

Einladung

zum Informatik-Kolloquium des
AB Programmiersprachen und Übersetzer am
Donnerstag, den 26. Feber 2009, um 15:00 Uhr s.t.
in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte)

Es spricht

Dr. Bernhard Scholz

The University of Sydney, NSW, Australia

über

Static Program Analysis for Bug and Security Vulnerability Checking of Systems Code

Abstract: A security vulnerability is a software bug that can be exploited by an external attacker. Security vulnerabilities expose a major threat for operating systems and programs that are executed with higher privileges, as an attacker can gain total control over a computer system by exploiting vulnerabilities. Even in a rigid software development process, bugs are introduced that may result in severe security vulnerabilities. This is especially true for large legacy systems written in C and C++.

Manual code inspections are the predominant approach to find security vulnerabilities. These inspections are time-consuming, repetitive and tedious. They can never be complete or time-effective, particularly in light of the large code-bases of software systems these days (thousands to millions of lines of code). Static bug checking tools that rely on sound program analyses, promise a solution to this problem. However, designing and implementing precise and scalable program analyses is still a big challenge.

In this talk I will report on my work conducted at the Sun Microsystems Laboratories in 2007/08. I will give an overview of our new project, Parfait; a static, layered program analysis framework for checking bugs in C systems code. The framework is coupled with security domain knowledge to better cater for security vulnerabilities in large systems code. The framework was designed to provide better precision of bugs (less false positives), be scalable (produce results for millions of lines of code in a run-time efficient manner), and support security vulnerability analysis.

Biography: Bernhard Scholz is senior lecturer in Computer Science at the University of Sydney. He has previously served on the Vienna University of Technology and the University of Vienna. He has also held a visiting professorship at the University of Victoria, BC, Canada and at the Sun Microsystems Laboratories. Before pursuing an academic career, Bernhard Scholz worked in industry as programmer and analyst at Baring Asset Management, London, UK. (<http://www.cs.usyd.edu.au/~scholz/>)

Zu diesem Vortrag lädt der *Arbeitsbereich für Programmiersprachen und Übersetzer am Institut für Computersprachen* herzlich ein.

Tee: 14:15 Uhr in der Bibliothek E185.1, Argentinierstr. 8, 4. Stock (Mitte).