JOHANNES KEPLER UNIVERSITY LINZ | JKU

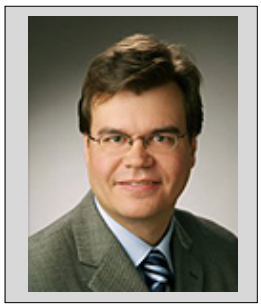
Univ.-Prof. Dr. Alois FERSCHA
Fachbereich Informatik

Altenberger Straße 69
A-4040 Linz
Tel.: +43 (732) 2468 4762
Fax: +43 (732) 2468 4765

ferscha@pervasive.jku.at
http://www.pervasive.jku.at

Dr. Florian Kerschbaum

SAP Applied Research



Ein optimierender Compiler für sichere Berechnungen

An Optimizing Compiler for Secure Computations

Sichere Berechnungen können vielfältig für Datenschutz und Datensicherheit in Netzwerken eingesetzt werden. Sie können unternehmensübergreifende Probleme in Lieferketten oder datenschutzfreundliche Analysen implementieren, so dass die Schutzziele aller Parteien gewährleistet werden. Die Entwicklung solcher Protokolle für sichere Berechnungen bleibt äußerst schwierig. Domänenspezifische Sprachen können dem Programmierer zwar helfen effizienter und effektiver zu implementieren, aber bestehende Compiler erzeugen schlechtere Ergebnisse als manuell erzeugter Code. Programmanalyse und automatisierte Optimierung können dieses Problem lösen. Basierend auf realen Beispielen zeigen wir generische Methoden zur Optimierung sicherer Berechnungen, die auch in einem Compiler automatisch durchgeführt werden können.

Secure multi-party computations have many applications in privacy and data security of networks. They can solve cross-organizational problems in supply chain management or privacy-enhanced data analysis, such that the protection needs of the parties are respected. Nevertheless, the development of protocols for multi-party computation is extremely complex. Domain-specific languages can help the programmer to implement more efficiently and effectively. However, compilers currently produce worse results than manually generated protocols. Program analysis and automated optimization can remedy this problem. Based on real-world examples we show general techniques for optimizing secure computations which can be automatically implemented in a compiler.

Zeit: Mittwoch, 6. Februar 2013, 10:00 Uhr

Ort: Johannes Kepler Universität Linz

Informatik-Gebäude, SCP 3, HS 19

Kurzbiographie

Florian Kerschbaum is a research expert in the security program of SAP Applied Research in Karlsruhe, Germany. In the academic year 2011/12 he was on leave as the temporary professor (Lehrstuhlvertreter) for the chair of privacy and data security at Dresden University of Technology. Before SAP he has worked for Siemens, the San Francisco-based startup Arxan, Intel and Digital Equipment in the job functions of project manager, software architect, and developer. He holds a Ph.D. in computer science from the Karlsruhe Institute of Technology, a master's degree from Purdue University, and a bachelor's degree from Berufsakademie Mannheim.