《自动化测试 2022》大作业要求

—— Mutation Testing & Fuzzing 方向要求

文献综述选题

1、变异测试

（1）变异测试优化技术综述

（2）变异测试应用综述

2、模糊测试

（1）模糊测试技术中种子调度技术综述

（2）定向模糊测试技术综述

（3）基于生成的模糊测试技术综述

（4）内核模糊测试技术综述

工具/流程实现选题

通用要求&前期准备

1、提交内容

工具代码、脚本代码（流程/分析） — Shell，C/C++，Python，R

过程报告：一些实现、配置和流程上的坑，配置的汇总、框架/流程设计 > 选题描述、项目结构、环境/实验设置（使用的 Subject，格式参考我给的表格；硬件配置等）、Fuzzing 配置、构建流程（引导）、框架设计、结果分析

运行结果：数据整理后得到的图、表 — 一系列 PDF，CSV，xlsx 等

提交格式：所有数据整理成 Zip 提交

2、备选 Fuzzers：AFL（Base）

A 组：AFL, AFL++, AFLGo, AFLFast, AFLSmart, Mopt, FairFuzz, EcoFuzz, Neuzz, MTFuzz

B 组：Vuzzer, Angora, LibFuzzer, Entropic

AFL 仓库：https://github.com/google/AFL

AFL 博客/文档：https://afl-1.readthedocs.io/en/latest/

3、实验对象（Subjects）

真实项目：https://docs.qq.com/sheet/DZGtod3FBZ2lXZHhS?tab=BB08J2，尽量下载最新版本

DARPA CGC dataset：https://github.com/CyberGrandChallenge/

LAVA-M：Lava: Large-scale automated vulnerability addition，S&P'16

4、C/C++项目的构建：gcc、clang、make、cmake、autoconf……

选题 1：基于变异测试的模糊器评估（Fuzz-Mut）

1、选题简介

模糊测试是一种重要的软件测试技术，得到了学术界和工业界的广泛关注。近年来，关于模糊测试的研究不断涌现。实现模糊测试的程序称为模糊器（Fuzzer）。面对如此众多的 Fuzzer，如何准确、有效地评估 Fuzzer 的性能成了一项值得关注的难题。**本选题从变异杀死的角度对 Fuzzer 进行评估。**

2、选题要求

编写脚本，利用变异测试工具重新运行模糊测试的产生的测试输入，从变异测试的角度（变异得分）评估 Fuzzer 的性能

工具：AFL（Fuzzer） + Mull（变异测试工具）

对象：所有 Real-world Projects

步骤：（1）利用 AFL 对实验对象进行模糊测试，产生测试输入；（2）利用 Mull 复现 AFL 产生的测试输入，记录变异杀死情况；（3）编写脚本对运行结果进行分析，绘制统计图

运行设置：（1）每个 Fuzz Campaign（$< fuzzer, subject >$）持续至少 1 小时，绘图默认按照分钟；（2）变异杀死的条件 Crash & **Differential Comparing**。实现 Differential Comparing 的小组可额外加分

3、参考资料

Mull 论文：Mull It Over: Mutation Testing Based on LLVM

Mull 文档：https://mull.readthedocs.io/en/0.19.0/

选题 2：基于覆盖率的模糊器评估（Fuzz-Cov）

1、选题简介

模糊测试是一种重要的软件测试技术，得到了学术界和工业界的广泛关注。近年来，关于模糊测试的研究不断涌现。实现模糊测试的程序称为模糊器（Fuzzer）。面对如此众多的 Fuzzer，如何准确、有效地评估 Fuzzer 的性能成了一项值得关注的难题。**本选题从代码覆盖的角度对不同 Fuzzer 进行评估。**

2、选题要求

编写脚本，利用不同 Fuzzer 对同一组待测项目进行模糊测试，之后再利用相同 gcov 复现测试输入，绘制比对统计图

工具：AFL+其他 A 组 Fuzzer*1+B 组 Fuzzer*1

对象：所有 Real-world Projects

步骤：（1）构建项目（Fuzz）、确定参数、运行不同的 Fuzzer；（2）利用 gcov 复现各种 Fuzzer 产生的测试输入、收集分支覆盖信息；（3）编写脚本对运行结果进行分析，绘制统计图，比较不同 Fuzzer 的性能

运行设置：每个 Fuzz Campaign（$< fuzzer, subject >$）持续至少 1 小时，绘图默认按照分钟

3、参考资料

Gcov 官网：https://gcc.gnu.org/onlinedocs/gcc/Gcov.html

Google Fuzzing Tutorials: https://github.com/google/fuzzing

各种 Fuzzer 的论文：Neuzz，MTFuzz，Angora

综述参考

[1] Mutation Testing Advances: An Analysis and Survey

[2] Fuzzing: A Survey for Roadmap, CSUR'22

[3] The Art, Science, and Engineering of Fuzzing: A Survey, TSE'19

联系方式

钱瑞祥，**qrx_at@163.com**，qianrx@smail.nju.edu.cn

关于大作业的问题建议大家集中发 163 邮箱，学校邮箱需要处理的事情比较多，容易遗漏大家的问题！

希望大家都可以养成**先想后问**的习惯，避免低级问题！