

模糊测试



[模糊测试_下载链接1](#)

著者:[美] Michael Sutton

出版者:机械工业出版社

出版时间:2009-1

装帧:

isbn:9787111257554

《模糊测试强制性安全漏洞发掘》主要内容：模糊测试的工作原理，模糊测试相比其他安全性测试方法的关键优势，模糊测试在查找网络协议，文件格式及Web应用安全漏洞中的技术现状等。演示了自动模糊工具的用法，并给出多个说明模糊测试强大效力的历史案例。

作者介绍:

Michael Sutton是SPI Dynamics公司的安全布道师。他还是Web应用安全组织(WASC)的成员，负责其中的Web应用安全统计项目。

Adam Greene目前担任纽约某大型金融新闻公司的工程师。此前他曾经是iDefense公司的工程师，这是位于Reston, VA. 的一家智能技术公司。Adam Greene在计算机安全领域的主要研究兴趣是可靠挖掘方法、模糊测试和基于UNIX系统的审核和挖掘开发。

Pedram Amini是Tipping Point公司的安全研究和产品安全评估组的项目领导。此前他曾经是iDefence实验室的主任助手，同时也是该实验室的创建者之一。他的主要兴趣是研究逆向工程——开发自动支持工具、插件和脚本。

这三位作者经常出席Black Hat安全大会并在其中做主题报告。

目录: 译者序

译者简介

序言

前言

致谢

第一部分 背景

第1章 安全漏洞发掘方法学

1.1 白盒测试

1.1.1 源代码评审

1.1.2 工具和自动化

1.1.3 优点和缺点

1.2 黑盒测试

1.2.1 人工测试

1.2.2 自动测试或模糊测试

1.2.3 优点和缺点

1.3 灰盒测试

1.3.1 二进制审核

1.3.2 自动化的二进制审核

1.3.3 优点和缺点

1.4 小结

第2章 什么是模糊测试

2.1 模糊测试的定义

2.2 模糊测试的历史

2.3 模糊测试阶段

2.4 模糊测试的局限性和期望

2.4.1 访问控制缺陷

2.4.2 设计逻辑不良

2.4.3 后门

2.4.4 内存破坏

2.4.5 多阶段安全漏洞

2.5 小结

第3章 模糊测试方法和模糊器类型

- 3.1模糊测试方法
- 3.1.1预先生成测试用例
- 3.1.2随机方法
- 3.1.3协议变异人工测试
- 3.1.4变异或强制性测试
- 3.1.5自动协议生成测试

- 3.2模糊器类型
- 3.2.1本地模糊器
- 3.2.2远程模糊器
- 3.2.3内存模糊器
- 3.2.4模糊器框架

3.3小结

第4章 数据表示和分析

- 4.1什么是协议
- 4.2协议域
- 4.3简单文本协议
- 4.4二进制协议
- 4.5网络协议
- 4.6文件格式
- 4.7常见的协议元素
- 4.7.1名字-值对
- 4.7.2块标识符
- 4.7.3块长度
- 4.7.4校验和
- 4.8小结

第5章 有效模糊测试的需求

- 5.1可重现性和文档记录
- 5.2可重用性
- 5.3过程状态和过程深度
- 5.4跟踪、代码覆盖和度量
- 5.5错误检测
- 5.6资源约束
- 5.7小结

第二部 分目标和自动化

第6章 自动化测试合测试数据生成

- 6.1自动化测试的价值
- 6.2有用的工具和库
- 6.2.1ETHERREAL／WIRESHARK
- 6.2.2LIBDASM和LIBDISASM
- 6.2.3LIBNET／LIBNETNT
- 6.2.4LIBPCAP
- 6.2.5METRO PACKET LIBRARY
- 6.2.6PTRACE
- 6.2.7PYTHON EXTENSIONS
- 6.3编程语言的选择
- 6.4测试数据生成和模糊启发式
- 6.4.1整型值
- 6.4.2字符串重复
- 6.4.3字段分隔符
- 6.4.4格式化字符串
- 6.4.5字符翻译
- 6.4.6目录遍历
- 6.4.7命令注入
- 6.5小结

