HZ BOOKS
华章科技

移动开发

原理分析透彻，结合Android系统源代码，从应用层、应用框架层、硬件抽象层、系统内核层等多角度剖析了Android的安全机制和实现原理，以及安全机制中存在的不足和潜在风险。

实用性强，不仅介绍了各种常用的实用分析工具、安全风险分析方法、安全策略，而且还针对Android在各种应用领域可能出现的安全问题给出了解决方案。

吴倩 赵晨啸 郭莹◎著

Android Security Mechanism and Application Practices

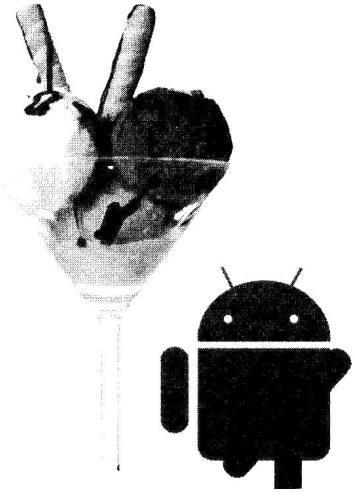
Android安全机制解析与应用实践

机械工业出版社
China Machine Press

Android Security Mechanism and Application Practices

Android安全机制解析与应用实践

吴倩 赵晨啸 郭莹◎著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Android 安全机制解析与应用实践 / 吴倩，赵晨啸，郭莹著 . —北京：机械工业出版社，2013.5

ISBN 978-7-111-42016-3

Ⅰ . A… Ⅱ . ① 吴… ② 赵… ③ 郭… Ⅲ . 移动终端 – 应用程序 – 程序设计 Ⅳ . TN929.53

中国版本图书馆 CIP 数据核字（2013）第 066947 号

本书是 Android 安全领域的经典著作，不仅深入剖析了原理，而且还给出了应对各种安全问题的方法，原理与实践并重。首先，结合 Android 系统的源代码从应用层、应用框架层、硬件抽象层、系统内核层等多角度剖析了 Android 的安全机制和实现原理，以及安全机制中存在的不足和潜在风险；然后详细讲解了各种常用的实用分析工具、安全风险分析方法、安全策略，以及各种常见安全问题（内核、文件系统、应用程序及无线通信）的解决方案。

全书共 9 章，分为三部分：准备篇（1~2 章）介绍了 Android 的系统架构和安全模型；原理篇（3~5 章）首先从源代码的角度深入剖析了 Android 系统的安全机制、系统安全性和应用安全性的实现原理，然后详细讲解了各种实用分析方法、分析工具和核心技术；实践篇（6~9 章）分别讲解了如何通过修改源代码来增强 Android 系统的安全性、加密文件系统的原理分析和系统配置、各种实用的安全解决方案（应用权限控制、应用程序签名、静态代码分析、防火墙、存储加密、组件开发的安全要点等），以及 Android 的无线通信安全。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：姜 影

三河市杨庄长鸣印刷装订厂印刷

2013 年 5 月第 1 版第 1 次印刷

186mm×240mm • 15 印张

标准书号：ISBN 978-7-111-42016-3

定价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

推 荐 序

随着人类社会进入信息化时代，各类信息技术产品已经成为人们生活和工作中各个环节不可缺少的部分，甚至对整个人类世界的行为都产生了潜在影响。但在人们享受信息技术带来的便利的同时，由此带来的信息安全问题也引起了人们的广泛重视。

在信息安全技术领域，网络与系统安全是主要方向之一。而在构成网络与系统安全技术体系的各分支中，毋庸置疑，操作系统安全是必不可少的核心组成。在过去的很多年，伴随着计算机从大型机时代发展到PC时代，操作系统安全研究也经历了以服务器操作系统安全为中心到服务器与PC终端操作系统安全并重的发展过程。UNIX、Linux、Windows NT、Windows 7等操作系统均集成应用了包括认证、访问控制、安全审计、可信计算等技术在内的安全机制，为人们利用计算机处理信息提供了安全保障。

近年来，随着智能手机、平板电脑等智能终端的迅猛发展，信息世界已进入后PC时代。相对应的，智能终端操作系统安全也成为信息安全领域广泛关注的议题。而对于已占据智能终端操作系统市场最大份额的Android操作系统，其安全势必成为工业界和学术界共同关注的目标。Android操作系统提供了哪些安全机制，其安全性如何，如何有效合理地利用其各类安全机制都成为终端制造商、应用开发商、终端用户共同关心的问题。

