Software Engineering Seminar

Directed Fuzzing Techniques

Description

Beyond the more general fuzzing techniques that are, among others, used to generate tests with a certain amount of coverage, there exist techniques to direct fuzzers with the goal to execute specific program parts (recent changes, critical system calls, ...). A recent approach is described in [1].

The student is to examine the approach described in the given paper and compare it to similar existing directed fuzzing techniques.

References

[1] Marcel Böhme, Van-Thuan Pham, Manh-Dung Nguyen, and Abhik Roychoudhury. Directed greybox fuzzing. In *Proceedings of the 24th ACM Conference on Computer and Communications Security*, CCS, pages 1–16, 2017.

Contacts

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