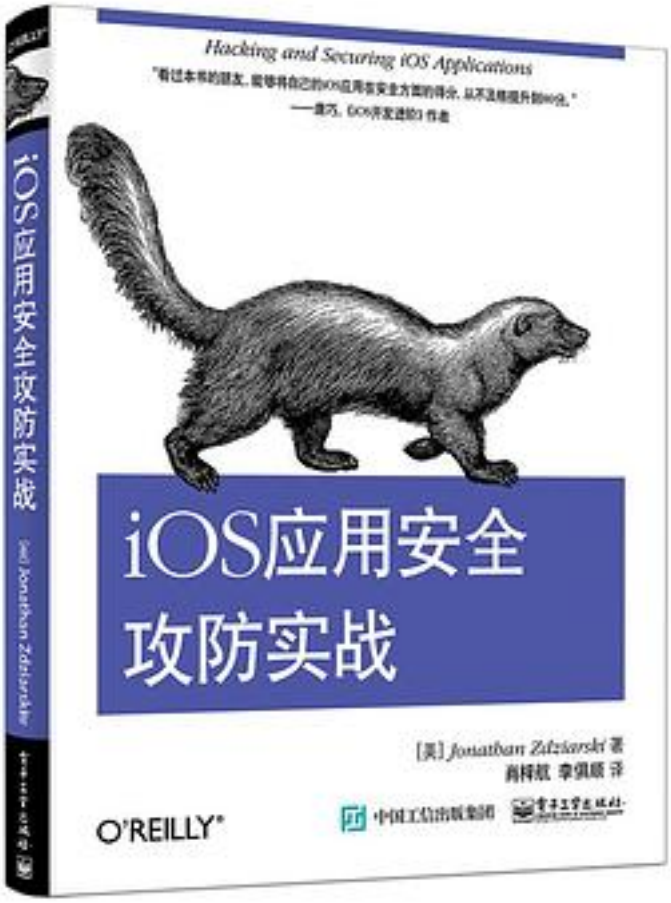
iOS应用安全攻防实战



iOS应用安全攻防实战_下载链接1_

著者:[美]约翰坦·斯的扎斯克

出版者:电子工业出版社

出版时间:2015-7

装帧:平装

isbn:9787121260742

数据被盗等安全问题已经不再是一件罕见的事情了。在这个信息化的时代里，数据就是价值，而且有越来越多的迹象表明，攻击者也正逐步将攻击目标转到移动端。如何保障自己的应用数据安全？《iOS应用安全攻防实战》将会提供一些用于防御常见攻击方法

的方式。安全专家Jonathan Zdziarski
将演示攻击者用来窃取数据、操控软件的许多技术，并向开发者介绍如何避免在软件中犯下各类常见的错误，以及避免软件被轻易地攻击。

作者介绍:

目录: 前言 xv
第1 章 你所知道的一切都是错的 1
单一化方案的误解 2
iOS 安全模型 4
iOS 安全模型的组件 4
钥匙和锁存在一起 7
密码等于弱安全 8
数字取证击败加密 9
外部数据同样也有风险 10
劫持流量 10
数据可能很快就被偷走 11
谁都不要信，包括你的应用软件 12
物理访问并非必需的 13
总结 14
第1 篇 攻击
第2 章 iOS 攻击基础 17
为什么要学习如何破解一台设备 17
越狱解析 18
开发者工具 18
终端用户越狱 20
越狱一台iPhone 21
DFU 模式 22
不完美越狱和完美越狱 24
攻破设备并注入代码 24
构建定制代码 25
分析你的二进制程序 27
测试你的二进制程序 29
代码守护化 31
以tar 归档包的形式部署恶意代码 35
以RAM 磁盘形式部署恶意代码 36
练习 50
总结 50
第3 章 窃取文件系统 53
全盘加密 53
固态NAND 53
磁盘加密 54
iOS 硬盘加密会让你在哪里失败 55
复制实时文件系统 56
DataTheft 载荷 56
定制launchd 66
准备RAM 磁盘 72
创建文件系统镜像 73
复制原始文件系统 75
RawTheft 载荷.....75
定制launchd 80
准备RAM 磁盘 81