本书作者基于自己的实际工作经验，从安全角度出发，结合Linux知识对Android基础知识、原生安全机制、新增安全增强机制以及应用安全进行了介绍，并结合相应代码进行了分析、梳理，介绍了相应的安全分析方法与工具。与单纯对Android系统进行整体介绍的书籍相比，本书更多地从安全视角进行材料的组织和编写，是一本较好的学习Android安全的基础参考读物，较为适合有一定的Android应用程序开发基础或者Linux安全基础，想要了解Android系统安全机制或想要掌握Android安全开发方法的读者阅读。

需要指出的是，智能终端操作系统安全作为一门新兴的研究领域，目前还处于刚刚起步的阶段，对于研究工作而言还有很长的路要走，现在的安全分析并不总是能够准确预言未来的发展，那么这本书就是一个起点。

归而总之，通过对 Android 安全基础知识的学习，一方面有利于对现状有更为清醒的认识，另一方面也可从知识体系上为未来进一步的研究与实践打下一个较好的基础。因此，无论对于安全研究人员、应用开发人员，本书都具有很好的参考价值。

田　静

中国科学院信息工程研究所所长

为什么写这本书

作为目前应用范围最广、最开放的高性能移动计算平台，Android 系统的信息安全保障面临着前所未有的挑战。传统计算机网络与计算机系统在过去三十年所面临的各种安全威胁与安全风险不但会在 Android 系统的生态环境中再现，而且，由于 Android 系统前所未有的开放性及无处不在的高性能网络计算能力，各类安全威胁将更加花样百出，并且无法预测。为应对各种安全威胁，Android 系统安全机制贯穿了系统架构设计的各个层面，涵盖了操作系统内核、硬件抽象层、JAVA 虚拟机、应用框架层，以及应用层的各个环节。然而，在开发与应用实践中，无论 是 OEM 厂家或方案设计公司的系统工程师、应用工程师，还是独立的第三方应用开发工程师，都迫切需要正确理解并有效运用 Android 系统提供的诸多安全机制，且要对 Android 已有安全机制的潜在缺陷与不足有充分的认识，并对多种尚未融入 Android 开发主干的安全机制，如 SE Android 等，不断跟踪了解，并适当加以应用。

本书作者基于过去近 20 年间在 UNIX/Linux 操作系统领域的研发实践以及近年来 Android 系统的开发经验，在本书中介绍了 Android 系统安全机制的实现原理，探讨分析了 Android 安全机制的不足与潜在风险，并且分享了相关安全增强与改进工作的最新进展与成果。本书采用原理阐述、相关源代码分析、实用分析工具介绍，以及安全风险分析、安全策略与解决方案相结合的方式，力图将理论与实践有机关联，重点是提升读者的实际应用能力。

本书在 Android 系统安全性分析中融入了对 UNIX/Linux 系统安全模型的介绍，总结归纳了在 UNIX/Linux 环境下进行安全程序设计的重要实用原则。毕竟，Android 的系统安

全机制完全基于 UNIX/Linux 的安全模型，而许多 Android 应用开发者并非资深的 UNIX/Linux 应用设计工程师。

OEM 厂家或方案设计公司的开发工程师与第三方应用开发工程师往往对系统安全与应用安全的理解与需求不尽相同，有时甚至差异甚大。本书虽然对 Android 的系统安全性与应用安全性分别进行了描述，但仍尽力阐明，在安全实践中不可能完全割裂两者之间的联系。片面强调任何一个方面，都不足以解决安全问题。

Android 系统具备无处不在的无线网络移动计算能力，所面临的安全风险也不仅限于 Android 设备的软、硬件安全与数据存储安全。实际上，除了系统自身的安全性外，在网络移动计算的各个应用领域、各个应用环节，Android 用户都面临着形形色色的安全威胁。本书作者将自己在移动计算与无线通信安全领域的研发实践加以提炼，并通过本书分享给读者。比如，通过在无线移动通信中短信、彩信与语音通话的端到端安全保障等方面的工作，与读者分享一系列闭环安全设计，以及全方位、多角度保护用户信息安全的实践思考。

本书的主要内容及特色

本书分为准备篇、原理篇、实战篇三大部分，共 9 章。首先介绍 Android 架构以及系统安全模型，然后分析 Android 安全机制源代码及 Android 系统存在的安全风险，接着介绍一系列的安全分析工具及方法，最后为内核、文件系统、应用程序及无线通信等方面的安全问题提出解决方案。其中还简要介绍了现代密码学中有关数字密码算法与协议等知识，供读者参考。

