NJIT

Department of Computer Science

Verification for Working Developers

Martin Kellogg
University of Washington

Hosted by Iulian Neamtiu

Date: Friday, February 11, 2022
Coffee: 10:45 AM – 11:00 AM
Seminar: 11:00 AM – 12:00 PM
Location: GITC 4402 (4th Floor Seminar Lecture Hall)
WebEx: https://njit.webex.com/njit/j.php?MTID=m606bbe93cf260f724bb10ff120f39438

https://cs.njit.edu/seminars

Abstract:

This talk discusses practical verification for real software developers. Making verification practical requires two big changes: verification tools must solve hard problems while still being simple enough for every developer to use and understand, and developers must be convinced to actually use them. This talk will discuss an example of work that has made progress on each of these two fronts.

First, accumulation typestate automata are a novel special-case of typestate automata that can be soundly checked without the need to run an expensive, whole-program alias analysis - making these "accumulation analyses" fast enough to run every time that software is compiled. Using accumulation analyses, we can detect and prevent serious bugs, including security vulnerabilities and resource leaks, in orders of magnitude less time than traditional approaches.

Second, compliance certification is a problem that many software developers already need to worry about. We have shown how verification is an excellent tool to solve some of the compliance problems that were previously checked via manual audits. Developers prefer this application of verification to the state-of-the-practice; that is, they were convinced of its value.

Bio:

Martin Kellogg is finishing up his PhD at the University of Washington in the PLSE group, advised by Michael Ernst. His work makes verification practical for real software engineers. He has published in venues including ICSE, ESEC/FSE, and ASE. He collaborates extensively with industry, especially with the AWS Automated Reasoning Group.