

Bachelor Thesis

GARBAGE COLLECTOR FUZZING FOR GRAALVM NATIVE IMAGE

DI Thomas Schrott

I. for System Software

T: +43 732 2468 4372

M: thomas.schrott@jku.at

Student: Aleksandar Stojanović
k12411325

Secretary:

Karin Gusenbauer

T: +43 732 2468 4342

M: karin.gusenbauer@jku.at

Advisor: DI Thomas Schrott

Defects in a garbage collector implementation can lead to subtle issues like memory corruption that are not noticed until some time after they initially occurred. Therefore, these defects are hard to find, reproduce or debug.

The goal of this project is to create an event-based garbage collector fuzzer, similar to [1], for GraalVM Native Image [2, 3]. The fuzzer generates random events (e.g., allocate an object, write a reference, perform a collection, ...). These events get executed within Native Image. When the execution fails, the event sequence can be used for debugging and fixing bugs.

GraalVM Native Image is primarily implemented in Java, so Java is also the main programming language that will be used in this project. Additionally, it is necessary to work with pointers and native memory.

Goals of this thesis are:

- Executing events within Native Image using the Serial GC and with limited side-effects on the VM
- Implementing a small number of events, necessary for fuzzing (e.g., object allocation, writing references, garbage collection, ...)
- Implementing/using a fuzzer for event creation

Non-goals of this thesis are:

- Fuzzing of other garbage collectors
- Implementing “all” possible events
- Multi-threaded fuzzing support
- Automatic test case reduction

Modalities

The progress of the project should be discussed at least every two weeks with the advisor. A time schedule and a milestone plan must be set up within the first 3 weeks. It should be continuously refined and monitored to make sure that the thesis will be compiled in time. The final version of the thesis must be submitted by March 31, 2027.

-
- [1] G. Polito, P. Tesone, N. Palumbo, S. Ducasse and J. Privat. 2023. Heap Fuzzing: Automatic Garbage Collection Testing with Expert-Guided Random Events:
<https://doi.org/10.1109/ICST57152.2023.00019>
- [2] <https://github.com/oracle/graal>
- [3] <https://www.graalvm.org/jdk25/reference-manual/native-image/>