期末报告要求-20191216 版

一．熟悉一款知名的 Fuzz 工具（70 分）

下载、安装 fuzz 工具，选择目标程序，对其进行模糊测试，之后分析 bug 种类、成因，最终形成测试实验报告。

（1） 选择 AFL 或者自选的模糊测试工具。

（2） 选择 AFL 的话，安装文档可以参考网上文档，或群里安装文档。目标程序的选择，可以参考：http://lcamtuf.coredump.cx/afl/，之 The bug-o-rama trophy case。

（3） 测试实验报告需要包括关键步骤，难点及如何解决，实验心得与总结。

二．安装 Csmith 工具（80 分）

Csmith 产生随机的且符合 C99 语法规范的 C 语言代码，对编译器进行动态和静态测试。Csmith 在其经过测试的每个工具中都发现了错误，且已发现了 400 多个以前未知的编译器错误。Csmith 生成的程序可以执行随机计算，计算其全局变量的校验和，将校验和打印到 STDOUT。

（1） 下载并安装该软件，依照文档进行安装测试，参考网址：http://embed.cs.utah.edu/csmith/

（2） 测试实验报告需要包括关键步骤，难点及如何解决，实验心得与总结。

三．AFL 源代码分析（30 分）

读懂程序码，使心法皆为我所用；摸清架构，便可轻松掌握全貌；望文生义，进而推敲函数功能；找到程序入口，再由上而下抽丝剥茧；阅读的乐趣，透过程序码认识作者。

（1） 参考文献:

https://scubsrgroup.github.io/BinaryDatabase/Fuzzing-%E5%AD%A6%E4%B9%A0%E8%B5%84%E6%BA%90%E6%B1%87%E6%80%BB.html#afl-2015

（2） 选择整个流程，或者选择重要模块和流程进行分析，以及整个过程中的收获，最后形成代码分析报告。

四．论文阅读（30 分）

针对 Fuzz 的某一项技术，或者本领域的新方法、新系统，查阅文献，对其进行归纳总结，形成论文阅读报告。

（1） 选择研究点，可参考文件“The Art, Science, and Engineering of Fuzzing: A Survey”，包含多个方面的介绍，但是不局限于以下内容 :Fuzz Testing Algorithm, Black-box Fuzzer, White-box Fuzzer，Grey-box Fuzzer, Instrumentation, Seed Selection, Seed Trimming, Model-based (Generation-based) Fuzzers, Model-less (Mutation-based) Fuzzers, Test case minimization, Maintaining a Minset。

（2） 其他推荐论文：

- ✓ 复旦白泽：https://www.jianshu.com/u/cd49be7bd6b5
- ✓ Recent Papers Related To Fuzzing：https://github.com/fengjixuchui/FuzzingPaper
- ✓ 四大安全牛会：ACM Conference on Computer and Communications Security (CCS)，IEEE Symposium on Security and Privacy (S&P)，Network and Distributed System Security Symposium (NDSS)，USENIX Security Symposium

（3） 论文阅读报告，3000 字左右。报告包括：目前存在的问题是什么，提议用什么方法，通过什么样的实验/模型来验证，结果如何，阅读心得。

说明：对上面任务，可以四选一，或者四选二，完成一个或多个报告，最后形成一个文档，以学号和姓名命名文件名，发送至邮箱：10336506@qq.com

提交截止时间：2020 年 1 月 6 日