南京邮电大学
毕 业 设 计（论 文）

题　　目　定向覆盖模糊测试工具的设计与实现

专　　业　计算机科学与技术

学生姓名　雷尚远

班级学号　B190303　B19030334

指导老师　王子元

指导单位　计算机学院、网络学院、网络空间安全学院

日期：　2023 年 3 月 x 日至 2023 年 6 月 x 日

毕业设计（论文）原创性声明

本人郑重声明：所提交的毕业设计（论文），是本人在导师指导下，独立进行研究工作所取得的成果。除文中已注明引用的内容外，本毕业设计（论文）不包含任何其他个人或集体已经发表或撰写过的作品成果。对本研究做出过重要贡献的个人和集体，均已在文中以明确方式标明并表示了谢意。

论文作者签名：

日期：　　年　　月　　日

摘　要

模糊测试（Fuzzing）是一种通过向目标系统提供非预期的输入并监视异常结果来发现软件安全漏洞的方法，是软件安全领域常用的方法之一。由于代码覆盖率与漏洞覆盖率密切相关，大多数模糊测试工具都是以代码覆盖率为导向。然而，由于大多数被覆盖测试的代码可能并不包含漏洞，这使得盲目地扩展代码覆盖率的方式在实际测试时效率较低。极端情况尤为如此。与盲目增加代码覆盖率的模糊测试不同，定向覆盖的灰盒模糊测试（DGF）将大部分时间用于检测特定目标区域（例如，易出错代码段）而不会浪费资源于不相关的部分。因此，DGF 特别适用于补丁测试、漏洞复现以及特殊漏洞检测等场景。目前，DGF 已成为一个快速发展的研究方向。基于一些先进的定向覆盖模糊测试工具的研究和相关调查，本文主要做了以下点工作：

(1) 基于现有的模糊测试工具框架 AFL（American Fuzzy Lop）以及 AFLGo 做了定向覆盖策略的设计和集成；
(2) 实现了简单的定向覆盖的模糊测试命令行工具；
(3) 针对相应的公开通用漏洞集（CVE）做了复现及定向实验对比测试。

此外本文亦通过分析工具设计以及实现过程中的局限性与不足，对于未来该方向的研究发展做出了一些展望。

关键词： 模糊测试；定向覆盖模糊测试；灰盒测试；软件安全

ABSTRACT

Fuzzing is a method of discovering software security vulnerabilities by providing unexpected inputs to a target system and monitoring for abnormal results. It is one of the commonly used methods in the field of software security. Most fuzzing tools are coverage-guided as code coverage is strongly correlated with bug coverage. However, since most covered codes may not contain bugs, blindly extending code coverage is less efficient, especially for corner cases. Unlike coverage-guided greybox fuzzing which increases code coverage in an undirected manner, directed greybox fuzzing (DGF) spends most of its time allocation on reaching specific targets (e.g., the bug-prone zone) without wasting resources stressing unrelated parts. Thus, DGF is particularly suitable for scenarios such as patch testing, bug reproduction, and special bug detection. For now, DGF has become a fast-growing research area.

Keywords: Fuzzing；Directed Greybox Fuzzing；Greybox test；Software Security

目　　录

第一章　　绪论

1986 年，南京市整体规划向南发展，决定在主城南部建设大型车站，并预留了南京南站地区的规划空间。1990 年 12 月，原中华人民共和国铁道部完成《京沪高速铁路线路方案构想报告》。京沪高铁的前期工作进展，极为缓慢，甚至搁浅停滞相当长的一段时间，铁路要在速度上与民航竞争很多人持怀疑态度。1991 年，南京南站进入早期规划阶段。

