Path-Sensitive Analysis for Security Flaws

Mary Lou Soffa
University of Virginia
soffa@virginia.edu

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.