ISSTAC -- Integrated Symbolic Execution for Space-Time Analysis of Code

Corina Pasareanu  NASA Ames Research Center Senior Systems Scientist SV Campus

Thursday, December 8th  4:30 EST Hamerschlag Hall 1107
1:30 PST Room 118 B23

Abstract:
Cybersecurity is one of the most critical challenges facing the computing discipline. Vulnerabilities that result from space-time usage of programs are especially hard to detect and defend against, since they are due to algorithmic behavior of programs rather than implementation errors. ISSTAC aims to build an integrated approach that provides both qualitative and quantitative reasoning for space-time analysis of Java programs. The approach is based on symbolic execution, a systematic program analysis technique which efficiently explores multiple program behaviors all at once, by manipulating symbolic path conditions collected over program paths. I will describe two critical ISSTAC components: The Worst-Case Analysis uses heuristics to efficiently search for algorithmic complexity vulnerabilities, and The Side-Channel Analysis uses quantitative information flow analysis to detect and quantify information leakage. The analyses are parameterized with respect to cost models for space-time consumption. Further both analyses produce actual test inputs that expose the vulnerabilities.

Bio:
Corina is performing research in software engineering at NASA Ames, in the Robust Software Engineering group. She is employed by Carnegie Mellon University, at the Silicon Valley campus. She is affiliated with CMU’s Cylab and also holds a courtesy appointment with CMU Electrical & Computer Engineering. At Ames she is developing and extending Symbolic PathFinder, a symbolic execution tool for Java bytecode. At CMU she is the PI of several research projects covering symbolic execution, compositional verification and security. She is/was Program/General Chair for several conferences including: ACM Sigsoft Symposium on Foundations on Software Engineering (FSE 2018), International Conference on Computer Aided Verification (CAV 2015), International Symposium on Software Testing and Analysis (ISSTA 2014), International Conference on Automated Software Engineering (ASE 2011). She is the recipient of several paper awards including an ACM Impact Paper Award (2010) and the ICSE 2010 Most Influential Paper Award. She is currently Associate Editor for the IEEE Transactions on Software Engineering (TSE) journal.

SEMINAR NOTES: (REFRESHMENTS SERVED AT 4:30 PM)