

《Android安全攻防实战》

图书基本信息

书名：《Android安全攻防实战》

13位ISBN编号：9787121261073

出版时间：2015-7

作者：[南非]麦凯恩 (Makan,K.) , [英]鲍恩 (Bown,S.A.)

页数：320

译者：崔孝晨,武晓音

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Android安全攻防实战》

内容概要

Android是目前最为主流的移动设备操作系统，占据了全球近84%的市场份额。因此，Android系统中的安全问题也就变得十分重要。

本书通过大量极富针对性的实验，通过对常见的安全场景中解决方案的讲解，帮助读者全面掌握各种攻-防实用技能。因而，本书的实用性也很强，即使是一时不能完全理解其中的技术原理的新手，根据作者给出的方法，也能解决实践中遇到的大部分问题；而高手也能从中借鉴到一些好的做法。

全书共分九章，涵盖了基本的Android开发环境和工具；app组件之间及它们与系统的交互方式；Android安全评估框架“drozer”；app及Android原生代码的逆向技巧；各类漏洞的利用及防护方式；使用SSL在网络通信中进行更有效的验证；利用第三方代码库或Android中新增的特性，通过加密和在开发时使用设备管理策略，加固app等内容。

《Android安全攻防实战》寓教于练，可供安全技术研究人员，软件开发人员，电子取证人员学习使用，对于各类高等院校中网络安全相关专业的师生也有较高的参考价值。

书籍目录

第1章 Android开发工具

1

1.1 简介

1

1.2 安装Android开发工具 (ADT)

2

1.3 安装Java开发包 (JDK)

5

1.4 更新API资源

9

1.5 另一种安装ADT的方法

11

1.6 安装原生开发包 (Native Development Kit, NDK)

15

1.7 虚拟Android设备

16

1.8 使用命令行创建Android虚拟设备 (AVD)

19

1.9 使用Android调试桥 (ADB) 与AVD交互

21

1.10 从AVD上复制出/复制入文件

22

1.11 通过ADB在AVD中安装app

23

第2章 实践app安全

24

2.1 简介

24

2.2 检查app的证书和签名

24

2.3 对Android app签名

33

2.4 验证app的签名

37

2.5 探索AndroidManifest.xml文件

37

2.6 通过ADB与activity管理器交互

47

2.7 通过ADB提取app里的资源

50

第3章 Android安全评估工具

56

3.1 简介

56

3.2 制作Santoku启动盘和安装Santoku

58

3.3 安装drozer

62	
3.4	运行一个drozer会话
71	
3.5	枚举已安装的包 (package)
72	
3.6	枚举activity
78	
3.7	枚举content provider
80	
3.8	枚举service
83	
3.9	枚举broadcast receiver
85	
3.10	确定app的受攻击面 (attack surface)
87	
3.11	运行activity
89	
3.12	编写drozer模块——一个驱动枚举模块
91	
3.13	编写一个app证书枚举器
94	
	第4章利用app中的漏洞
98	
4.1	简介
98	
4.2	收集logcat泄露的信息
101	
4.3	检查网络流量
106	
4.4	通过activity manager被动嗅探intent
111	
4.5	攻击service
117	
4.6	攻击broadcast receiver
121	
4.7	枚举有漏洞的content provider
123	
4.8	从有漏洞的content provider中提取数据
126	
4.9	向content provider插入数据
129	
4.10	枚举有SQL-注入漏洞的content provider
131	
4.11	利用可调试的app
134	
4.12	对app做中间人攻击
139	
	第5章保护app
146	

5.1 简介	146
5.2 保护app的组件	147
5.3 通过定制权限保护组件	149
5.4 保护content provider的路径 (path)	152
5.5 防御SQL注入攻击	155
5.6 验证app的签名 (防篡改)	157
5.7 通过检测安装程序、模拟器、调试标志位反逆向工程	161
5.8 用ProGuard删除所有日志消息	164
5.9 用GexGuard进行高级代码混淆	168
第6章逆向app	173
6.1 简介	173
6.2 把Java源码编译成DEX文件	175
6.3 解析DEX文件的格式	177
6.4 解释Dalvik字节码	194
6.5 把DEX反编译回Java	202
6.6 反编译app的原生库	205
6.7 使用GDB server调试Android进程	207
第7章网络安全	211
7.1 简介	211
7.2 验证SSL自签名证书	212
7.3 使用OnionKit库中的StrongTrustManager	221
7.4 SSL pinning——限定受信SSL的范围	223
第8章原生代码中漏洞的利用与分析	231
8.1 简介	231
8.2 检查文件的权限	

232	
8.3	交叉编译原生可执行程序
241	
8.4	利用竞争条件引发的漏洞
249	
8.5	栈溢出漏洞的利用
254	
8.6	自动fuzzing测试Android原生代码
261	
	第9章加密与在开发时使用设备管理策略
274	
9.1	简介
274	
9.2	使用加密库
275	
9.3	生成对称加密密钥
277	
9.4	保护SharedPreferences数据
281	
9.5	基于口令的加密
283	
9.6	用SQLCipher加密数据库
287	
9.7	Android KeyStore provider
290	
9.8	在开发时使用设备管理策略
293	

《Android安全攻防实战》

精彩短评

- 1、译者注的那么多改错，就知道作者这书是多毛躁不认真...
- 2、内容一般，翻译一般，看目录就觉得没什么条理性，看完果然是这样...

《Android安全攻防实战》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com