360 公司创始人、董事长兼 CEO，知名天使投资人

周鸿祎 | 推荐

Android

安全技术揭秘与防范

周圣韬◎著

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

Android
安全技术揭秘与防范

周圣韬◎著

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

Android安全技术揭秘与防范 / 周圣韬著. -- 北京 : 人民邮电出版社, 2015.9
ISBN 978-7-115-40166-3

Ⅰ. ①A… Ⅱ. ①周… Ⅲ. ①移动终端－应用程序－程序设计－安全技术 Ⅳ. ①TN929.53

中国版本图书馆CIP数据核字(2015)第194413号

内 容 提 要

本书从分析 Android 系统的运行原理、框架和主要模块入手，着重分析了 Android 系统存在的安全技术问题，以及这些技术在移动设备上产生的安全问题，帮助读者了解如何静态分析 Android 软件，如何动态调试 Android 软件，如何开发出安全的 App，如何使自己的系统不被盗版，以及 Android 漏洞、逆向工程和反汇编等核心技术。这本书几乎每一个部分，都结合实际例子，一步步讲解，可以使读者了解 App 安全的问题，给开发者一些防范技术，是一本特别实用的 Android 安全指南。移动设备开发者、安全研究人员、Android 应用程序开发者和负责评估 Android 安全性的技术人员都可以在本书中找到必要的指导。

◆ 著　　周圣韬
责任编辑　张　涛
责任印制　张佳莹　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：21.75
字数：502 千字　　2015 年 9 月第 1 版
印数：1－3 000 册　　2015 年 9 月北京第 1 次印刷

定价：69.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前　言

随着 Android 的快速发展，智能设备得到了很大的普及，小到手机、一副眼镜和一块手表，大到智能 TV 和汽车上的智能设备，Android 系统已经深入到各个方面，形成了一个 IT 生态系统，但由于 Android 系统是开源的，许多人在研究系统源程序的基础上开发了很好的产品，如小米手机、各种 App 应用、各种穿戴设备等。在技术被利用的同时，一些黑客也开始对这种系统产生了兴趣，有的破解别人的 App 源程序作为自己的应用谋取利益，有的编写黑客程序窃取手机里的通信记录，有的逆向别人的系统进行盗版等，Android 系统的安全问题越来越受大家的关注。为了给读者增强 Android 系统的安全知识，帮助个人保护好个人隐私，帮助开发者开发出更安全的 App 程序，帮助企业建立稳固的系统，本书特意就 Android 系统存在的安全技术问题以及安全补救的技术进行了全面的阐述，并通过实例让读者达到学以致用的目标。

本书的结构

读者学习本书应该按照章节顺序进行阅读，这样可以系统地学习 Android 的安全知识，但是正在深入研究 Android 安全技术的读者，也可以将本书作为一本参考资料。本书共分为 11 章，几乎涵盖了安全研究人员学习 Android 所需要了解的所有内容。这些章节通过图、表、效果图、源程序和反汇编程序等来介绍 Android 安全技术，并探讨了 Android 系统漏洞、逆向工程和 App 的安全技术。全书的主要内容为：理解 Android 系统、Root 你的设备、Root 漏洞、Root 安全、键盘监控、APK 静态分析、常用分析利器、资源逆向工具 AXMLPrinter、超级编辑器 UltraEdit、常用的 Smali 注入代码、广告植入与去除、APK 动态分析、代码安全分析、使用 Log 进行逻辑跟踪、网络抓包、调试 WebView App、SQL 注入攻击、动态注入技术、Hook 原理、Hook 的危害、App 登录劫持、Hook 检测/修复、应用加固与渗透测试、防止利用系统组件漏洞、Activity 编码安全、Brocast Recevier 编码安全、Service 编码安全、Provider 编码安全、防止逆向、DEX 保护、防止二次打包、防止进行动态注入、Android 渗透测试、应用程序渗透测试、系统安全措施、启动验证、磁盘加密、屏幕安全、图案锁、USB 调试安全、ADB 认证秘钥、增强型内核 SELinux/SEAndroid、SELinux 的启动与关闭、内核攻击与防护、Linux 可加载的内核模块、剖析内核模块、系统接口重定向、内核级 Rootkit 攻击位置、攻击内核剖析、隐藏潜伏模块、内核级 Rootkit 检测、Android Rootkit 检测系统模型、电话子系统攻击检测、Rootkit 的植入与启动等核心知识。

由于写作仓促，加上作者水平有限，书中难免存有不足之处，希望广大读者阅读后给出完善建议，Android 学习交流 QQ 群：341989536。编辑联系邮箱：zhangtao@ptpress.com.cn。