准备篇包括第 1 章和第 2 章。

- 第 1 章简单直接地阐明 Android 系统架构、应用程序组件、系统启动流程以及系统升级等方面的要点。
- 第 2 章对 Android 安全模型进行初步介绍，内容涉及 Linux 内核安全机制及 Android 安全机制，使读者迅速进入本书的知识氛围。

原理篇包括第 3 ～ 5 章。

- 第 3 章在 Android 系统实现的源代码层面为读者详细剖析 Android 安全模型的架构原理与实现方式。
- 第 4 章对 Android 的安全模型进行风险分析，并列举已知的安全风险和漏洞。
- 第 5 章向读者介绍一系列能进行系统安全性分析的软、硬件工具与方法。有兴趣的读者在使用这些安全分析工具与方法满足自己好奇心的同时，也会感受到这些工具

的威力，进而能够更加缜密地思考安全策略。

实战篇包括第 6 ～ 9 章。

- 第 6 章介绍采用 SE Android 对 Android 系统内核安全进行增强。
- 第 7 章介绍对 Android 文件系统进行加密的方法。
- 第 8 章从应用安全的角度，针对各种安全威胁与风险，提出对应的策略与解决方案。
- 第 9 章向读者展示了无线移动通信中用户实时语音通信与信息交互应用中的安全实践与思考。

本书面向的读者

- 希望融入火热的、更具（至少同样具有）挑战性的 Android 系统与应用开发的 UNIX/Linux 系统与应用开发工程师。
- Android 系统 OEM 厂家或方案设计公司的系统工程师与应用工程师。
- 独立的第三方 Android 应用开发工程师。
- 无线移动通信信息安全系统分析师与设计师。
- Android 设备资深发烧友。

如何阅读本书

本书采用由浅入深、循序渐进的方式组稿，绝大部分读者可以顺序阅读。但是，一些特殊读者可以像下面这样选择性阅读。

- 有一定开发经验的 Android 开发者，可以快速扫过第 1 章，从第 2 章进入本书的阅读。
- 资深 UNIX/Linux 开发者会发现许多耳熟能详的设计概念与实践思想，但是一定不要在阅读时想当然，Android 系统设计屡有奇思妙想与创新思维，只有仔细思考才能不断体会 40 年来 UNIX 系统设计的意想不到之妙。
- 资深的 Android 系统开发者，可重点关注第 6 章与第 7 章的内容，Android 系统主干发布（Trunk Release）必定包含更多的内置安全机制。
- 活跃的 Android 应用开发者可以直奔第 8 章，平常散落各个角落的应用程序设计安全要点尽在其中。
- 对无线移动通信信息安全有兴趣的读者可以重点关注第 9 章。端到端的移动通信安

全方案不限于 Android 系统的范畴，其不但具备一定普遍性，而且是保障实时通信信息安全的最佳实践之一。

勘误及支持

写了多年代码之后第一次写书，加之水平有限，书中错误难免，希望各位读者随时指出不足之处、不吝赐教，欢迎通过 android_security@126.com 与我们联系。也希望您在写代码的同时，能拨冗挥笔，共享妙思。在此预先向各位表示感谢。

致谢

记得 UNIX 的发明者 Ken Thompson 曾经说："别写文章、写代码！"（Don't Write Paper，Write Code!），我们一直以自己能多写代码为荣！可是，多年之后的今天，才发现写本书是多么的不容易！

首先感谢杨福川编辑与姜影编辑！我们的突发奇想在杨福川编辑的激励与指导下开始有了最初构思与书稿架构。姜影编辑则在长达几个月的写作过程中，孜孜不倦地审阅书稿，她的耐心与专业使我们这些写代码的人对出版规范和要求有了深刻的认识。

其次要感谢我们的家人与领导，感谢他们在写作的过程中给予我们的支持与理解！感谢与我们天天一起工作的同事！他们不但给了我们许多灵感与建议，而且贡献了许多新思想、新代码。最真诚的感谢献给与我们在一起每天不倦编码的同事穆德龙、陶娅、许永嘉与张亚光。

推荐阅读

深入Android应用开发：核心技术解析与最佳实践

作者：苗忠良 等著　ISBN：978-7-111-37957-7　定价：79.00元

内容简介

如何才能真正进阶为Android应用开发高手？必须深入理解Android核心技术的底层原理和在开发中总结并使用各种最佳实践，别无他法！本书以Android的源代码为主，SDK为辅，针对应用开发者的需求，对各种核心技术的使用方法、底层原理和实现细节进行了深入而详细的讲解，同时辅之以大量案例和最佳实践，为开发者的进阶修炼和开发高质量的应用提供了绝佳指导。

