Software Engineering Seminar

Effective Bug Detection using Fuzzing

Description

Fuzzing can be used to effectively find bugs (vulnerabilities,crashes,...) in software systems. One major problem is, e.g., the execution of branches that are protected by so-called ”*magic byte comparisons*” (e.g., string equality comparison). Previous techniques struggle to efficiently find the correct input values to execute these branches. Recently, a program-state based fuzzing technique has been proposed that supposedly deals with this problem at the minor cost of some execution speed [1].

The student is to examine and to discuss the technique given in the provided paper, to evaluate its capabilities and to compare it to other fuzzing approaches.

References

[1] Yuekang Li, Bihuan Chen, Mahinthan Chandramohan, Shang-Wei Lin, Yang Liu, and Alwen Tiu. Steelix: program-state based binary fuzzing. In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, ESEC/FSE 2017, Paderborn, Germany, September 4-8, 2017*, pages 627–637, 2017.

Contacts

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