

Framework for Targeted Tracing of Software Execution with Debug Symbols

Short Description

Reasoning about software quality, potential bugs, and its dynamic behavior (e.g., execution hot spots) is not an easy task. Existing approaches for doing so predominantly rely on static analysis. However, static analysis is inherently imprecise. The goal of this project is to design and implement a framework for targeted tracing of software execution that considers relating of executed instructions with debug symbols in order to provide more information for the execution trace analysis.

The basic technology for tracing will be based on DynamoRIO binary instrumentation tool. It will be necessary to enable DynamoRIO to extract debug symbols according to executed instructions. Furthermore, it will be necessary to create an external execution engine of this framework in a language more suitable for doing complex analysis (e.g., Python or Java). The framework should be configurable with options of targeting specific functions and threads for execution tracing, with the possibility of an online configuration (i.e., during the execution). The framework should write the execution trace in a configurable form of JSON files.