

IT-Sicherheit und Quantencomputing: Auszeichnung für Oberöreicher und Steirer

Utl.: Heinz Zemanek Preis 2024 für herausragende Dissertationen =

Wien (OTS) - Die Heinz Zemanek Preisträger 2024 sind der Oberöreicher Lukas Burgholzer und der Steirer Martin Schwarzl. Der Preis, zu Ehren des österreichischen Computerpioniers Heinz Zemanek, wird alle zwei Jahre von der [Österreichischen Computer Gesellschaft] (<https://ocg.at>) (OCG) für herausragende Dissertationen im Bereich der Informatik vergeben.

Das finale Hearing des [Heinz Zemanek Preis] (<https://www.ocg.at/hzp>) vor der 19-köpfigen Jury unter dem Vorsitz von Prof. Stefan Szeider (TU Wien) fand am 16. Mai 2024 in der OCG statt. Burgholzer und Schwarzl konnten sich gegen fünf weitere Kandidat*innen mit herausragenden Informatik-Dissertationen durchsetzen. Burgholzers Arbeit beschäftigt sich mit der Entwicklung von Software für Quantencomputing (JKU, Betreuer: RobertWille). Schwarzl schrieb über Seitenkanal-Angriffe aus der Ferne und deren Prävention (TU Graz, Betreuer: Daniel Gruss).

„Alle Finalist*innen für den Heinz Zemanek Preis haben sich bereits gegen eine sehr starke Konkurrenz durchgesetzt. Die Auswahl der Preisträger*innen ist alle zwei Jahre eine Herausforderung. Die vielköpfige Jury ist einerseits notwendig, um die breite Expertise der informatischen Fachbereiche abzudecken, andererseits gibt es immer viel Diskussionsstoff. Auch dieses Jahr konnten wir uns schließlich auf zwei Arbeiten einigen, die sich durch exzellente wissenschaftliche Leistung sowie durch hohe Relevanz für aktuelle und zukünftige Technologien auszeichnen“, kommentiert Stefan Szeider die Entscheidung.

OCG Präsident Wilfried Seyruck betont den motivierenden Wert von wissenschaftlichen Preisen: "Wissenschaftliche Auszeichnungen erhöhen die Sichtbarkeit und erleichtern die Vernetzung in der Scientific Community, sie fördern das Vertrauen in die eigenen Fähigkeiten und inspirieren zu weiterem Engagement und Forschung. Zudem bieten diese Preise finanzielle Unterstützung und können Türen für wertvolle Karrierechancen öffnen, weil sie Lebensläufe bereichern."

Zwtl.: Burgholzer:

DesignAutomationToolsandSoftwareforQuantencomputing

„Quantencomputer werden Realität!“, eröffnete der Oberösterreicher Lukas Burgholzer seine Präsentation. „Die Leistungsfähigkeit entsprechender Maschinen wird immer besser, sodass bereits in wenigen Jahren praktisch relevante Anwendungen mit ihnen möglich sein könnten. Allerdings bringt die leistungsfähigste Maschine nichts, wenn Endanwender*innen sie nicht benutzen können. Und hier liegt derzeit noch ein großes Problem: Quantencomputer werden von Physiker*innen entwickelt, die Anwendungspotentiale liegen aber in Gebieten wie z.B. der Chemie, dem Finanzwesen oder der Physik. Software kann diese ‚Welten‘ miteinander verknüpfen“.

In seiner Dissertation am Institut für Integrierte Schaltungen der Johannes Kepler Universität Linz (unter Leitung von Prof. Dr. Robert Wille) entwickelte der 30-Jährige zahlreiche Methoden, welche es erlauben Quantenanwendungen zu simulieren, sie effizient und automatisch auf echten Quantencomputern ausführen zu können und schließlich auch die Korrektheit des gesamten Prozesses verifizieren zu können. Die resultierenden Software-Tools wurden dabei nicht nur open-source der Community zugänglich gemacht (z.B. als Teil des Munich Quantum Toolkits; siehe [<https://mqt.readthedocs.io/en/latest/>] (<https://mqt.readthedocs.io/en/latest/>)), sondern werden auch in Workflows von Firmen wie IBM oder großen Quantencomputing-Initiativen wie dem Munich Quantum Valley eingesetzt.

Zwtl.: Durch Zufall zum Quantencomputing

Dass sich Burgholzer mit Software für Quantencomputing beschäftigen würde, war dabei nicht von Anfang an klar. Er begann sein Studium in Linz im Studiengang Technische Mathematik ohne je eine Zeile Programmcode geschrieben zu haben. Schnell wurde aber sein Interesse am Programmieren geweckt, was ihn dazu veranlasste, parallel zum Masterstudium in der Industriemathematik auch den Bachelorstudiengang in Informatik zu beginnen. Im Rahmen seiner Bachelorarbeit lernte er schließlich seinen späteren Doktorvater, Prof. Dr. Robert Wille, kennen und bekam erstmals Einblick in das Gebiet des Quantencomputings. Diese Erfahrung löste eine solche Begeisterung aus, dass Burgholzer nach seinem Informatikabschluss direkt eine Promotionsstelle bei Prof. Wille antrat, um weiter an diesem Thema zu forschen. Knapp vier Jahre später ist Burgholzer eine

der führenden Persönlichkeiten auf dem Gebiet der Softwareentwicklung für Quantencomputing und setzt seine Forschung am Lehrstuhl für Design Automation der Technischen Universität München als Postdoktorand fort.

