Software Engineering Seminar

Analysis of Neural Networks with Fuzzing

Description

Fuzzing is a testing technique, which is based on heuristic-driven random generation of test inputs. It was recently used in the detection of security vulnerabilities, in which it showed great success. Another current trend is the usage of neural networks in all kind of software systems, although the testing of neural networks is still poorly investigated. Recent work like TensorFuzz by Odena and Goodfellow [2] and DeepHunter by Xie et al. [3] apply fuzzing on the analysis of neural networks. There are also more focused approaches like DLFuzz by Guo et al. [1], which uses differential testing to expose incorrect behavior of the neural network.

The goal of this seminar topic is to collect the current research directions in fuzzing for neural networks. Therefore, it 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


Contacts

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