Bachelor Thesis Topic

Evaluating Fuzzing for Model-Driven Software Engineering (MDSE) Tools

Motivation and Background

Fuzzing for fuzz testing [1] is an established technique that aims to discover unexpected program behavior (e.g., bugs, security vulnerabilities, or crashes) by feeding automatically generated data into a program under test. However, the application of fuzzing to test Model-Driven Software Engineering (MDSE) tools is still limited due to the difficulty of existing fuzzers to provide syntactically and semantically valid input models that conform to a given meta-model. Recently, MoFuzz [2] has been introduced, a fuzzer suite that is able to efficiently produce input models to fuzz MDSE tools using various model generation and mutation strategies. Although MoFuzz has been evaluated on a set of generic MDSE tools based on the UML2 meta-model [3], it is unclear how well it performs on tools that take as input instance models of alternative meta-models (e.g., BPMN2 [4]).

Goals

The goal of this thesis is to extent the original evaluation of MoFuzz to include additional MDSE tools that are based on a variety of meta-models beyond UML2 and compare the results against the baseline techniques.

Description of the Task

The specific tasks are:

- Understand the overall approach of MoFuzz and familiarize with its implementation [5].
- Prepare experiments: Collect benchmark subjects and input meta-models, write test drivers.
- Perform experimental evaluation and comparison against baseline techniques.

Research Type

Theoretical Aspects:	**∗∗∗
Industrial Relevance:	***∗∗
Implementation	*****

Prerequisite

The student should be enrolled in the bachelor of computer science program, and has completed the required course modules to start a bachelor thesis.

Skills required

Programming skills in Java, understanding of, or willingness to learn, the software engineering methods (like fuzz testing) and tools (e.g., the Eclipse Modeling Framework) needed for the project.

Contacts

Hoang Lam Nguyen (nguyehoa@informatik.hu-berlin.de)
Software Engineering Group, Institut für Informatik, Humboldt-Universität zu Berlin

References

[1] Manès, Valentin Jean Marie, et al. "The art, science, and engineering of fuzzing: A survey." IEEE Transactions on Software Engineering (2019).
[2] Nguyen, Hoang Lam, Nebras Nassar, Timo Kehrer, and Lars Grunske. “MoFuzz: A Fuzzer Suite for Testing Model-Driven Software Engineering Tools”. 2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE). 2020.
[3] Object Management Group (OMG). 2017. Unified Modeling Language (UML) 2.5.1 specification. https://www.omg.org/spec/UML
[4] Object Management Group (OMG). 2014. Business Process Model and Notation (BPMN) 2.0.2 specification. https://www.omg.org/spec/BPMN
[5] MoFuzz tool. https://github.com/hub-se/MoFuzz