第7章 环境变量和参数的模糊测试

7.1本地化模糊测试介绍

7.1.1命令行参数

7.1.2环境变量

7.2本地化模糊测试准则

7.3寻找目标程序

7.4本地化模糊测试方法

7.5枚举环境变量

7.6自动化的环境变量测试

7.7检测问题

7.8小结

第8章 环境变量和参数的模糊测试自动化

8.1iFUZZ本地化模糊器的特性

8.2iFUZZ的开发

8.3iFUZZ的开发语言

8.4实例研究

8.5益处和改进的余地

8.6小结

第9章 Web应用程序和服务器的模糊测试

9.1什么是Web应用程序模糊测试

9.2目标应用

9.3测试方法

9.3.1建立目标环境

9.3.2输入

9.4漏洞

9.5异常检测

9.6小结

第10章 Web应用程序和服务器的模糊测试：自动化

10.1 Web应用模糊器

10.2WebFuzz的特性

10.2.1请求

10.2.2模糊变量

10.2.3响应

10.3必要的背景知识

10.3.1识别请求

10.3.2漏洞检测

10.4 WebFuzz的开发

10.4.1开发方法

10.4.2开发语言的选择

10.4.3设计

10.5实例研究

10.5.1目录遍历

10.5.2溢出

10.5.3SQL注入

10.5.4XSS脚本

10.6益处和改进的余地

10.7小结

第11章 文件格式模糊测试

11.1目标应用

11.2方法

11.2.1强制性或基于变异的模糊测试

11.2.2智能强制性或基于生成的模糊测试

11.3输入

11.4漏洞

- 11.4.1拒绝服务
- 11.4.2整数处理问题
- 11.4.3简单的栈和堆溢出
- 11.4.4逻辑错误
- 11.4.5格式化字符串
- 11.4.6竞争条件
- 11.5漏洞检测
- 11.6小结

第12章 文件格式模糊测试：UNIX平台上的自动化测试

- 12.1NOTSPIKEFILE和SPIKEFILE
- 12.2开发方法
 - 12.2.1异常检测引擎
 - 12.2.2异常报告(异常检测)
 - 12.2.3核心模糊测试引擎
- 12.3有意义的代码片段
 - 12.3.1通常感兴趣的UNIX信号
 - 12.3.2不太感兴趣的UNIX信号
- 12.4僵死进程
- 12.5使用的注意事项
 - 12.5.1ADOBE ACROBAT
 - 12.5.2REALNETWORKS REALPLAYRE
- 12.6实例研究：REALPLAYER REALPIX格式化字符串漏洞
- 12.7语言
- 12.8小结

第13章 文件格式模糊测试：Windows平台上的自动化测试

- 13.1 Windows文件格式漏洞
- 13.2 FileFuzz的特性
 - 13.2.1创建文件
 - 13.2.2应用程序执行
 - 13.2.3异常检测
 - 13.2.4保存的审核
- 13.3必要的背景知识
- 13.4 FileFuzz的开发
 - 13.4.1开发方法
 - 13.4.2开发语言的选择
 - 13.4.3设计
- 13.5实例研究
- 13.6益处和改进的余地
- 13.7小结

第14章 网络协议模糊测试

- 14.1什么是网络协议模糊测试
- 14.2目标应用
 - 14.2.1数据链路层
 - 14.2.2网络层
 - 14.2.3传输层
 - 14.2.4会话层
 - 14.2.5表示层
 - 14.2.6应用层
- 14.3测试方法
 - 14.3.1强制性或基于变异的模糊测试
 - 14.3.2智能强制性模糊测试和基于生成的模糊测试
 - 14.3.3修改的客户端变异模糊测试
- 14.4错误检测
 - 14.4.1人工方法(基于调试器)

14.4.2自动化方法(基于代理)

