Replication of Entropic

Entropic as published in ESEC/FSE'20 under the title “Boosting Fuzzer Efficiency: An Information Theoretic Perspective” by Marcel Böhme (marcel.boehme@acm.org, mboehme), Valentin Manès (valentinmanes@outlook.fr, Jiliac), and Sang Kil Cha (sangkilc@kaist.ac.kr, sangkilc), was independently evaluated by the developers of LibFuzzer @ Google and invited for integration into mainline LibFuzzer. Moreover, our main results were independently replicated within the Fuzzer benchmarking platform Fuzzbench. The FuzzBench project is described at https://google.github.io/fuzzbench/ and a report of recent results can be found at https://www.fuzzbench.com/reports/sample/index.html. A technical description of Entropic can be found in the paper available on the first author's website: https://mboehme.github.io/paper/FSE20.Entropy.pdf

Entropic is a source-based grey-box fuzzer based on LibFuzzer. It boosts performance by changing how weights are assigned to the seeds in the corpus. Seeds revealing more ‘‘information’’ about globally rare features are assigned a higher weight. Entropic performances, in terms of bug finding and coverage, show that an efficient fuzzer maximizes information. In the paper, Entropic was evaluated with subjects gathered in the Fuzzer Test Suite repository and subjects from the OSS-Fuzz repository.

FuzzBench is a service that evaluates fuzzers on a wide variety of real-world benchmarks. The goal of FuzzBench is to rigorously evaluate fuzzing research and make fuzzing research easier for the community to adopt. FuzzBench evaluation subjects are mostly the same as in the Fuzzer Test Suite. This benchmark does not include the OSS-Fuzz subjects used for Entropic evaluation. In Entropic evaluation, the OSS-Fuzz evaluation intended to do a large scale validation of its performance. On the other hand, all subjects in the Fuzzer Test Suite contain bugs to be discovered. And it balances the number of subjects to make evaluation doable in relatively small amounts of time (and given finite resources).

The original paper based its evaluation on a well-established benchmark. This plus the decision of basing Entropic implementation on a famous and well-maintained project such as LibFuzzer, greatly helped in the replication of our results.