfähige Quantencomputer entwickeln, deren volles Potenzial aber nicht perfekt ausnutzen können,"* sagt Prof. Wille.

Im vom ERC unterstütztem Forschungsprojekt werden Methoden für die Simulation und den Nachweis der Korrektheit entsprechender Quantenprogramme erforscht. Außerdem werden so genannte Compiler entwickelt, die Quantenprogramme automatisch übersetzen, so dass sie auch auf den tatsächlichen Maschinen ausgeführt werden können. In den Arbeiten kooperiert das Team von Prof. Wille mit Kolleg*innen aus Wissenschaft und Industrie weltweit. Das Projekt wird mit zwei Millionen Euro für die nächsten Jahre gefördert. *„Ein ERC Grant ist eine ganz besondere Auszeichnung, auf die ich sehr stolz und für die ich sehr dankbar bin. Es ist das Ergebnis von zwei Jahren Vorbereitung und Teamwork an der JKU und ich freue mich, jetzt mit der Umsetzung unserer Ideen beginnen zu können"* freut sich Prof. Wille.

„Ich freue mich für Professor Wille und sein Team. In ihrer Forschung geht es um nicht weniger als die Zukunft des Computers. Der ERC Consolidator Grant ist ein internationales Markenzeichen. Prof. Wille hat damit auf eindrucksvolle Weise bestätigt, dass er zur Spitze der europäischen Forschungsgemeinschaft gehört. Zugleich ist es ein weiteres Kompliment für das LIT und den Fachbereich Informatik der JKU, der zuletzt auch im weltweiten THE-Ranking einen großen Sprung nach vorne gemacht hat", so JKU Rektor Meinhard Lukas. Zugleich sei es eine weitere Bestätigung dafür, dass Oberösterreich der richtige Standort für die neue Technische Universität für Digitalisierung und digitale Transformation sei und der JKU bei der Gründung eine Schlüsselrolle zukommen müsse. Lukas betonte abschließend, dass der Preis auch eine Auszeichnung für ein neues, übergreifendes Verständnis von Technologie sei, das Wille und sein Team an den Tag legen. *„Gerade mit diesem Mindset ist eine Entwicklung möglich, die uns auch im internationalen Vergleich hervorstechen lässt."*

Michael Schäfl: "Wegbereiter für Quantencomputer",
in *Oberösterreichische Nachrichten*, 10.12.2020, Seite unbekannt

---

OBERÖSTERREICHER DES TAGES

Wegbereiter für Quantencomputer

Robert Wille erhält einen der begehrtesten Wissenschaftspreise Europas

VON MICHAEL SCHÄFL

Wo ein Wille, da ein Weg: Einer der renommiertesten Wirtschaftspreise Europas geht heuer nach Oberösterreich. Robert Wille, Professor für Integrierte Schaltungen an der Linzer Johannes-Kepler-Universität, sicherte sich den begehrten „Consolidator Grant" des European Research Council. Und die damit verbundene Fördersumme von zwei Millionen Euro.

„Das ist die mit Abstand höchste Auszeichnung, die ich bis jetzt bekommen habe", sagt der Bremer. „Der größte Erfolg meiner wissenschaftlichen Karriere. Gleich nach meiner Berufung nach Linz, die ist mir natürlich noch wichtiger." Es ist eine oberösterreichische Erfolgsgeschichte. Vor fünf Jahren kam Robert Wille von Deutschland an die Kepler-Uni und wurde hier zu einem der jüngsten Professoren. „Ich habe in Bremen Informatik studiert und promoviert, war an der Uni Potsdam und in Dresden, aber als ich hörte, dass an der JKU eine Stelle frei wird, habe ich mich sofort beworben", sagt der 38-Jährige. Seither leitet er das Institut für Integrierte Schaltungen und gemeinsam mit Rene Mayrhofer das Secure and Correct Systems Lab des Linz Institute of Technology (LIT). Doch dem nicht genug, seit Mai ist Robert Wille zudem wissenschaftlicher Leiter des Software-Kompetenzzentrums Hagenberg. Viel Freizeit bleibt da nicht. „Aber das macht nichts, meine Arbeit ist meine Passion, Arbeits- und Freizeit fließen quasi ineinander", sagt der Informatiker. „Wenn ich am Wochenende eine tolle Idee habe, dann bastle ich daran." Wofür er die zwei Millionen Euro an Forschungsgeldern aufwenden möchte, ist für Wille klar: Sie fließen in seine Passion, die Erforschung des Quantencomputers. Eine neue Art der Technologie, schneller und leistungsfähiger als herkömmliche Computer. „So können wir Probleme, die wir mit unseren bekannten Computern in Jahrhunderten nicht lösen könnten, schneller bearbeiten", sagt der 38-Jährige. „Jetzt können wir den Quantensprung hinbekommen."

