Automated Software Testing for the 21st Century

Patrice Godefroid
Principal Researcher, Microsoft Research

During the last decade, research on automating software testing using program analysis has experienced quite a resurgence. A key technical challenge is automatic code-driven test generation: given a program with a set of input parameters, how to automatically generate a set of input values that, upon execution, will exercise as many program statements as possible. Although automating test generation using program analysis is an old idea, practical tools have only started to emerge over the last few years. This recent progress was enabled by advances in dynamic test generation, automated constraint solving, and modern computers' increasing computational power. All these tools combine techniques from static program analysis (symbolic execution), dynamic analysis (testing and runtime instrumentation), model checking (systematic state-space exploration), and automated constraint solving (SMT solvers). However, they target different application domains and include other original techniques. This talk will present an overview of recent advances on automatic test generation, and discuss applications of these techniques in the software industry.

About the Speaker

Dr. Godefroid's research interests include program (mostly software) specification, analysis, testing and verification. He is probably best known for his pioneering work on partial-order reduction for model checking concurrent systems, for his work on VeriSoft, the first software model checker for mainstream programming languages such as C and C++, for his work on 3-valued model checking with may/must abstractions for sound program verification and falsification, and for his work on automatic test generation with DART. More recently, he co-developed SAGE, the first whitebox fuzzer for security testing, which was credited to have found roughly one third of all the security vulnerabilities discovered by file fuzzing during the development of Microsoft's Windows 7.

He received a B.S. degree in Electrical Engineering (Computer Science elective) and a Ph.D. degree in Computer Science from the University of Liege, Belgium, in 1989 and 1994 respectively. From 1994 to 2006, he worked at Bell Laboratories (part of Lucent Technologies), where he was promoted to "distinguished member of technical staff" in 2001.