ObfusEval: Evaluating Reliability of Obfuscating Transformations

Tetsuya Kitaoka †, Yuichiro Kanzaki ‡, Takashi Ishio †, Kazumasa Shimari †, and Kenichi Matsumoto †

† Nara Institute of Science and Technology, ‡ National Institute of Technology, Kumamoto College

1. Motivation

Many code obfuscation tools have been proposed so far.

Code obfuscation tools

Tigress — C

Obfuscator-LLVM — LLVM

ProGuard — Java

Obfuscating transformation is the conversion method implemented in these tools.

Can they appropriately obfuscate programs without causing defects?

Reliability

We are developing a tool to evaluate the reliability of obfuscating transformation.

2. Proposed Metrics

Test Pass Rate:

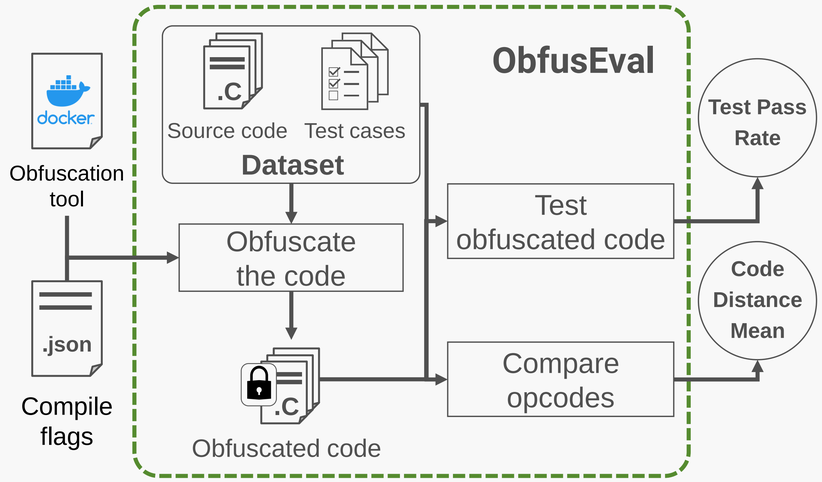
How an obfuscated program keeps the original functionality.

Code Distance Mean:

How an obfuscated program is changed from the original one.

3. Tool Overview

Our tool measures these metrics of obfuscating transformation using a benchmark dataset.



Current dataset:

- Searching
- Sorting
- etc.

40 programs

Achieved 80〜100% line coverage

Test cases

4. How to Calculate the Metrics

Code Distance Mean:

Longest Common Substrings

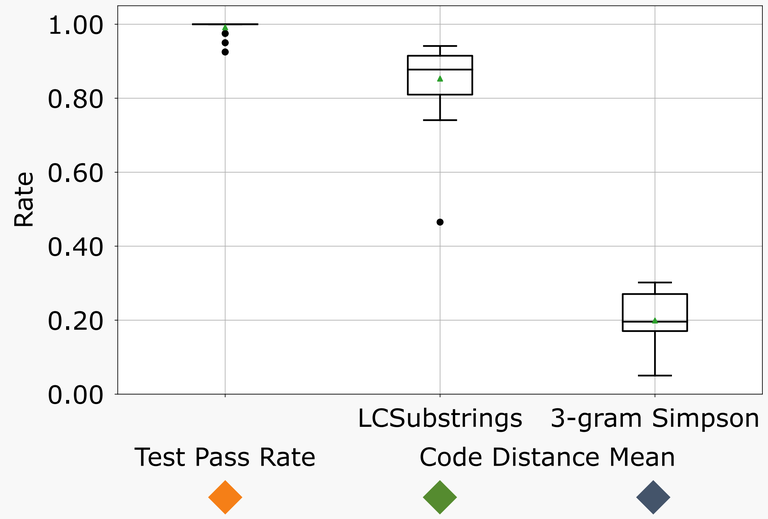
The more instructions are transformed on the whole, the higher the score is.

3-gram Simpson

The more different 3-grams of instructions are from the original ones, the higher the score is.

5. Case Study

Our tool measured these metrics of existing obfuscating transformations.



- Some transformations broke some programs.
- All transformations changed the instructions.
- 3-grams of code fragments are similar to the original ones.

6. Current Status

- We investigate why the Test Pass Rate of some transformations did not reach 1.00.
- We need to set criteria for a better benchmark dataset.

Acknowledgments

This work was supported by JSPSKAKENHI Grant Numbers JP22K11986, JP22K21279, JP20H05706, and JP19K11916.