14.4.3其他方法

14.5小结

第15章 网络协议模糊测试：UNIX平台上的自动化测试

15.1使用SPIKE进行模糊测试

15.1.1选择测试目标

15.1.2协议逆向工程

15.2SPIKE 101

15.2.1模糊测试引擎

15.2.2通用的基于行的TCP模糊器

15.3基于块的协议建模

15.4SPIKE的额外特性

15.4.1特定于协议的模糊器

15.4.2特定于协议的模糊测试脚本

15.4.3通用的基于脚本的模糊器

15.5编写SPIKE NMAP模糊器脚本

15.6小结

第16章 网络协议模糊测试：Windows平台上的自动化测试

16.1ProtoFuzz的特性

16.1.1包结构

16.1.2捕获数据

16.1.3解析数据

16.1.4模糊变量

16.1.5发送数据

16.2必要的背景知识

16.2.1错误检测

16.2.2协议驱动程序

16.3ProtoFuzz的开发

16.3.1开发语言的选择

16.3.2包捕获库

16.3.3设计

16.4实例研究

16.5益处和改进的余地

16.6小结

第17章 Web浏览器模糊测试

17.1什么是Web浏览器模糊测试

17.2目标

17.3方法

17.3.1测试方法

17.3.2输入

17.4漏洞

17.5错误检测

17.6小结

第18章 Web浏览器的模糊测试：自动化

18.1组件对象模型的背景知识

18.1.1在Nutshell中的发展历史

18.1.2对象和接口

18.1.3ActiveX

18.2模糊器的开发

18.2.1枚举可加载的ActiveX控件

18.2.2属性、方法、参数和类型

18.2.3模糊测试和监视

18.3小结

第19章 内存数据的模糊测试

19.1内存数据模糊测试的概念及实施该测试的原因

19.2必需的背景知识

19.3究竟什么是内存数据模糊测试

19.4目标

19.5方法：变异循环插入

19.6方法：快照恢复变异

19.7测试速度和处理深度

19.8错误检测

19.9小结

第20章 内存数据的模糊测试：自动化

20.1所需要的特性集

20.2开发语言的选择

20.3Windows调试API

20.4将其整合在一起

20.4.1如何在特定点将“钩子”植入目标进程

20.4.2如何处理进程快照和恢复

20.4.3如何选择植入钩子的点

20.4.4如何对目标内存空间进行定位和变异

20.5一个最好的新工具PyDbg

20.6一个构想的示例

20.7小结

第三部分 高级模糊测试技术

第21章 模糊测试框架

21.1模糊测试框架的概念

21.2现有框架

21.2.1antiparser

21.2.2Dfuz

21.2.3SPIKE

21.2.4Peach

21.2.5通用模糊器

21.2.6Autodafe

21.3定制模糊器的实例研究：Shockwave Flash

21.3.1SWF文件的建模

21.3.2生成有效的数据

21.3.3对环境进行模糊测试

21.3.4测试方法

21.4模糊测试框架Sulley

21.4.1Sulley目录结构

21.4.2数据表示

21.4.3会话

21.4.4事后验证阶段

21.4.5一个完整的实例分析

21.5小结

第22章 自动化协议解析

22.1模糊测试存在的问题是什么

22.2启发式技术

22.2.1代理模糊测试

22.2.2改进的代理模糊测试

22.2.3反汇编启发式规则

22.3生物信息学

22.4遗传算法

22.5小结

第23章 模糊器跟踪

23.1我们究竟想要跟踪什么

23.2二进制代码可视化和基本块

23.2.1CFG

23.2.2CFG示例

23.3构造一个模糊器跟踪器

23.3.1刻画目标特征

23.3.2跟踪

23.3.3交叉引用

23.4对一个代码覆盖工具的分析

23.4.1PStalker设计概览

23.4.2数据源

23.4.3数据探查

23.4.4数据捕获

23.4.5局限性

23.4.6数据存储

23.5实例研究

23.5.1测试策略

23.5.2测试方法

23.6益处和改进的余地

23.7小结

第24章 智能故障检测

24.1基本的错误检测方法

24.2我们所要搜索的内容

24.3选择模糊值时的注意事项

24.4自动化的调试器监视

24.4.1一个基本的调试器监视器

24.4.2一个更加高级的调试器监视器

24.5调试器在应用程序前先看到的异常和调试器再次看到程序未捕获的异常的比较

24.6动态二进制插装

24.7小结

第四部分 展望

第25章 汲取的教训

25.1软件开发生命周期

25.1.1分析

25.1.2设计

25.1.3编码

25.1.4测试

25.1.5维护

25.1.6在SDLC中实现模糊测试

25.2开发者

25.3QA研究者

25.4安全问题研究者

25.5小结

第26章 展望

26.1商业工具

26.1.1安全性测试工具beSTORM

26.1.2BreakingPoint系统BPS-1000

26.1.3Codenomicon

26.1.4GLEG ProtoVer Professional

26.1.5安全性测试工具Mu-4000

26.1.6Security Innovation Holodeck

26.2发现漏洞的混合方法

26.3集成的测试平台

26.4小结

• • • • • ([收起](#))

[模糊测试_下载链接1_](#)

标签

安全

漏洞

模糊测试

测试

fuzzing

软件安全漏洞发掘

软件

计算机科学

评论

偏实用的一本书，不算深，但从工具到方法都介绍的很全面，如果想深入了解，可以根据书上提供的链接继续摸瓜。总之作为入门书还是很好的。书中定义的Fuzzing Test指的是通过提供非预期输入并监视异常结果来发现软件故障的方法，唔，所以你知道封面为啥有只毛茸茸的大熊了...毛茸茸测试，误，模糊测试的好处是无需大量逆向工程就可以自动化的找到比较容易发现的漏洞，但对于某些类型的漏洞，很可能永远也没法通过这种方法找到，比如由多个步骤链起来的缺陷。另外，在漏洞检测实例分析中，此书用前东家的服务器保护当靶子，我看了很亲切...

书不错，模糊测试的思想和技巧都讲到了，想自己写个Fuzzer也能明白个七八。但翻译的就够呛了，诸多的语句不通，第24章介绍DynamoRIO的时候把MIT翻译成“马萨诸塞

技术研究所”也是又一次拉低了技术翻译界的下限。

内容很全面，作者也很有功力。其中还有一位是paimei的开发者，崇敬。

做黑盒模糊测试的入门书籍，建议有时间的话读英文原版的。对于黑盒测试的整体概念的理解会有帮助，实际测试时可以当做工具书参考。

对这个方向是个不错的指导书

详细阅读了部分章节,粗略阅读了部分章节,省略了几章.总体来讲对fuzz各类型和各平台都有介绍.翻译错误较多.

[模糊测试_下载链接1](#)

书评

模糊测试是对协议的测试，协议可以看成一组输入的向量。

一个模糊测试框架，包括这些部分：

0.协议的交互器（更好的是一个ProxyFuzzer，能支持正常交互的拦截与重放）；可配置payload在协议中的填充的位置 1.协议自身约束的自动化生成，如校验和，web request的token等 2.paylo...

[模糊测试_下载链接1](#)