Zwtl.: Schwarzl: Remote Side-Channel Attacks and Defenses

Martin Schwarzls Arbeit an der TU Graz, im Rahmen der CoreSec Group unter der Leitung von GI-Dissertationspreisträger Daniel Gruss, beschäftigt sich mit der Untersuchung neuer netzwerkbasierter Seitenkanalattacken und effizienter Gegenmaßnahmen. „Der Schutz privater Daten im Internet hat höchste Priorität. Allerdings sind moderne Hardware und Software auf eine hohe Performanz optimiert. Abhängig von den Nutzereingaben hinterlassen diese Optimierungen messbare Seiteneffekte, die sich in der Zeit, im Stromverbrauch oder in der elektromagnetischen Strahlung des Geräts widerspiegeln. Seitenkanalattacken nutzen diese Seiteneffekte aus, um sensible Daten von Systemen abzugreifen“, erklärt der Steirer das Phänomen.

Zwtl.: Neue Angreifer-Szenarien im Internet

Auch Cloud-Anbieter stehen vor der neuen Herausforderung, sich auch vor netzwerkbasierter Seitenkanalattacken zu schützen. Schwarzl präsentiert in seiner Forschung neu entdeckte Attacken, die es ermöglichen, ohne direkten Zugang zum Gerät, sensitive Daten von Zielsystemen auszulesen. Das bedeutet, dass jeder betroffene Server sogar aus dem Internet attackiert werden kann. Die*der Angreifer*in benötigt hierfür lediglich eine stabile Netzwerkverbindung zum Server. Die Folgen der Angriffe sind gravierend, denn mit diesen Attacken könnte z. B. eine unentdeckte Industriespionage in großem Maße durchgeführt werden. Mit netzwerkbasierter Seitenkanalattacken ist es möglich, Kund*innendaten von Webseiten ohne Berechtigung auszulesen. Die Angriffe zielen auf Datenbanksysteme, Webanwendungen, Browser und virtuelle Maschinen ab, die weitläufig in der Praxis genutzt werden. Zusätzlich zu den beschriebenen Angriffen werden neue Techniken gezeigt, um Sicherheitsmechanismen von Betriebssystemen zu umgehen.

Des Weiteren wird in Schwarzls Dissertation eine neue Sicherheitsmaßnahme gegen Spectre-Attacken im lokalen und Cloud-Szenario vorgestellt. „In Kollaboration mit dem US-Konzern Cloudflare haben wir eine effiziente Gegenmaßnahme für netzwerkbasierter Spectre-Attacken entwickelt. Diese Gegenmaßnahme

erkennt bösartige Angreifer*innen und isoliert diese", so der 29-Jährige. Die publizierten Arbeiten der Dissertation erhielten mediale Aufmerksamkeit in Fachzeitschriften und wurden auf renommierten internationalen akademischen und wirtschaftlichen Konferenzen präsentiert.

Zwtl.: Leidenschaft für Ethical Hacking

Schon in der Schulzeit faszinierte Schwarzl das Cracking und Modding von Computerspielen. Er nahm an einer Reihe an Hacking-Challenges teil und erweiterte stetig sein Wissen über Sicherheitslücken von Soft- und Hardware, so dass er während seines Studiums auch österreichische Firmen in IT-Sicherheitsfragen beriet. Im Jahr 2018 trat erstmals die Seitenkanalattacke Spectre auf, die es ermöglichte, sämtliche Daten wie Passwörter aus Systemen auszulesen. Die CoreSec-Gruppe der TU Graz mit Michael Schwarz, Daniel Gruss und Moritz Lipp hatte wesentlich zur Entdeckung beigetragen und Martin Schwarzl für eine wissenschaftliche Laufbahn motiviert.

~

Rückfragehinweis:

Österreichische Computer Gesellschaft (OCG)
Irina Scheitz
Kommunikation
066488674860
scheitz@ocg.at
www.ocg.at

~

Digitale Pressemappe: <http://www.ots.at/pressemappe/439/aom>

*** OTS-ORIGINALTEXT PRESSEAUSSENDUNG UNTER AUSSCHLIESSLICHER
INHALTLICHER VERANTWORTUNG DES AUSENDERS - WWW.OTS.AT ***

OTS0039 2024-06-07/09:54

070954 Jun 24

Link zur Aussendung:

https://www.ots.at/presseaussendung/OTS_20240607_OTS0039