„Dieser Preis ist der größte Erfolg meiner wissenschaftlichen Karriere. Gleich nach meiner Berufung nach Linz."

Robert Wille, Professor für Integrierte Schaltungen, JKU

APA: "18 in Österreich tätige Forscher erhalten vom ERC Millionen-Förderung",
in *Der Standard*, 10.12.2020

DERSTANDARD › Wissenschaft

EUROPÄISCHEN FORSCHUNGSRAT

18 in Österreich tätige Forscher erhalten vom ERC Millionen-Förderung

"Consolidator Grants" sollen helfen, Position als eigenständige Forscher zu festigen

9. Dezember 2020, 14:15, 11 Postings

Die rekordverdächtige Zahl von 18 in Österreich tätigen Wissenschaftern erhält einen sogenannten Consolidator Grant des Europäischen Forschungsrats ERC. Die mit jeweils bis zu drei Millionen Euro dotierte Förderung soll es Wissenschaftern ermöglichen, ihre Position als eigenständige Forscher zu festigen.

Insgesamt erhalten in der aktuellen Ausschreibungsrunde 327 Forscher eine solche Förderung, dabei werden in Summe 655 Millionen Euro ausgeschüttet. Die Fördernehmer kommen aus 39 Ländern und werden in 23 europäischen Staaten ihre Projekte verwirklichen. Die meisten Preise gingen an Projekte in Deutschland und Großbritannien (jeweils 50), Frankreich (34) und den Niederlanden (29). Unter den 18 hierzulande durchgeführten Projekten, die mit einem Grant bedacht wurden, lassen sich acht den Bereichen Geistes-, Kultur- und Sozialwissenschaften zuordnen.

Universität Wien stark vertreten

Die meisten Förderpreise gehen an die Universität Wien, wo gleich sieben Wissenschafter einen Consolidator Grant erhalten: **Tara Andrews** vom Institut für Geschichte will in ihrem ERC-Projekt mit digitalen Methoden Kontakte und Kommunikation der gesamten christlichen Welt im 11. Jahrhundert unter die Lupe nehmen und damit das Verständnis der kulturellen und gesellschaftlichen Trends zu jener Zeit verbessern, als die Kreuzzüge lanciert wurden. Wie man mit Hilfe elektrischer Felder winzige Teilchen dirigiert und damit einen Ausgangspunkt für hochfunktionelle Materialien schafft, etwa zur Effizienzsteigerung von Brennstoff-Zellen, wird die Chemikerin **Jia Min Chin** vom Institut für Physikalische Chemie untersuchen.

Julia Lajta-Novak vom Institut für Anglistik und Amerikanistik der Uni Wien will in ihrem Projekt ein wichtiges Kapitel der britischen und irischen Lyrikgeschichte (1965-2020) neu schreiben, indem sie den Fokus vom geschriebenen auf das gesprochene Wort verlegt und damit eine Methode der Lyrikgeschichtsschreibung entwickeln, die speziell auf den mündlichen Vortrag abzielt. In noch nie da gewesener molekularer Detailgenauigkeit will **Joao Matos** vom Department für Chromosomenbiologie zeigen, wie der Austausch von mütterlicher und väterlicher genetischen Informationen entlang von Chromosomen vor sich geht. Sogenannte Catalan-Zahlen stehen im Mittelpunkt des ERC-Projekts von **Anton Mellit** vom Institut für Mathematik, in dem er algebraische und geometrische Methoden zusammenführen will, um offene Probleme in der Mathematik zu adressieren.

Indem sie Mikroben auf Marsmeteoritengestein züchtet, will **Tetyana Milojevic** vom Institut für Biophysikalische Chemie der Uni Wien besser verstehen, wie voraussichtlich schon bald zur Verfügung stehende Proben vom Mars auf Spuren von Leben und auf potenzielle biologische Signaturen hin untersucht werden können. **Heinz Christoph Steinhardt** vom Institut für Ostasienwissenschaften untersucht in seinem Projekt das soziale Kreditsystem, mit dem China vertrauenswürdigeres Verhalten in Wirtschaft und Gesellschaft anstrebt.

