Informatik-Kolloquium

Der Fachbereich Informatik der Johannes Kepler Universität Linz[1] lädt in Zusammenarbeit mit der Österreichischen Gesellschaft für Informatik (ÖGI) zu folgendem Vortrag ein:

Vijay Ganesh (MIT, USA)

Solvers for Software Reliability and Security

28. Juli 2010, 15.00 Uhr
Johannes Kepler Universität Linz, HS 12

Abstract:
The task of building reliable and secure software remains one of the most important and challenging issues in computer science. In recent years, there has been rapid progress in the scalability and effectiveness of software reliability tools. A key reason for this success is the dramatic improvement in the speed of constraint solvers over the last decade. Constraint solvers are essential components of most software reliability tools, whether they are based on formal methods, program analysis, testing or synthesis. My research on constraint solvers has directly contributed to this trend of increasing solver efficiency and expressive power, thus advancing the state-of-the-art in software reliability research.

In this talk, I will present two solvers that I have designed and implemented, namely, STP and HAMPI. I will talk about the techniques that enable STP and HAMPI to scale, and also some theoretical results. I will also talk about the contexts and applications where each solver is best suited.

STP is a solver for the theory of bit-vectors and arrays. STP was one of the first constraint solvers to enable an exciting new testing technique called Dynamic Systematic Testing (aka Concolic Testing). STP-enabled concolic testers have been used to find hundreds of previously unknown bugs in Unix utilities, OS kernels, media players, and commercial software, some with approximately a million lines of code.

[1] Der Fachbereich (http://informatik.jku.at) besteht aus folgenden Instituten:
Anwendungsorientierte Wissensverarbeitung (FAW), Bioinformatik, Computational Perception, Computergrafik, Computer-Architektur, Formale Modelle und Verifikation, Informationsverarbeitung und Mikroprozessortechnik (FIM), Integrierte Schaltungen, „integriert studieren", Pervasive Computing, Systemsoftware, Systems Engineering und Automation, Telekooperation

ÖGI-Sekretariat, z.Hd. Frau Inge Naderer
Johannes Kepler Universität Linz, Altenberger Straße 69, A-4040 Linz, Austria
oegi@fim.uni-linz.ac.at http://oegi.ocg.at

Next, I will describe HAMPI, a solver for a rich theory of equality over bounded string variables, bounded regular expressions, and context-free grammars. Constraints in this theory are generated by analysis of string-manipulating programs. HAMPI has been used to find many unknown SQL injection vulnerabilities in applications with more than 100,000 lines of PHP code using static and dynamic analysis.

Finally, I will conclude my talk with two future research programs. First, I will discuss how faster solvers can enable qualitatively novel approaches to software reliability. Second, I will discuss how we can go from specific solver techniques to solver design paradigms for rich logics.

Biography:
Vijay Ganesh, MIT (http://people.csail.mit.edu/vganesh)

Dr. Vijay Ganesh is a Research Scientist at MIT since 2007. He completed his PhD in computer science from Stanford University in September 2007. He also has an MS in computer science from Stanford University, and a Bachelor of Technology degree from College of Engineering, Trivandrum, India.

His primary research interests are constraint solvers (SAT/SMT solvers), and their applications to software reliability, computer security and biology. He works on both the theory and practice of constraint solvers. He has designed and implemented several constraint solvers, most notably, STP and HAMPI. STP was one of the first solvers to enable an exciting new testing technique called systematic dynamic testing (or concolic testing). STP has been used in more than 100 research projects relating to software reliability and computer security. More recently he designed another solver, HAMPI, aimed at solving string constraints generated by the analysis of PHP, JavaScript and Perl programs. His paper on HAMPI won the ACM Distinguished Paper Award (2009). STP was the co-winner of the SMTCOMP competition for bit-vector solvers in 2006. Dr. Ganesh has also done research in automated software testing, in particular, whitebox fuzzing.

Univ.-Prof. Dr. Armin Biere
Institut für formale Modelle und Verifikation

[1] Der Fachbereich (http://informatik.jku.at) besteht aus folgenden Instituten:
Anwendungsorientierte Wissensverarbeitung (FAW), Bioinformatik, Computational Perception, Computergrafik, Computer-Architektur, Formale Modelle und Verifikation, Informationsverarbeitung und Mikroprozessortechnik (FIM), Integrierte Schaltungen, „integriert studieren", Pervasive Computing, Systemsoftware, Systems Engineering und Automation, Telekooperation