Title

Detecting Security Vulnerabilities via Static Analysis

Team Members

Robert Zajac
Graham Mosley

Summary of Proposed Project

Security flaws in programs are a huge source of vulnerabilities in larger software systems. In this project we analyze the extent to which we can detect these flaws using static analysis tools in spite of the different features of different programming languages. In particular we will compare and contrast the Bandit tool for Python, Flawfinder for C/C++, and Xanitizer for Java (among others potentially) by running these tools on real programs and analyzing what kind of vulnerabilities they are able to find.

Additionally, we will compare these tools to general static analysis tools like the clang static analyzer to see the extent to which specializing static analysis for finding security flaws actually makes a difference in results. One of the biggest challenges we will face is finding non-trivial programs which have meaningful security flaws that these tools can find.