Parker Harris cs4240
Ashvin Warrier

Project 3 Final Report

In this project, we generate the ICFG graph from the input using the SVF library. This library breaks the IR into different blocks and edges, connecting all of the different function calls together. Reachability analysis using the SVF library is simply using different graph algorithms in order to figure out all the possible paths from one point to another. We start by traversing through the graph and finding the call block node for src and sink function calls. Once we have these, we pass them into a depth-first search algorithm that traverses the graph, looking for any non-looping paths that start from src and end at sink. The depth-first algorithm works recursively by keeping track of any visited blocks as well as the current path. Each edge on the vertex calls the function with the destination of the edge. If the destination of any edge is already in the visited list, then we know we have found a loop. Therefore, in this case, we end that potential path. Once the destination of a vertex is found the be the sink that was passed into this recursive function, we can add that path to the set of solutions. By the end of this, we have all paths that have successfully traversed from src to sink and can be considered reachable.