1.1 名字自己替换

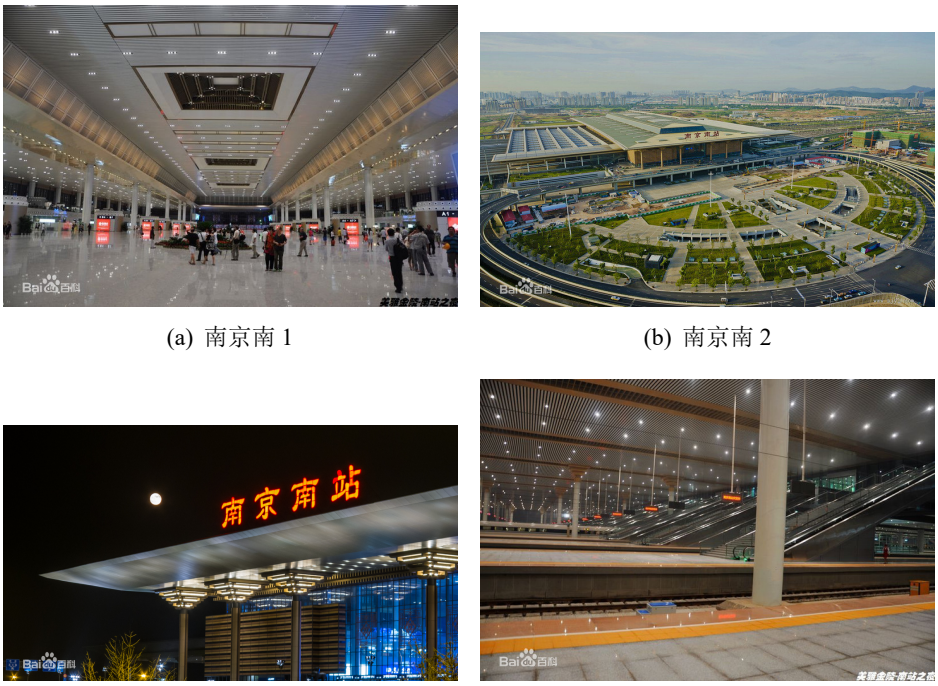
1.1.1 名字自己替换

1994 年 12 月，中国国务院批准开展京沪高速铁路预可行性研究。铁道部开展京沪高铁选线，提出“北线方案”，即从上元门地区，通过隧道过江。南京的规划部门则拿出“南线方案”，从大胜关过江。铁道部牵头，进行比选得出的结论是：两个方案在技术上都可行，主要差别在于工程造价、经济效益、运营条件等方面。江苏省和南京市要求南线方案，而铁道部看好的始终是北线方案。南京力主南线，是放长了眼光。如果从南京北部走，已经不具备扩建条件。南京火车站虽然前面是玄武湖、背面是小红山，景观很美，但是已经没有拓展空间。此外，更重要的是，在全国任何一个城市，铁路带动城市发展的效果都非常明显，南京要想进一步发展南部区域，这是个好机会。显然，高铁建在哪里，也就意味着南京今后的发展框架，是继续囿于老城狭小的空间里，还是大步向南拓展。铁道部青睐北线的理由：新线与既有线的衔接方便。清末修建的津浦铁路，即从天津到浦口；在长江南岸，之后又修建了沪宁铁路。浦口火车站、下关火车站、南京站，南京重要的火车站，向来都是位于城北。并且，当时铁道部的人都认为，南京的城市中心就在北边。另一方面，铁路的机务段、职工宿舍等都在城北，建成之后，职工上下班都方便。为了说服铁道部，南京方面列出了南线的九大优势：无论高铁从哪里走，从完善南京枢纽总体布局的角度来看，都必须建大胜关长江大桥；根据国务院批准的南京城市规划，南京城市今后将主要向东南方向发展，大胜关方案符合城市扩展方向；南面的场站位置已预留多年，有较为理想的建站条件；沿线拆迁量小，对城市干扰和环境影响小；利于形成方便的铁路——航空换乘及铁路与城市道路联结条件……不过，这些最初并没有打动铁道部，铁道部仍然坚持北线方，双方为此对峙了好几年。

1.1.2 名字自己替换

1995 年，为了促进高铁尽快上马，南京稍稍“松口”。在当年的一份紧急报告里，有这样一句话——“南北方案之争不宜过多坚持，而从规划上对北线方案提出完善意见为妥”。南京市规划局做了两手准备，针对南线、北线方案，分别做了规划控制。从 1995 年起，南京根据两个方案，开始分别严格控制沿线用地建设，同时冻结了南北两条线周围的土地。而这个具有预见性的做法，使得后来的工作变得轻松许多。

南京南站如图1.1所示。



(a) 南京南 1　　(b) 南京南 2

(c) 南京南 3　　(d) 南京南 4

图 1.1　南京南站

1.2 俄罗斯和乌克兰

本论文主要创新点与贡献如下[1]:

xxxxxxxxxxxxxx

1.3 什么是快乐星球

本文的章节结构安排如下：

xxxxxxx

第二章　　第二章了！

这是一个参考文献示例[2]

2.1 Apple M1

这是一个公式

$$y = Ax + b \tag{2-1}$$

第三章　　需要几章自己加一下！

结束语

致　谢

本论文采用 LaTeX 模版编写的，是基于南京邮电大学 2021 年理工艺教类的 Word 模板进行严格迁移编写的。本模板地址https://github.com/dhiyu/NJUPT-Bachelor感谢 imguozr（https://github.com/imguozr/NJUPThesis-Bachelor ）和 lemoxiao（https://github.com/lemoxiao/NJUPThesis-Scholar ）的工作，为本模板的形成奠定了大量的基础。

参考文献

[1] 荣洁. 俄罗斯民族性格和文化[J]. 俄罗斯中亚东欧研究, 2005(1): 66-70.

[2] Lv J, Xu M, Feng L, et al. Progressive identification of true labels for partial-label learning[C]// International Conference on Machine Learning. PMLR, 2020: 6500-6510.

附录 A

1 本科期间的学术成果发表情况

- 发表一篇 Nature
- 获得了诺贝尔奖
- 当选足球先生
- 开发了 1nm 光刻机一台

2 本科期间的获奖情况

- 设计了一块 RTX5090
- 准备移民火星
- 去太阳上面看看