

FACULTY CANDIDATE SPRING 2007 SEMINAR

April 12, 2007

PGH 563

11:00 AM

Host: Dr. Chapman

Dr. Dinghao Wu

Microsoft, Inc.

Title: Software Correctness, Verification, and Mathematical Proof in Real World

As software engineering technology advances, software scale and complexity grow even faster today. This puts urgent demands on theory and tools that can improve programmer productivity and software quality. In this talk, I'll demonstrate how various program analysis and verification techniques can be applied to achieve this goal.

Specifically, I'll present the KISS transformation technique that leverages sequential program analysis tools to verify concurrency properties such as free of race conditions. KISS issues no false alarms and overcomes the exponential factor in concurrent analysis algorithms. KISS has been implemented in a tool shipped worldwide with Windows Vista to verify device driver properties.

I'll also briefly present my experience on two other formal software verification projects and show that, with advances of automated theorem proving and program analysis techniques, formal software verification, the holy grail of software practice, is a reachable goal at this time, despite that significant research efforts are still necessary to achieve this.

Bio:

Dinghao Wu got his Ph.D. in computer science from Princeton University in 2005. Since then he has been a research engineer in the Center for Software Excellence at Microsoft. His research interests include programming languages and compilers, software engineering, software verification and program analysis, formal methods, and language-based security. He has worked on projects, such as foundational proof-carrying code, software model checking, and concurrency error detection via sequential program analysis, to improve program reliability & security, and programmer productivity. Since joining Microsoft, he has been working on various program analyses, verification, and testing tools and applying them to large programs, such as Windows Vista, which has over 50 million lines of code.