

# 自动化程序修复

于4月 29, 2019由SWRhapsody发布

## Automatic patch generation

### Introduction

[1] 是个挺好的网站，推荐一下。

### Code

这个研究方向其实挺老的，查文献可以发现从上个世纪就有很多这方面的研究，但目前的发展并不如机器学习这样好，很多研究成果感觉离商业化的目标还是有点远的。

对于一个成功的自动化程序修复系统来说要完成很多指标：速度，**scalability**（不太清楚怎么翻译比较好），生成补丁的质量，生成的补丁是否和程序员手写的相似（不要可读性太差或用太多的代码完成简单的工作）等等。为了完成这些目标在过去的研究中人们提出了大量不同的解决方式。

在具体介绍各种方法前我们先来看下系统是如何定位bug以及如何判断bug是被修复与否的。

### Patch validation

目前大部分的自动化程序修复系统使用测试来验证补丁是否能够修复bug，也有程序通过crash[6] 或其他方法来判断的，这里只简单讲通过测试来验证的方法。

测试集一般分为两个，**positive testing** 和 **negative testing**。**Positive testing** 是需要修复程序要成功通过的测试，用于验证程序是否具有完整功能（避免出现打了补丁之后 bug 没了功能也受损的情况）。

**Negative testing** 是程序应该通过但无法通过的测试。

这个方法有几个缺点，因为用测试来验证程序是否修复成功容易让修复系统生成能通过测试但其实不正确的补丁，并且十分依赖测试集覆盖是否完整。举个例子

```
1 int operation a(int a, int b){
```

## SWRhapsody

6 }

假设这个算法接受两个不大于100的正整数，返回一个大于等于0的数。修复系统生成的补丁为 `return a-b+100` 这个 `+100` 确实让函数的输出达标了，但 `+100` 在算法中是错误的。

### Fault localization

错误定位是自动程序修复系统中十分重要的一个部分，能否准确的定位 `bug` 的位置将直接影响补丁的生成。错误定位目前分为好几个流派。通过 `signature` 或者 `pattern` 来识别代码中的错误（类似于静态

代码分析工具），通过测试来定位 `bug` 的位置，通过各种 `memory sanitizer` 来定位，借助插桩，`annotation` 来定位等等。

目前用的比较多的是通过测试来定位的，在测试时给每行代码一个权重，如果这行代码在 `positive testing` 中执行的次数越多其权重就越低，如果在 `negative testing` 中执行的次数越多就权重越高。权重越高意味着越可能时出错的地方。

### Patch generation

[3]

### Reference

[1] [Program Repair.org](#)

[2] ???

[3] [Automatic Software Repair: A Bibliography](#)

[4] [自动程序修复方法研究述评](#)

[5] [Genetic Programming](#)

[6] [Repairing crashes in Android apps](#)

分类: UNCATEGORIZED



## SWRhapsody

0 条评论

发表评论

名称 \*

电子邮件 \*

网站

在想些什么?

发表评论

## 近期文章

[携程Apollo YAML 反序列化](#)[CVE-2020-5410](#)[CodeQL部分源码简读](#)[服务器与网关的不一致](#)[CodeQL 部分使用记录](#)

## SWRhapsody

---

### 文章归档

[2020年8月](#)

[2020年6月](#)

[2020年5月](#)

[2020年3月](#)

[2020年1月](#)

[2019年12月](#)

[2019年11月](#)

[2019年8月](#)

[2019年7月](#)

[2019年5月](#)

[2019年4月](#)

[2019年1月](#)

[2018年11月](#)

[2018年10月](#)

[2018年9月](#)

[2018年4月](#)

[2018年3月](#)

[2018年2月](#)

[2018年1月](#)

### 分类目录

[Article Collection](#)

[Cheat Sheet](#)

## SWRhapsody

[Exploit](#)[HackTheBox](#)[Penetration Test](#)[Uncategorized](#)

## 相关文章

UNCATEGORIZED

### WordPress Social Warfare XSS

Introduction Plugin name: Social Warfare [阅读更多...](#)

UNCATEGORIZED

### Criminology

Introduction 网络安全也要学习犯罪学了吗，每次写这类文章都 [阅读更多...](#)

UNCATEGORIZED

### IOT

# SWRhapsody

---

ABOUT

Hestia |由Themelsle开发