INFORMATIK-KOLLOQUIUM
AB Programmiersprachen und Übersetzer
Institut für Computersprachen

Einladung

zum Informatik-Kolloquium des
AB Programmiersprachen und Übersetzer am
Montag, den 28. Februar 2011, um 15 Uhr c.t.
im Hörsaal EI 5 Hochenegg, Elektrotechnik, Gußhausstraße 25-29 (Altbau), 2. Stock

Es spricht

Prof. Dr. Michael Franz

University of California, Irvine, CA, USA

über

Recent Advances in Compiler Research - Firefox's TraceMonkey and Beyond

Common to practically all compilers built over the past 50 years has been the concept of the "control flow graph", a model of a program that a compiler builds and then traverses while generating target code. Even just-in-time and embedded compilers use such control flow graphs, although they tend to make the unit of compilation smaller than traditional batch compilers (e.g., one method at a time rather than one class at a time).

Trace Compilation, to which we have made significant contributions, represents a radical departure from this long established convention. A novel intermediate representation, the Trace Tree, is constructed lazily on-demand while the program is simultaneously executed, incrementally compiled, and optimized. The advantage of this technique is that the compiler doesn't expend any resources on parts of the program that are not frequently executed; traditional compilers construct control-flow graphs for unimportant and even for unreachable parts of a program and need to prune such graphs later.

Our specific approach to trace compilation is now in the process of being adopted widely across and beyond academia. Working with the Mozilla foundation, we incorporated our technique into the Firefox browser, starting with version 3.5. By incorporating our invention, Mozilla was able to raise Firefox's JavaScript performance by a surprising factor of 7. Our Trace Compilation technique is now being used daily by several hundred million users around the globe. Other groups of researchers that are now using trace compilation include Oracle, Adobe, Google, and Microsoft, and we are collaborating with several of these projects.

In a second project, we are investigating compiler-generated software diversity as a defense mechanism against software attacks. Our solution is centered on an "App Store" containing a diversification engine (a "multicompiler") that automatically generates a unique version of every program each time that a downloader requests it. All the different versions of the same program behave in exactly the same way from the perspective of the end-user, but they implement their functionality in subtly different ways. As a result, any specific attack will succeed only on a small fraction of targets. An attacker would require a large number of different attacks and would have no way of knowing a priori which specific attack will succeed on which specific target. Equally importantly, our approach makes it much more difficult for an attacker to generate attack vectors by way of reverse engineering of security patches.

Biography: Prof. Michael Franz is a Professor of Computer Science in UCI's Donald Bren School of Information and Computer Sciences, a Professor of Electrical Engineering and Computer Science (by courtesy) in UCI's Henry Samueli School of Engineering, and the director of UCI's Secure Systems and Software Laboratory. He is currently also a visiting Professor of Informatics at ETH Zurich, the Swiss Federal Institute of Technology, from which he previously received the Dr. sc. techn. (advisor: Niklaus Wirth) and the Dipl. Informatik-Ing. ETH degrees. (http://www.ics.uci.edu/∼franz/)

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).