Android开发精要

作者：范怀宇 著　ISBN：978-7-111-39058-9　定价：69.00元

内容简介

这如何才能写出贴近Android设计理念、能够更加高效和可靠运行的Android应用？通过Android的源代码去了解其底层实现细节是最重要的方法之一！

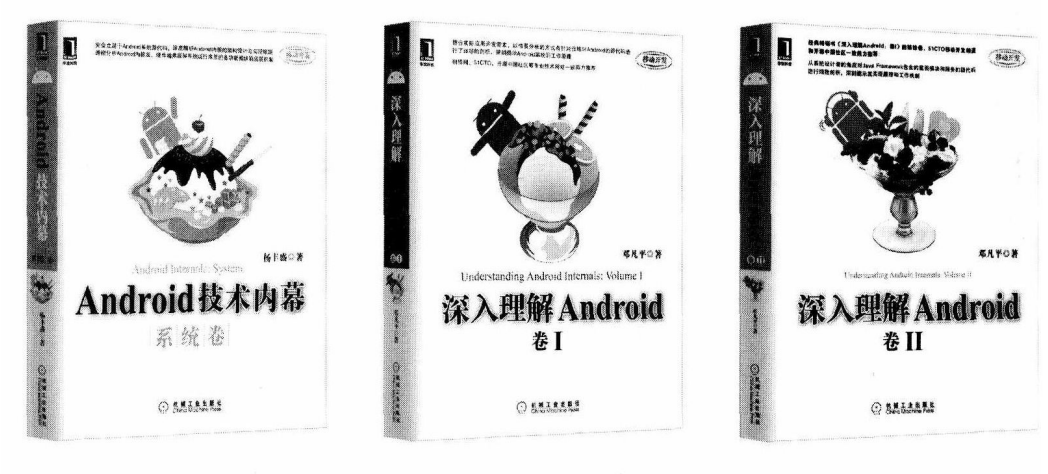
AIR Android应用开发实战

作者：邱彦林 著　ISBN：978-7-111-39177-7　定价：69.00元

内容简介

本书由资深Adobe技术专家兼资深Android应用开发工程师亲自执笔，既系统全面地讲解了如何利用Adobe AIR技术开发Android应用，又细致深入地讲解了如何将已有的基于PC的AIR应用移植到Android设备上。不仅包含大量实践指导意义极强的实战案例，而且还包括大量建议和最佳实践，是系统学习AIR Android应用开发不可多得的参考书。

推荐阅读



Android技术内幕：系统卷

作者：杨丰盛 ISBN：978-7-111-33727-0 定价：69.00元

国内首本系统对Android的源代码进行深入分析的著作，畅销书。全书将Android系统从构架上依次分为应用层、应用框架层、系统运行库层、硬件抽象层和Linux内核层等5个层次，旨在通过对Android系统源代码的全面分析来帮助开发者加深对Android系统架构设计和实现原理的认识，从而帮助他们解决开发中遇到的更加复杂的问题。

深入理解Android：卷I

作者：邓凡平 ISBN：978-7-111-35762-9 定价：69.00元

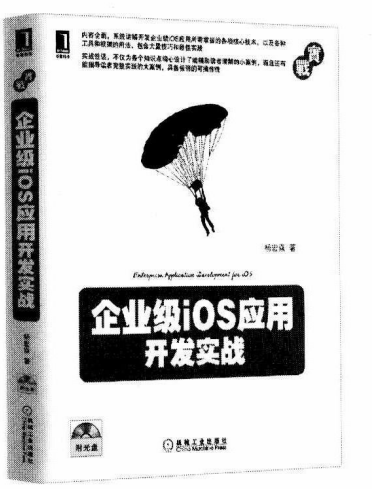
这是一本以情景方式对Android的源代码进行深入分析的书，口碑和销量都很好。内容广泛，以对Framework层的分析为主，兼顾Native层和Application层；分析深入，每一部分源代码的分析都力求透彻；针对性强，注重实际应用开发需求，书中所涵盖的知识点都是Android应用开发者和系统开发者需要重点掌握的。

