INFORMATIK-KOLLOQUIUM
AB Programmiersprachen und Übersetzer
Institut für Computersprachen

Einladung

zum Informatik-Kolloquium des
AB Programmiersprachen und Übersetzer am
Donnerstag, den 27. Oktober 2016, um 15:00 Uhr s.t.
Hörsaal HS4, Freihaus, Wiedner Hauptstr. 8, Turm B (gelber Bereich), 2. Stock.

Es spricht

Prof. Dr. Alejandro Russo

Chalmers University of Technology, Gothenburg, Sweden

über

Preserving Privacy with Monads

In an all-connected society, users consciously (or unconsciously) value their privacy. Even skeptical people will recognize its importance; if they do not, ask them to unlock their smartphone and hand it out to someone else — they will most probably refuse! Users want to have control on how their data gets disseminated, specially today when private information gets handled by software with heterogeneous trustworthiness — consider, for example, the various smartphones apps with access to user' private photos, messages, and contacts that exists today. Unfortunately, current software practices are insufficient to protect privacy: users who wish to benefit from software functionality are often forced to grant access to their private data with no guarantees how it gets handled. The key insight to guarantee privacy is not about granting or denying access to private data, but ensuring that information only flows into the appropriated places.

Information-Flow Control (IFC) is a research area dedicated to protect privacy of data. Based on programming languages techniques, IFC scrutinizes source code to track how data of different sensitivity levels (e.g., public or private) flows within a program, where alarms are raised when privacy might be at stake. IFC tools often provide specially designed compilers to build privacy-preserving apps. Rather than building a compiler from scratch (a major task on its own), Haskell plays a unique privileged role in this scenario: it can provide IFC security via libraries. As long as developers program against the libraries' API, code is secure by construction. This talk shows how to build such libraries by specially designing monads capable to restrict the propagation of private data. The presentation explores the different techniques used in a wide range of libraries, namely LIO, MAC, and HLIO, where IFC is enforced dynamically (in the form of an execution monitor), statically (by leveraging Haskell's type-system), and as a combination of both.

Biographie: Alejandro Russo is an associate professor at Chalmers University of Technology working on the intersection of functional languages, security, and systems. He is the recipient of a Google Research Awards and several grants from the Swedish research agencies Vetenskapsrdet, STINT, and Barbro Osher foundation. Internationally, Prof. Russo worked on prestigious research institutions like Stanford University, where he was appointed visiting associate professor. His research ranges from foundational aspects of security to developing tools to secure software written in Haskell, Python, and JavaScript. (http://www.cse.chalmers.se/~russo/)

Zu diesem Vortrag lädt der *Arbeitsbereich für Programmiersprachen und Übersetzer am Institut für Computersprachen* herzlich ein.
Tee: 14:30 Uhr in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte).