第一图书网, tushu007.com

<<Android安全机制解析与应用实 >

图书基本信息

书名：<<Android安全机制解析与应用实践>>

13位ISBN编号：9787111420163

10位ISBN编号：7111420160

出版时间：2013-4

出版时间：机械工业出版社

作者：吴倩,赵晨啸,郭莹

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

前言

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抉 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。

内容概要

《Android安全机制解析与应用实践》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。

《Android安全机制解析与应用实践》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。

作者简介

吴倩：美国纽约市立大学计算机科学硕士，有近20年的系统软件开发与项目管理经验，在信息安全、嵌入式系统设计、移动通信软件开发、Linux/UNIX操作系统等方面有深入的研究和实践，经验丰富。旅美学习、工作多年后回国参与创立高科技公司，并在大学任教，先后承担了多项国家科研基金项目与产业化项目，发表论文十余篇，拥有多项授权国家发明专利，著有《Java语言程序设计：面向对象的设计思想与实践》一书。
赵晨啸　英国西英格兰大学电子学硕士，近10年软件系统开发经验，精通Linux/UNIX操作系统与Android嵌入式系统设计，主持多项无线移动通信安全设备的设计与开发工作，拥有多项国家发明专利与实用新型专利。
郭莹　济南大学计算机科学硕士，5年通信软件开发经验，精通Linux与Android系统软件设计，承担多款无线移动通信安全设备的设计与开发工作，拥有一项国家发明专利及多项实用新型专利。

书籍目录

推荐序前言第一部分 准备篇第1章 Android基础 / 21.1 Android 系统架构 / 21.1.1 Linux内核层 / 31.1.2 硬件抽象层 / 41.1.3 系统运行库层 / 51.1.4 应用程序框架层 / 71.1.5 应用层 / 71.2 应用程序组件 / 81.3 Android系统启动 / 101.3.1 Linux系统启动 / 101.3.2 Android应用系统启动 / 151.4 Android系统升级 / 171.4.1 Android数据线升级 / 171.4.2 Android SD卡升级 / 171.4.3 Android 在线升级 / 181.5 本章小结 / 18第2章 Android安全模型 / 192.1 Linux安全模型 / 202.1.1 用户与权限 / 212.1.2 进程与内存空间 / 242.2 Android安全机制 / 262.2.1 进程沙箱 / 262.2.2 应用权限 / 282.2.3 进程通信 / 292.2.4 内存管理 / 322.2.5 Android系统分区及加载 / 352.2.6 应用程序签名 / 362.3 Android开发工具提供的安全性机制 / 372.4 本章小结 / 38第二部分 原理篇第3章 Android安全机制源代码分析 / 403.1 文件系统权限的代码实现 / 413.2 进程通信机制的代码实现 / 443.2.1 匿名共享内存 / 443.2.2 Binder机制 / 503.3 Android应用程序安全机制 / 563.3.1 Android应用程序权限机制的源代码分析 / 563.3.2 应用程序签名机制实现的源代码分析 / 623.4 本章小结 / 65第4章 Android安全性分析 / 664.1 Android系统安全分析 / 664.1.1 Linux内核 / 664.1.2 系统库 / 674.1.3 Dalvik虚拟机 / 674.2 Android应用安全分析 / 684.2.1 应用程序权限 / 684.2.2 应用程序安装 / 694.2.3 网络浏览器 / 704.2.4 数据库与SQL注入 / 704.2.5 软件更新 / 714.3 硬件安全分析 / 724.4 恶意软件 / 724.4.1 Linux恶意软件 / 734.4.2 Android恶意软件 / 744.5 安全风险与漏洞 / 754.5.1 已知安全风险 / 754.5.2 潜在安全漏洞 / 764.6 本章小结 / 76第5章 Android实用安全分析工具 / 785.1 实用分析方法 / 785.1.1 Linux系统信息分析 / 795.1.2 Android应用信息分析 / 865.2 实用分析工具 / 925.2.1 Android系统调试工具 / 925.2.2 dumpsys工具 / 1035.2.3 应用程序分析工具 / 1045.3 专业分析工具与技术 / 1075.3.1 常用逻辑分析工具与技术 / 1075.3.2 常用物理分析工具与技术 / 1085.4 本章小结 / 110第三部分 实践篇第6章 SE Android—增强Android安全性 / 1146.1 内核安全风险与增强策略 / 1146.2 SE Android概述 / 1146.3 SE Android编译与安装 / 1156.3.1 源代码获取 / 1156.3.2 源代码结构 / 1166.3.3 源代码编译和安装 / 1186.4 SE Android安全策略概述 / 1246.4.1 seapp_contexts文件 / 1256.4.2 property_contexts文件 / 1256.4.3 mac_permissions.xml文件 / 1266.5 SE Android兼容性测试工具 / 1276.6 SE Android的权限限制策略 / 1276.6.1 强制限制的权限模型 / 1286.6.2 安装时MAC / 1286.6.3 权限取消 / 1286.6.4 权限标签传播 / 1296.6.5 SE Android的其他类与权限策略 / 1296.7 本章小结 / 129第7章 Android加密文件系统 / 1307.1 加密文件系统概述 / 1307.2 加密算法介绍 / 1317.2.1 AES加密算法 / 1317.2.2 加密模式 / 1317.3 加密文件系统源代码分析 / 1337.3.1 Linux内核的dm-crypt / 1347.3.2 Android的vold / 1387.3.3 工作流程分析 / 1457.4 加密文件系统配置 / 1487.4.1 块设备选取与配置 / 1487.4.2 init.rc配置 / 1497.5 本章小结 / 150第8章 Android应用安全实用解决方案 / 1518.1 安全风险控制策略 / 1518.2 应用权限控制 / 1548.2.1 权限控制策略 / 1548.2.2 权限定义和运用 / 1568.3 应用程序签名 / 1598.3.1 数字签名基础知识 / 1608.3.2 数字签名算法 / 1608.3.3 数字签名使用方式 / 1638.3.4 应用程序签名的实现 / 1648.4 静态代码分析 / 1668.5 防火墙 / 1688.6 数据存储加密 / 1708.7 应用程序组件开发的安全要点 / 1728.7.1 私有组件与公有组件 / 1728.7.2 Activity安全 / 1738.7.3 Service安全 / 1748.7.4 Content Provider安全 / 1758.7.5 Broadcast Receiver安全 / 1808.7.6 Intent安全 / 1828.7.7 Binder安全 / 1848.8 本章小结 / 185第9章 Android的无线通信安全 / 1869.1 无线移动通信的安全威胁与防范 / 1869.1.1 语音通信的空口加密与明文传输 / 1879.1.2 短信与彩信的存储转发机制 / 1889.1.3 传统的搭线窃听与合法监控 / 1899.1.4 端到端的通信安全机制 / 1899.2 Android的无线移动电话系统 / 1909.2.1 无线移动电话系统的结构 / 1909.2.2 无线移动电话系统的RIL层实现 / 1909.2.3 无线移动电话系统的应用层框架 / 1939.3 加密短信和彩信收发 / 1969.3.1 普通短信与彩信的收发流程 / 1969.3.2 短信与彩信的数字加密处理 / 2089.3.3 加密短信与彩信的传输处理 / 2109.3.4 加密短信与彩信的存储与调阅 / 2109.4 加密实时语音通信 / 2149.4.1 AT命令与电话建立流程 / 2149.4.2 Android音频系统的电话部分 / 2169.4.3 电话状态下音频通道的设置 / 2179.4.4 电话音频加密处理 / 2189.5 本章小结 / 222

编辑推荐

《Android安全机制解析与应用实践》编辑推荐：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。

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