Für Grants für ÖAW-Forscher

Seit Anfang November an der Uni Wien tätig ist eigentlich auch **Eva Beaujouan** vom Institut für Demographie. Vom ERC wird sie aber noch der Österreichischen Akademie der Wissenschaften (ÖAW), ihrer bisherigen Arbeitsstätte, zugerechnet, die mit ihr auf fünf "Consolidator"-Preise kommt. Beaujouan wird in ihrem Projekt Faktoren untersuchen, die das Kinderkriegen von Eltern über 30 Jahren in Ländern mit niedrigen Geburtenraten beeinflussen. **Andrea Cuomo** vom Institut für Mittelalterforschung will mit digitalen Methoden zu einem tieferen Verständnis von spätbyzantinischem Griechisch beitragen. **Pascale Hugon** vom Institut für Kultur- und Geistesgeschichte Asiens, widmet sich der frühen Entwicklung der tibetischen Scholastik und will damit tibetischen Denkern mehr Aufmerksamkeit verschaffen.

Wie menschliche Immunzellen gezielt für die Bekämpfung von Tumoren eingesetzt werden können, ist das Ziel des ERC-Projekts von **Christoph Bock** vom Forschungszentrum für Molekulare Medizin (CeMM) der ÖAW. **Nicolas Rivron** vom Institut für Molekulare Biotechnologie (IMBA) geht mit seinem Projekt der Frage nach, wie sich Zellen während der Entwicklung selbst organisieren, um einen gesunden Organismus zu formen.

Weitere Institutionen

Robert Wille vom Institut für Integrierte Schaltungen der Universität Linz arbeitet in seinem ERC-Projekt an Methoden für die Simulation und den Nachweis der Korrektheit von Programmen für Quantencomputer und entwickelt Compiler, die Quantenprogramme so übersetzen, dass sie auch ausgeführt werden können. **Raya Muttarak** vom Internationalen Institut für angewandte Systemanalyse (IIASA) in Laxenburg bei Wien will in ihrem ERC-Projekt die Auswirkungen des globalen Klimawandels auf die Bevölkerungsentwicklung abschätzen und prognostizieren.

Zwei ERC-Grants gehen an die Universität Innsbruck: **Ivana Stiperski** vom Institut für Atmosphären- und Kryosphärenwissenschaften will die Theorie für Turbulenzen in der Atmosphäre und damit Wettervorhersagen und Klimaprojektionen über Berggebieten verbessern. Als "molekularer Architekt" wird **Thomas Magauer** vom Institut für Organische Chemie sogenannte Polyencyclisierungen untersuchen, um derzeit unzugängliche Naturstoffe mit beispielsweise krebs-, antiviraler oder entzündungshemmender Wirkung zu konstruieren.

Ein Simulationssystem für Transporte zu Wasser und zu Land zwischen der Adria und der Donau im ersten Jahrhundert unserer Zeitrechnung will **Leif Scheuermann** vom Zentrum für Informationsmodellierung der Universität Graz in seinem Projekt aufbauen und dabei unter anderem mit Experimenten zur Ermittlung des Fahrverhaltens römischer Karren und Kähne möglichst realitätsnahe Transportzeiten errechnen. **Laura Kovacs** vom Institute of Logic and Computation der Technischen Universität (TU) Wien schließlich will auf Basis der mathematischen Logik Methoden entwickeln, die automatisch analysieren, ob Computercodes fehlerhaft sind oder nicht. Mit dem aktuellen Consolidator Grant erhält sie bereits ihren dritten Förderpreis vom ERC. (APA, red, 9. 12. 2020)

Autor unbekannt: "Top-Auszeichnung für Robert Wille vom LIT", in *Volksblatt*, 13.12.2020

Top-Auszeichnung für Robert Wille vom LIT

Der Consolidator Grant des Europäischen Forschungsrats (European Research Council) zählt zu den renommiertesten Wissenschaftsauszeichnungen Europas. Einer der begehrten Grants geht heuer an ein Forschungsteam, das der Zukunft vorgreifen will: Der 37-jährige Robert Wille vom LIT der Johannes Kepler Universität Linz entwickelt Methoden, mit denen die Arbeit von Quantencomputern verbessert wird. „Für konventionelle Rechner haben wir hocheffiziente Verfahren und Werkzeuge, um entsprechende Programme zu entwickeln. Diese fehlen uns bisher für Quantencomputer. Wir laufen Gefahr, dass wir am Ende deren volles Potenzial aber nicht perfekt ausnutzen können," erklärt Wille.

