第一图书网, tushu007.com

<<Android应用程序安全>>

图书基本信息

书名：<<Android应用程序安全>>

13位ISBN编号：9787121213830

10位ISBN编号：7121213834

出版时间：2013-10

出版时间：电子工业出版社

作者：[美]古纳塞克若（Gunasekera,S.）

译者：王文君,董欢欢

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：http://www.tushu007.com

内容概要

本书是一本系统讲解Android应用开发安全的书籍。
它首先介绍了Android系统的架构和安全机制，然后详细说明了Android应用中存在的安全风险，并提出如何实现相应的安全控制以保护用户的私密信息。
同时，本书还深入讲解了数据加密、认证技术以及企业级安全等概念。
通过本书的介绍，希望读者能够了解如何鉴别哪些是敏感数据、如何使用Android API保证数据的机密性和完整性、如何构建企业级安全的应用以及如何实现客户/服务端应用之间数据管理与传输的安全性等。

本书适用于Android应用开发人员、设计人员、测试人员、架构师、项目经理、安全咨询顾问等，是一本实用的讲解Android应用安全的教材和使用手册。

作者简介

Sheran Gunasekera是一名拥有13年信息安全经验的安全研究人员和软件开发者。
他是ZenConsult Pte.公司的研发主管，负责个人计算机和移动设备平台的安全研究。
Sheran一直积极致力于BlackBerry和移动Java的研究，并且是揭露首个企业认可的恶意应用内部工作原理的白皮书的作者，这些恶意软件被部署在阿联酋电信运营商签约用户的移动设备上。
他曾在中东、欧洲和亚太地区的安全会议上发表演讲，提供有关针对移动设备的恶意软件分析，以及针对Web和移动设备的安全软件开发的培训。
他还在其有关安全的博客上撰写并发表文章（http://chirashi.zenconsult.net）。

第一图书网, tushu007.com

书籍目录

第1章　Android架构　1
1.1　Android架构的组件　3
1.1.1　内核　4
1.1.2　类库　5
1.1.3　Dalvik虚拟机　5
1.1.4　应用程序框架　6
1.1.5　应用程序　8
1.2　这本书是关于什么的　9
1.3　安全　9
1.3.1　保护用户　10
1.3.2　安全风险　10
1.4　Android安全架构　12
1.4.1　特权分离　12
1.4.2　权限　13
1.4.3　应用程序代码签名　14
1.5　总结　14
第2章　信息：应用的基础　16
2.1　保护你的应用免受攻击　17
2.1.1　间接攻击　17
2.1.2　直接攻击　19
2.2　项目1：“ Proxim ”和数据存储　19
2.3　信息分类　27
2.3.1　什么是个人信息　29
2.3.2　什么是敏感信息　29
2.4　代码分析　29
2.4.1　实施加密　30
2.4.2　加密结果　32
2.5　重构项目1　33
2.6　练习　35
2.7　总结　36
第3章　Android安全架构　37
3.1　重温系统架构　38
3.2　理解权限架构　40
3.2.1　Content Provider　41
3.2.2　Intent　46
3.3　权限检查　47
3.3.1　使用自定义权限　48
3.3.2　保护级别　49
3.3.3　自定义权限的示例代码　50
3.4　总结　53
第4章　动手实践（第一部分）　55
4.1　Proxim应用　56
4.2　总结　64
第5章　数据存储和密码学　65
5.1　公钥基础设施（PKI）　67

5.2 密码学中用到的术语 70
5.3 手机应用中的密码学 71
5.3.1 对称加密算法 72
5.3.2 密钥生成 73
5.3.3 数据填充 74
5.3.4 分组密码的几种模式 75
5.4 Android系统中的数据存储 80
5.4.1 用户数据共享 81
5.4.2 内部存储 84
5.4.3 SQLite数据库 87
5.5 加密的数据存储 93
5.6 总结 101
第6章 对话Web应用 103
6.1 搭建环境 105
6.2 HTML、Web应用和Web服务 113
6.2.1 Web应用的组成 115
6.2.2 Web应用用到的技术 117
6.3 OWASP与Web攻击 124
6.4 认证技术 126
6.4.1 自签名证书 131
6.4.2 中间人攻击 132
6.4.3 OAuth 134
6.4.4 加密的挑战/应答 143
6.5 总结 143
第7章 企业级应用开发安全 144
7.1 安全的连接 145
7.2 企业应用程序 147
7.3 手机中间件 147
7.3.1 数据库访问 149
7.3.2 数据表示 155
7.4 总结 162
第8章 动手实践（第二部分） 163
8.1 OAuth 164
8.1.1 获得令牌 165
8.1.2 处理授权 166
8.2 挑战与应答 178
8.3 总结 193
第9章 发布和出售你的应用 194
9.1 开发人员注册 195
9.2 你的应用处在暴露中 197
9.2.1 可供下载的资源 198
9.2.2 逆向工程 202
9.3 应该进行许可验证吗 208
9.4 Android许可验证库 208
9.4.1 下载Google API Add-On 215
9.4.2 复制LVL文件至单独目录 217
9.4.3 导入LVL源文件作为一个Library项目 217

9.4.4 在应用中构建和引入LVL 222
9.5 许可策略 229
9.6 有效利用LVL 231
9.7 模糊处理 233
9.8 总结 236
第10章 恶意软件和间谍软件 238
10.1 恶意软件的四个阶段 240
10.1.1 感染 240
10.1.2 破坏 240
10.1.3 传播 241
10.1.4 泄露 241
10.2 案例学习1：政府批准的恶意软件 241
10.2.1 感染 242
10.2.2 破坏 243
10.2.3 传播 243
10.2.4 泄露 243
10.2.5 检测 244
10.3 案例学习2: 零售恶意软件——FlexiSPY 246
10.4 反取证 248
10.5 总结 250
附录A Android权限常量 252
附录B 如何使用Apache Wink创建RESTful Web Services 262

第一图书网, tushu007.com

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:http://www.tushu007.com