informatik
Studium mit Zukunft

JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

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:

DI Tobias Jeske
TU Hamburg-Harburg

A Compiler for Optimised Zero-Knowledge Proofs of Knowledge

Dienstag, 23. 11. 2010, 13.45 Uhr
Johannes Kepler Universität, T642

Abstract: In electronic environments in which user actions can be easily traced there is a natural human want for privacy. A typical example of this is an application in which a user uses a mobile phone as a virtual door key. In this scenario it is easily possible to log the time whenever a valid user enters the door. In some practical environments even this (theoretical) possibility of privacy breach prevents the usage of electronic door access systems.

A Zero-knowledge proof of knowledge is a powerful cryptographic building block which can solve privacy issues in protocols.

What is problematic is that this privacy protection is paid by a significant increase of protocol complexity. It becomes quite cumbersome to efficiently implement such proofs by hand, especially for non-experts in cryptography. In addition, the processing speed drastically decreases by using zero-knowledge proofs of knowledge. This is a serious problem, especially on mobile devices where the processor speed is much lower than on desktop computers.

In our department we are working on finding solutions for these two problems. Firstly, we simplified the development of privacy-preserving protocols by using a high-level language. The developer specifies the protocol on the basis of building blocks, which hide the internal cryptographic details. Secondly, our compiler supports the possibility to optimize the proofs and outputs code for various platforms (e.g. desktop computers, mobile phones) to increase performance.

o. Univ.-Prof. Dr. Jörg R. Mühlbacher
Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM)

[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