创建文件系统镜像 82
练习 83
社会工程学的作用 83
无法正常使用的诱饵设备 84
未激活的诱饵设备 85
包含恶意代码的诱饵 ...86
密码工程学软件 86
总结 87
第4 章 取证跟踪和数据泄露 89
提取照片的地理标签 90
被合并到一起的GPS 缓存 91
SQLite 数据库 93
连接到一个数据库 93
SQLite 内建命令 94
执行SQL 查询 95
重要的数据库文件 95
联系人地址簿 95
地址簿头像 97
Google 地图数据 99
日历事件 105
通话记录 105
电子邮件数据库 106
笔记 107
照片元数据 108
短信 108
Safari 书签 109
短信spotlight 缓存 109
Safari Web 缓存 110
Web 应用缓存 110
WebKit 存储 110
语音邮件 110
对残余的数据库记录进行逆向 111
短信草稿 113
属性列表 113
重要的属性列表文件 . 114
其他重要的文件 119
总结 121
第5 章 对抗加密 123
Sogeti 数据保护工具 123
安装数据保护工具 124
构建暴力破解器 125
构建需要的Python 库 126
提取加密密钥 126
KeyTheft 载荷 126
定制launchd 127
准备RAM 磁盘 128
准备内核 129
执行暴力破解 130
解密钥匙链 133
解密原始磁盘 135
解密iTunes 备份文件 137
通过间谍件对抗加密 137
SpyTheft 载荷..... 138
将spyd 守护化 143

定制launchd 144
准备RAM 磁盘 145
执行载荷 145
练习 146
总结 146
第6 章 无法销毁的文件 ... 147
刮取HFS 日志 148
还原闲置空间 150
常被还原出来的数据 150
应用软件屏幕截图 150
已删除的属性列表 152
已删除的语音邮件和录音 152
以删除的键盘缓存 152
照片和其他个人信息 . 152
总结 153
第7 章 操作运行时环境 ... 155
分析二进制软件 156
Mach-O 文件格式 156
class-dump-z 简介 160
符号表 161
加密的二进制文件 163
计算偏移值 164
转储内存 165
将解密的代码复制回文件 167
重置cryptid 168
利用Cycript 操作运行时 . 170
安装Cycript 171
使用Cycript 171
破解简单的锁 173
替换方法 180
撒网搜寻数据 182
记录数据 185
更多严重的隐含问题 . 186
练习 194
SpringBoard 动画 194
接听来电 195
屏幕截图 195
总结 195
第8 章 操纵运行时库 197
Objective-C 程序解析 197
类实例变量 199
类方法 200
类方法缓存 200
反汇编与调试 201
监视 206
底层Objective-C 框架 208
Objective-C 接口 210
恶意代码注入 212
CodeTheft 载荷 212
使用调试器注入 213
使用动态连接攻击注入 215
全设备感染 216
总结 217
第9 章 劫持流量 219

APN 劫持 219
交付载荷 222
清除 224
简单的代理设置 225
攻击SSL 225
SSLStrip 225
Paros Proxy 227
浏览器警告 228
攻击应用软件级别的SSL 验证 231
SSLTheft 载荷 233
劫持基础HTTP 类 238
POSTTheft 载荷 238
分析数据 241
Driftnet 243
构建 243
运行 244
练习 246
总结 246
第2 篇 防护
第10 章 加密实现 249
密码强度 249
当心随机密码生成器 . 252
Common Crypto 介绍 253
无状态操作 253
有状态加密 258
主密钥加密 261
地理加密 266
使用口令的地理加密 . 269
拆分服务器端密钥 271
安全内存 273
清除内存 274
公钥加密体系 275
练习 280
第11 章 反取证 281
安全的文件擦除 281
美国国防部 5220.22-M 标准擦除 282
Objective-C 284
擦除SQL 记录 286
键盘缓存 292
随机化PIN 码 292
应用程序屏幕快照 294
第12 章 运行时库安全 297
篡改响应 297
擦除用户数据 298
禁止网络访问 298
报告机制 299
启用日志记录 299
暗桩和自杀分支 299
进程调试检测 300
阻挡调试器 302
运行时库类完整性检查 304
检查内存地址空间 304
内联函数 316
反汇编复杂化 324

优化标记 324
去除符号 329
循环展开-funroll-loops 336
练习 339
第13 章 越狱检测 341
沙盒完整性检测 341
文件系统检测 343
越狱文件是否存在 343
/etc/fstab 文件大小 344
符号链接检测 345
分页执行检查 345
第14 章 下一步 347
像攻击者一样思考 347
其他逆向攻击 347
安全对抗代码管理 348
灵活的方式实现安全 349
其他不错的书籍 349
附录A 新的起点 351
・・・・・・(收起)

iOS应用安全攻防实战_下载链接1_

标签

安全

iOS

ios

计算机

攻击

防御

技术

Security

评论

内容本身应该不错，可能是翻译问题？和之前那本UI的有的一拼？买中文版是因为便宜读起来省力，读这本的时候会想这英文原文到底是啥。。。建议看英文版去吧。

----
iOS应用安全攻防实战_下载链接1_

书评

test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test-test

----
iOS应用安全攻防实战_下载链接1_