



Fall 2009 CIS Distinguished Lecture

Path-Sensitive Analysis for Security Flaws

Mary Lou Soffa
(University of Virginia)

10am-11pm, Thursday, December 3
TECH Center 111

Abstract: Despite increasing efforts in detecting and managing software security flaws, the number of security attacks is still rising every year. As software becomes more complex, security flaws are more easily introduced into a software system and more difficult to eliminate. In this talk, I present our research on the development of a framework for detecting and managing security flaws. The key idea is to develop static analysis tools to determine program paths that lead to various types of vulnerabilities. I describe a path-sensitive analysis that can handle a number of software vulnerabilities, including buffer overflow, integer errors, violation of safety properties, and flaws that can cause denial of service. The novelty of the work is that we address the scalability of path-sensitive analysis using a demand-driven algorithm, to provide both precision and scalability. We first develop a general vulnerability model to easily specify new types of vulnerabilities or application specific security flaws to guide our demand-driven analysis. Our analysis starts at the program points where vulnerability could possibly occur. A partial reversal of the dataflow analysis is performed to determine the types of paths with regard to feasibility and vulnerability, including the severity of the vulnerability. With this technique, we are able to more precisely identify vulnerabilities. Our experiments show that we are able to detect and classify more vulnerabilities than current tools and the analysis scales to above 1 million lines of code. We also provide information about the vulnerability to help with the user understand and remove its root cause.

Bio: Mary Lou Soffa is the Owen T. Cheatham Professor of Sciences and Department Chair of the Computer Science Department at the University of Virginia. From 1977 to 2004, she was a Professor of Computer Science at the University of Pittsburgh and also served as the Dean of Graduate Studies in the College of Arts and Sciences from 1991 to 1996. Her research interests include software tools for debugging and testing programs, virtual execution environments, optimizing compilers, and program analysis. She has published over 150 papers in journals and conferences. Her papers have received a number of best paper awards as well a designation of one of the 40 most influential papers in 20 years to appear in the Programming Language Design and Implementation Conference. She has directed 24 Ph.D. students to completion, half of whom are women. She also directed over 50 M.S. students, with half being women. Soffa received the Nico Habermann Award in 2006 for outstanding contributions toward increasing the numbers and successes of underrepresented members in the computing research community. In 1999, she received the Presidential Award for Excellence in Science, Mathematics and Engineering Mentoring. She was elected an ACM Fellow in 1999 and selected as a Girl Scout Woman of Distinction in 2003. She served for ten years on the Board of the Computing Research Association (CRA) and continues as a member of CRA-W, the committee on the status of women in computer science and engineering of the CRA. She co-founded the CRA-W Graduate Cohort Program and the CRA-W Cohort for Associate Professors. She has served on the Executive Committees of both ACM SIGSOFT and SIGPLAN as well as conference chair, program chair or program committee member of many conferences. Currently, she is an ACM Council Member-at-Large and serves on the ACM Publications Board.

Refreshments will be served!