Software Engineering Seminar

Combining Fuzzing and Symbolic Execution

Description

Fuzzing is a great technique to, for example, discover and reproduce software system vulnerabilities. However, there exist problems with finding test inputs for complex checks (e.g., string equality checks). Symbolic Execution, on the other hand, is theoretically able to exhaustively check every program branch, but practically struggles to do so, due to the path explosion problem. Recent approaches propose to combine fuzzing techniques and symbolic execution to effectively tackle the problems that both techniques have on their own.

The student should examine and discuss the approaches given in the papers and compare them to each other and to similar existing techniques.

References


Contacts

Simon Heiden (heiden@informatik.hu-berlin.de)
Software Engineering Group
Institut für Informatik
Humboldt-Universität zu Berlin