Software Engineering Seminar

Stateful Fuzzing

Description

Fuzzing is a powerful testing technique, which is based on heuristic-driven random generation of test inputs. Introduced by Miller et al. [3], fuzzing recently gained a tremendous research and industry hype for the identification of security vulnerabilities. Often such vulnerabilities are hidden in specific states of the program under test, and hence, a specific sequence of interaction is necessary to identify them.

Stateful fuzzing is a relatively new research topic, which tries to tackle this problem. For example protocol fuzzing [1, 2] is one type of stateful fuzzing, which focuses on finding bugs in predefined sequences of interactions. Recent work like [4] by Catherine Zuo, applies stateful fuzzing for the testing of file systems behavior.

The goal of this seminar topic is to collect the current research directions in stateful fuzzing. Therefore, it is is necessary to perform an initial literature analysis based on the provided publications. The student should examine and discuss the approaches given in the papers and compare them to each other and to similar existing techniques. Additionally, the student is asked to provide a critical discussion of the current research directions, which should also include an outlook for possible future work.

References

[1] Greg Banks, Marco Cova, Viktoria Felmetsger, Kevin Almeroth, Richard Kemmerer, and Giovanni Vigna. Snooze: Toward a stateful network protocol fuzzer. In Sokratis K. Katsikas, Javier López, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *Information Security*, pages 343–358, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[2] R. Ma, Daguang Wang, C. Hu, W. Ji, and Jingfeng Xue. Test data generation for stateful network protocol fuzzing using a rule-based state machine. *Tsinghua Science and Technology*, 21(3):352–360, June 2016.

[3] Barton P. Miller, Louis Fredriksen, and Bryan So. An empirical study of the reliability of unix utilities. *Commun. ACM*, 33(12):32–44, December 1990.

[4] Catherine Zuo. *SibylFuzzer: stateful fuzzing for file systems*. PhD thesis, Massachusetts Institute of Technology, 2017.

Contacts

Yannic Noller (`noller@informatik.hu-berlin.de`)
Software Engineering Group
Institut für Informatik
Humboldt-Universität zu Berlin