Finding Previously-Discovered Bugs in Software Applications (2 Years)

Problem Statement
A software bug can exist in different software applications as a consequence of software code reuse. In the absence of source code and debugging symbols, it is challenging to determine if a bug occurs in different applications.

Objective
We would like to:
1. Study the different techniques and their limitations for finding occurrences of a previously-discovered bug in software applications.
2. And evaluate the different techniques to determine their effectiveness.

Conceptually, this may involve extracting a signature from a discovered bug and developing an algorithm to effectively analyse a set of binary executables from applications for the presence of the signature. The challenges include describing what a suitable signature might be and designing a robust algorithm that can withstand syntactical variations due to the compilation process. Ideally, it should also be proved that the bug is reachable, since non-reachable bugs need not be patched.

Deliverables
A software tool to analyze a set of binary executables for occurrences of a known bug, with a clear user manual.

Tool Inputs
a. A binary executable with a known bug
b. A set of binary executables

Tool Outputs
a. A listing of a subset of the input binary executables that contain the bug

References