深入理解Android：卷II

作者：邓凡平 ISBN：978-7-111-38918-7 定价：79.00元

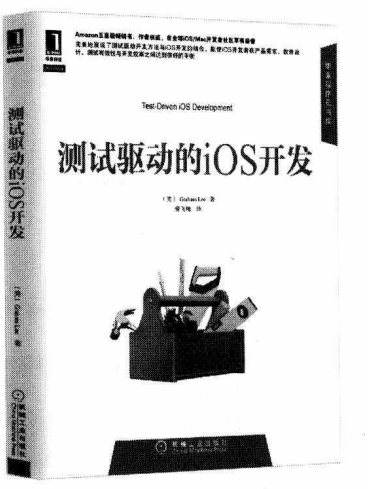
本书是“深入理解Android”系列的第2本，第1本书上市后获得广大读者高度评价，在Android开发者社群内口口相传。本书不仅继承了第1本书的优点并改正了其在细微处存在的一些不足，而且还在写作的总体思想上进行了创新，更强调从系统设计者的角度去分析Android系统中各个模块内部的实现原理和工作机制。

推荐阅读



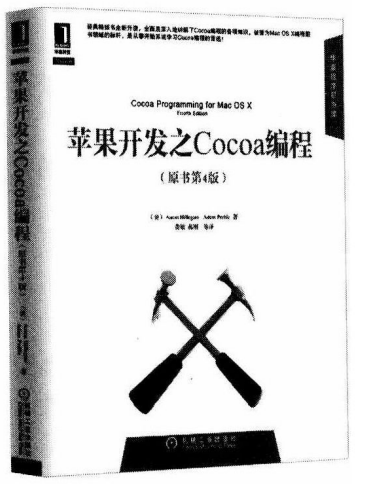
内容全面，系统讲解开发企业级iPhone应用所需掌握的各项核心技术，以及各种工具和框架的用法，包含大量技巧和最佳实践

实战性强，不仅为各个知识点精心设计了能辅助读者理解的小案例，而且还有能指导读者实践的大案例，具备极强的可操作性

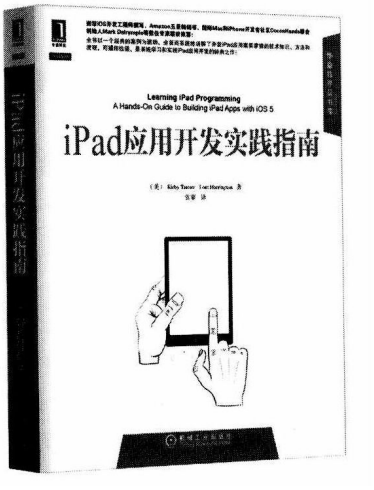


Amazon五星级畅销书，作者权威，在全球iOS/Mac开发者社区享有盛誉！

完美地展现了测试驱动开发方法与iOS开发的结合，能使iOS开发者在产品需求、软件设计、测试有效性与开发效率之间达成很好的平衡

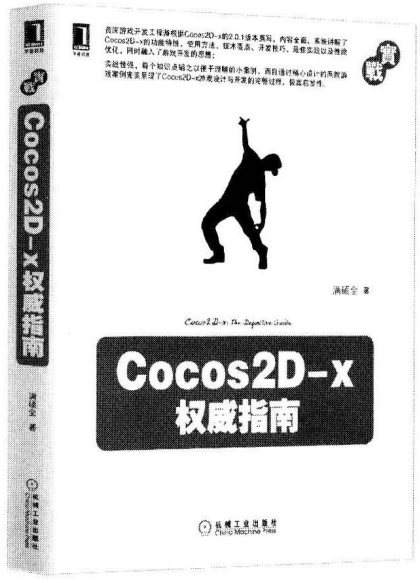


经典畅销书全新升级，系统且深入地讲解了Cocoa编程的各项知识，被誉为Mac OS X编程图书领域的标杆，被公认为从零开始学习Cocoa的首选！



资深iOS开发工程师撰写，Amazon五星级畅销书，国际Mac和iPhone开发者社区CocoaHeads联合创始人Mark Dalrymple等数位专家联袂推荐！

推荐阅读



Cocos2D权威指南

资深专家根据Cocos2D最新版本撰写，内容全面，系统讲解了Cocos2D的使用方法、技术要点、工作原理、开发技巧、最佳实践以及性能优化。

实战性强，通过精心设计的典型案例完美呈现了Cocos2D游戏设计与开发的完整过程，极富启发性。

Cocos2D-x权威指南

资深游戏开发工程师根据Cocos2D-x的2.0.1版本撰写，内容全面，系统讲解了Cocos2D-x的功能特性、使用方法、技术要点、开发技巧、最佳实践以及性能优化，同时融入了游戏开发的思想。

实战性强，每个知识点辅之以便于理解的小案例，而且通过精心设计的两款游戏案例完美呈现了Cocos2D-x游戏设计与开发的完整过程，极富启发性。

第三部分　实践篇