Menschen

Sonntag | 13. Dezember 2020 | www.kurier.at

16 KURIER

Managerin des Jahres
Die Buchhändlerin Melanie Hofinger ist Gewinnerin der VKB-Auszeichnung „Managerin des Jahres".

Robert Wille pendelt zwischen Bremen und Linz

Glosse

VON CLAUDIA STELZEL-PÖLL

Miteinander reden, wäre sinnvoll gewesen

Ein Corona-Massentest in einem Schulzentrum, das an zwei von vier Tagen im Vollbetrieb ist. Wissen Sie, wer das versteht? Außer denen, die es beschlossen haben, genau niemand. Wir reden hier bzw. von Volksschule, Mittelstufe, Hort, Kindergarten und Krabbelstube in mehreren Gebäudeteilen, die aber alle miteinander verbunden sind, sich teils Ein- und Durchgänge teilen. Die Aufregung in Pasching war groß, als die Entscheidung bekannt gegeben wurde. Vor allem: Es gibt so viele schlüssige Alternativen, die mit wenig Aufwand und Willen bestens gepasst hätten. Ja, ich bin in diesem Fall befangen, weil meine beiden Ihren Tochter besuchen in besagtem Zentrum die Volksschule, die jüngste den Kindergarten. Wir Eltern dürfen seit Wochen das Gebäude – verständlicherweise – nicht betreten, aber jetzt schleust man innerhalb von vier Tagen zwei fremde Schulfremde durchs Haus.

Was geholfen hätte? Miteinander reden, über die Gemeindegrenzen hinausdenken, Bedenken ernst nehmen und deuteln. Drüberfahren ist einfach, ein gleichwertiges Miteinander aber viel verbindender.

claudia.stelzl@kurier.at

„Bin ein Herzblut-Informatiker"

Robert Wille. Der Linzer Professor erhält den mit zwei Mio. Euro dotierten Wissenschaftspreis Consolidator Grant

VON JOSEF ERTL

Der Nobelpreis ist mit einer Million Euro dotiert. Der Linzer Informatiker **Robert Wille** erhält nun einen Förderpreis von zwei Millionen Euro, den „Consolidator Grant" des Europäischen Forschungsrates. „Damit sind wir in der internationalen Spitze", so Wille zum KURIER.

Der 37-jährige Deutsche entwickelt Methoden, mit denen die Arbeit von Quantencomputern verbessert wird. Vor fünf Jahren wurde er im Alter von 32 Jahren als einer der jüngsten Professoren an die Linzer Kepler Universität (JKU) berufen. Wille leitet heute das Institute für Integrated Circuits and Correct Systems Lab des Linz Institute of Technology (LIT). Seit Mai ist er zudem wissenschaftlicher Leiter des Software Competence Centers Hagenberg (80 Mitarbeiter).

„Wir haben für Quantencomputer eine neue Technologie, die für bestimmte Probleme deutlich besser und schneller ist, für die konventionelle Rechner Tausende von Jahren brauchen können", erklärt Wille seine Arbeit. „Wir haben bei den Quantenrechnern Physiker, die eine Erfolgsmeldung nach der anderen veröffentlichen. Es braucht aber noch die Informatik für praxisrelevante Anwendungen. Das ist das Ziel von dem, was wir vorgeschlagen haben."

„Ich bin ein Herzblut-Informatiker", so Wille, „der aber durchaus offen ist, mit anderen Disziplinen wie der Physik zu kooperieren. Wir versuchen, beide Disziplinen so zusammen zu bekommen, dass wir die Technologie Quantenrechner, die physikalisch dominiert ist, mit der Informatik so zu verbinden, dass wir das Beste aus beiden Welten nutzen können."

„Die Möglichkeiten, die es hier gibt, haben mich nach Linz geführt", sagt Wille, der am Wochenende nach Bremen pendelt. „Das begeistert mich bis heute am Forschungsstandort Oberösterreich." Der Preis sei auch eine Auszeichnung dafür, dass die JKU auf dem Weg zur internationalen Spitze sei. „Wir wollen ganz vorne mitspielen." Die neue Digital-Universität sei „eine große Chance für die Region".

KONTAKT
Johannes Kepler Universität Linz
LIT Secure and Correct Systems Lab
contact@lit-systems.jku.at
Altenberger Straße 69
4040 Linz, Österreich
T +43 732 2468 4739
jku.at/ lit-secure-and-correct-systems-lab

JKU LINZ INSTITUTE OF TECHNOLOGY