

EINLADUNG

Zeit: Donnerstag, 16.11.2006, 16.30 Uhr

Ort: AH I, Ahornstr. 55

Referent: Prof. Dr. Martin Hofmann (LMU München)

Titel: From Type Systems to Program Logic

Abstract:

Type Systems allow one to automatically ascertain that a given program enjoys a particular desired property, e.g. not to call undefined methods, not to violate a certain security or resource policy, etc.

A program logic (in the sense of e.g. Hoare Logic) allows one to ascertain arbitrary properties of programs as long as they are expressible in the program logic. A formalisation of a program logic in a theorem prover like Coq allows one to use proofs in a program logic as principally unforgeable certificates of program properties, known as "foundational proof-carrying code" (FPCC). However, program logics are in general not automatic, in fact undecidable in most cases.

We propose to automatically produce proofs in a formalised program logic from a successful type-based analysis of a program. In this way, such analyses can be used to produce certificates in the sense of FPCC.

I will illustrate this approach with two examples: a type system for bounded heap allocation, and a type system for secure information flow. Both exhibit subtle fine points: how can we express in program logic properties of non-terminating programs (e.g. one that keeps allocating memory)? How can we express in program logic properties that involve two runs of a program instead of one as is required to express security of information flow?

This work has been done in the context of the EU funded projects MOBIUS (IST-15905) and MRG (IST-33149) whose support is herewith gratefully acknowledged.

Es laden ein, die Dozenten der Informatik