Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Wednesday, February 14th, 2024 - 10:15, SQUARE 11-2091 (Arena)

Committing Authenticated Encryption: NIST Finalists and Generic Composition

Patrick Struck

Patrick Struck did his PhD at Technical University of Darmstadt under the supervision of Juliane Krämer. Afterwards he was PostDoc at University of Regensburg and is now at University of Konstanz, where he leads the Cryptography and Cyber Security group. His research interest are provable security of cryptographic algorithms and, in particular, post-quantum cryptography and authenticated encryption.

The talk focuses on committing authenticated encryption. Simply speaking, a committing authenticated encryption scheme comes with the guarantee that it is hard to find two contexts (keys K/K', nonces N/N', and associated data A/A') which decrypt the same ciphertext C. We analyze the finalists of the NIST lightweight cryptography standardization process and show that only 3 out of 10 finalists are committing authenticated encryption scheme while we give attacks against the others. We then analyze the generic composition paradigm and show that Encrypt-and-MAC is committing whereas Encrypt-then-MAC is not.

From insight to impact.

Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Thursday, February 15th, 2024 - 13:30, SQUARE 11-2091 (Arena)

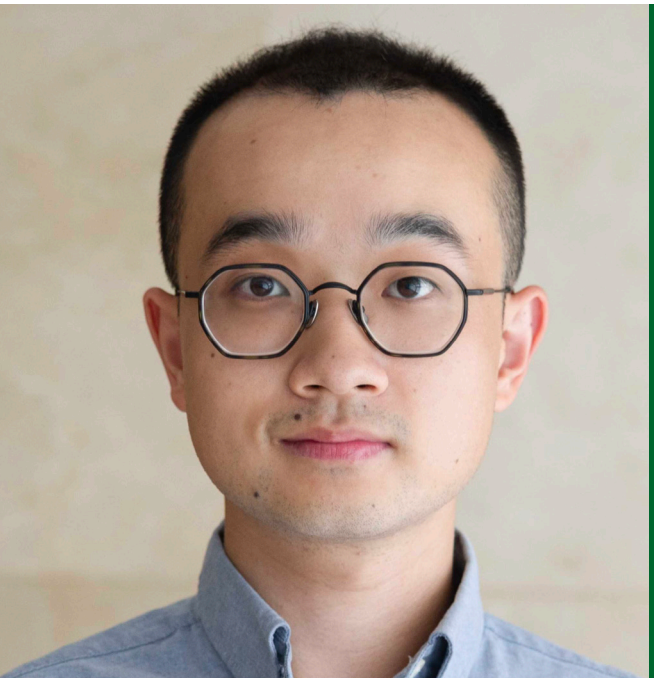
Solidifying the Foundations for Software Verification

Zhang Chengyu

Software verification lies at the heart of building reliable software. Consequently, the dependability of verification tools is pivotal for software reliability. It is thus critical to develop effective methodologies and practical tools to help solidify the foundational verification tools. In this talk, I will present effective techniques and extensive effort for uncovering numerous bugs in modern SMT solvers and software verification tools. The talk will focus on both the theoretical and practical challenges of solidifying the verification foundations and introduce the latest advances.

Chengyu Zhang is a postdoctoral fellow in the Department of Computer Science at ETH Zurich. He is passionate about fundamental and practical innovations for improving the reliability of software. His research spans programming languages, software engineering, and formal methods. He served as an artifact evaluation co-chair of OSDI and ATC 2022, a reviewer for TOSEM and TSE, and a program committee member of ASE 2024, ECOOP 2023, and ESEC/FSE 2023 with a Distinguished Reviewer Award. His work has been recognized by a PLDI Distinguished Paper Award and a Google Open Source Peer Bonus, and supported by an Amazon Research Award and CCF-ANT Research Award.

From insight to impact.



Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Thursday, February 29th, 2024 - 16:15, SQUARE 11-2091 (Arena)

Mine, Assess, Enhance - Computational Support for Improving Argumentative Writing Skills in Higher Education

Christina Niklaus

In today's world, effective academic writing is paramount for students' success, as it enables them to articulate their understanding, engage in critical thinking, and communicate their ideas effectively. Argumentative writing support plays a vital role in cultivating these skills, empowering students to construct convincing arguments, critically evaluate diverse perspectives, and develop their own positions. Traditionally, argumentative writing support has relied heavily on human feedback from experienced educators. However, providing consistent, high-quality feedback is resource-intensive and does not scale to large-scale online education settings. Thus, there is a growing need to develop computational approaches to automate this task. This talk explores the emerging role of computational methods in augmenting human feedback and enhancing the effectiveness of argumentative writing support. We will delve into techniques for automatically assessing writing quality, identifying areas for improvement, and generating targeted feedback to provide students with comprehensive and personalized guidance.

Christina Niklaus is an Assistant Professor for Computer Science with focus on Databases and Data Engineering at the University of St.Gallen. Her research primarily centers on Data Science and Natural Language Processing, dealing with the analysis of large-scale textual data. In particular, she is interested in developing intelligent systems that are capable of automatically processing and understanding the meaning of information at scale. To achieve this goal, Christina's work concentrates on the extraction of knowledge from big textual data, resulting in a structured machine-readable representation. Christina studied Computer Science at the University of Bamberg, ENSEEIHT Toulouse, and the University of Passau. In 2016, Christina joined the Data Science and Natural Language Processing Group at the University of Passau as a research assistant. She subsequently moved to the University of St.Gallen in 2019. In 2022, she completed her Ph.D. with distinction at the University of Passau.

From insight to impact.

Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Tuesday, March 12th, 2024 - 14:15, Room 01-307

Unlocking Developer Productivity at Microsoft: Every Second Counts

Brian Houck

Unlocking the productive potential of engineer teams is about more than just software tools, it's about shifting the focus back to the driving force behind it all: the developers themselves. Join us for a discussion on how Microsoft uses a blend of research techniques to build an understanding of the human factors that impact developer productivity, and what they do about it.

We'll share the practical tips and strategies that their teams use to measurably improve their developer experiences. Which metrics does Microsoft use to measure their developer experiences (and why)? What is the impact of meetings on productivity? How does the day of the week impact code throughput? How much does dealing with bureaucratic toil make developers want to quit? What is the #1 most frequently cited workplace challenge amongst developers across the entire industry? Learn the answers to these questions and more!

As a Productivity Engineer at Microsoft, Brian specializes in elevating the wellbeing and productivity of internal engineering teams. His mission goes beyond mere metrics; it's about humanizing the workplace. Through his research into tooling, processes, and cultural dynamics, Brian has successfully implemented strategies that not only boost efficiency, but also foster a collaborative and satisfying work environment.

Brian takes human-centered approach, focusing on improving the day-to-day experiences for developers. This philosophy has led to multiple company-wide initiatives and policies that have measurably enhanced team dynamics and productivity. His passion lies in continually exploring innovative ways to improve our work culture, ensuring that every individual feels valued, motivated and productive.

From insight to impact.

Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Thursday, March 14th, 2024 - 16:15, SQUARE 11-2091 (Arena)

When Business Processes meet the Internet of Things: Will they have a happy future?

Ronny Seiger

Business Process Management (BPM) research and development focused its attention on automating and optimizing digital processes of enterprises over the past decades. With the advent of the Internet of Things (IoT), these digital processes might also be enabled to interact with the physical world, including smart devices and humans--all together forming smart Cyber-physical Systems (CPS). In this talk, we will have a look at software engineering-focused research projects to adopt BPM technologies for developing CPS. We will discuss the integration of large numbers of sensors, actuators including robots, and humans into CPS processes. We also investigate how to make these processes resilient against external interruptions and failures and how to apply process mining in this context. Industry-driven use cases from the domains of smart manufacturing, smart healthcare, and smart homes will be used to showcase the new concepts and technologies. Throughout the talk, we will discuss challenges and mutual benefits of bringing the worlds of BPM and IoT closer together.

Ronny Seiger received his PhD in computer science from Technische Universität Dresden, Germany in 2018. Since 2022 he is an Assistant Professor for Computer Science with focus on Software Engineering Methods and Techniques at the University of St.Gallen. His experience includes research and industry projects on software engineering and software architectures, Business Process Management (BPM) technologies, Cyber-physical Systems (CPS) and Internet of Things (IoT), as well as robotics and distributed systems. His main research is at the intersection of BPM, software engineering, and IoT with a focus on applying BPM technologies for analyzing and automating processes in Cyber-physical systems.

From insight to impact.

Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Thursday, April 11th, 2024 - 16:15, SQUARE 11-2091 (Arena)

The Recruiting Process Unveiled: Strategies to Crack the Code and Succeed in Your Application

Anne Gebhardt & Fabiana Decortes

This talk provides practical strategies for students looking to enhance their application success. Our speakers draw on real-world insights to examine the critical components prior and within the recruiting process. The objective is to offer a clear understanding and provide a framework for students to navigate the complexities inherent in job applications. Additionally, this talk serves as an opportunity to address any questions you may have always wanted to ask an HR expert.

From insight to impact.

Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Wednesday, May 15th, 2024 - 16:15, Tellstrasse 2, Room: 58-022

Fundamental Challenges and Opportunities for the ICT-Industry

Stephan Schnez

The ICT (Information and Communication Technologies) industry faces some fundamental challenges because certain engineering guardrails which have been guiding the industry for the last decades approach physical and/or economic limits. In my presentation, I will outline these and explain why these not only lead to performance challenges but also raise concerns in terms of the sustainability of the ICT industry and its services. I will then present some approaches of how to potentially overcome these challenges and what opportunities these present – for both researchers in academia and in the industry, as well as start-ups and established companies.

Stephan Schnez joined Huawei's Central Research Institute in 2019 where he is responsible for technology strategy and planning, based in Zurich. His core interests are related to quantum technologies and optics/photonics for novel approaches in communication and computing technologies. Before that, he spent more than seven years as a researcher and a project manager at ABB with a focus on energy storage and renewable energy systems.
Stephan Schnez studied physics at the University of Heidelberg (Germany) and at the University of Manchester (UK) and received his Ph.D. in experimental physics from ETH Zurich (Switzerland) with a thesis on quantum electronics and graphene nanostructures. He has been a lecturer on "Energy and Digitalization" at the University of Freiburg (Germany) since 2017.

From insight to impact.

Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Thursday, May 16th, 2024 - 16:15, SQUARE 11-2091 (Arena)

Human-Centered Security: Focusing on the human in IT security and privacy research

Verena Zimmermann

The role of the human for security and privacy is highly relevant, e.g., when it comes to secure authentication, communication, or the detection of phishing e-mails. As such, the human is an important element in today's security-critical systems. Yet, humans have often been considered a weak link as it is finally them who create weak passwords or click on phishing links. Measures to prevent these insecure behaviours include automation, training or the creation of policies. But why do users behave insecurely in the first place? And how can we change that?

This talk aims to shine light on the psychological aspects of IT security and privacy that help to understand human security behaviour and provide examples from different application areas. Furthermore, it will outline a mindset that suggests viewing the human as a potential solution with regard to security and privacy rather than only viewing the human as a weak link to be dealt with.

Verena Zimmermann is Assistant Professor (Tenure Track) for Security, Privacy and Society at ETH Zürich. Her research interests comprise the Human Aspects of Safety, IT Security and Privacy. After her studies in psychology, she has completed her dissertation in the interdisciplinary research area of Usable Security at TU Darmstadt in Germany. Within the research group Work and Engineering Psychology and ATHENE, the German National Center for Applied Cybersecurity, she worked on several security-related research projects. Her dissertation with the title «From the Quest to Replace Passwords towards Supporting Secure and Usable Password Creation" received dissertation awards by the German Association for Data Protection and Data Security e.V. (GDD) and the Ernst-Ludwigs-Hochschulgesellschaft.

From insight to impact.