Software Engineering Seminar

Anti-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. Fuzzing is actually used as a testing technique, which identifies dangerous inputs that allow the developers to fix security vulnerabilities. On the other hand, fuzzing can also be used to find vulnerabilities, with the goal to exploit them.

In order to mitigate this risk, the fuzzing research community recently coined the term *anti-fuzzing* as a defense strategy. Very recent works by Güler et al. [1] and Jung et al. [2] try to protect binary executables against the analysis of fuzzing or hybrid fuzzing testing techniques.

The goal of this seminar topic is to collect the current research directions in anti-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] Emre Güler, Cornelius Aschermann, Ali Abbasi, and Thorsten Holz. Antifuzz: Impeding fuzzing audits of binary executables. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1931–1947, Santa Clara, CA, August 2019. USENIX Association.

[2] Jinho Jung, Hong Hu, David Solodukhin, Daniel Pagan, Kyu Hyung Lee, and Taesoo Kim. Fuzzification: Anti-fuzzing techniques. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1913–1930, Santa Clara, CA, August 2019. USENIX Association.

[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.

Contacts

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