本书面向的读者

任何想要加深对 Android 安全认识的人都可以阅读本书，不管是软件开发者、嵌入式系统设计师、安全架构师，还是安全研究人员，本书都会帮助你拓宽对 Android 安全的理解。

目　录

第 1 章 Android 简介

近年来我们对“Android”这个词已经不再陌生。在过去的几年时间里，Android 的快速发展已经影响到了每个人的日常生活。如今 Android 不仅仅意味着一台手机、一部平板电脑，也可能是一台电视、一只手表、一部智能汽车、一副眼镜。然而，在一个生态系统形成的同时，总会有一群人希望通过一些不常规的手段谋取利益。

本章主要从 Android 黑色产业链与破解人员的动机来分析 Android 的安全问题。

1.1 Android 的发展历史

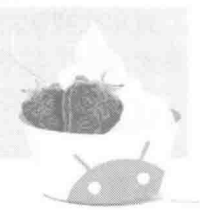
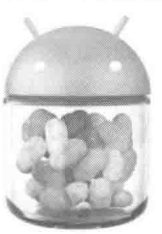
Android 是一种基于 Linux 的、开放源代码的操作系统，主要适用于移动设备，如智能手机和平板电脑等，Android 操作系统最初由 Andy Rubin 开发，主要支持手机。2005 年 8 月由 Google 收购注资。2007 年 11 月，Google 与 84 家硬件制造商、软件开发商及电信运营商组建开放手机联盟共同研发 Android 系统。随后，Google 以 Apache 开源许可证的授权方式，发布了 Android 的源代码。第一部 Android 智能手机发布于 2008 年 10 月。Android 逐渐扩展到平板电脑及其他领域上，如电视、数码相机、游戏机等。2011 年第一季度，Android 在全球的市场份额首次超过塞班系统，跃居全球第一。2013 年的第四季度，Android 平台手机的全球市场份额已经达到 78.1%。2013 年 9 月 24 日，Google 开发的操作系统 Android 迎来了 5 岁生日，全世界采用这款系统的设备数量已经达到 10 亿台。

1.2 Android 系统进化史

Android 系统一向以甜品名称为版本代号，而名称首字母是按照 ABCEFG 排序的。Android 1.5，它的代号是纸杯蛋糕（Cupcake），是 Android 正式步入市场的第一步。Android 2.3 是最经典的 Android 系统版本，至今仍占有很大份额。Android 4.x 是目前占据市场份额最大的版本。Android 5.0 发布之后，Android 已经向智能穿戴设备迈进了一大步。尤其是 Android 5.0 版本会强制开启 SELinux（Android 上又称为 SEAndroid），这是美国国家安全局推出的 Linux 史上最杰出的安全子系统，新设备也会默认自动开启加密。

表 1-1 显示了 Android 各版本的代号、发布时间和特性。

表 1-1　Android 操作系统的发展表

时间	版本	简介	Logo
2008 年 9 月	Android 1.1	Google 发布第一版 Android 系统，其拥有完整的应用商店，以及 HTML 网页浏览等功能	
2009 年 4 月	Android 1.5 Cupcake	Google 推出 Android 1.5，加入全新智能虚拟键盘、来电照片显示、复制/粘贴等功能	
2009 年 9 月	Android 1.6 Donut	Android 1.6 亮相，新增手势搜索、语音搜索应用集成、语音阅读等功能	
2009 年 10 月	Android 2.0/2.1 Eclair	Android 2.0 发布。2010 年 1 月，Android 2.1 优化了支持多分辨率显示、界面改进	
2010 年 5 月	Android 2.2 Froyo	Android 2.2 横空出世，支持 Flash 10.1、移动热点、多语言键盘等功能	
2010 年 12 月	Android 2.3 Gingerbread	Google 推出 Android 2.3，支持 NFC、原生视频聊天、全新商店、Google Music 等功能	
2011 年 2 月	Android 3.0 HoneyComb	Android 3.0 发布，专为平板优化，加入全新 Gmail 应用、Google Talk 等功能	
2011 年 10 月	Android 4.0 Icecream Sandwich	Android 4.0 提升了流畅度，支持虚拟按键替代物理按键，可在主界面建立文件夹	
2012 年	Android 4.1/4.2/4.3 Jelly Bean	Android 4.1/4.2 亮相，支持离线语音输入等功能。2013 年 7 月，Android 4.3 发布	

（续）

时间	版本	简介	LOGO
2013 年 9 月	Android 4.4 KitKat	Android 4.4 最低支持 512MB RAM 机型、无线打印、内置 Hangouts IM 和健身应用	
2014 年 10 月	Android 5.0 Lollipop	Material Design 设计风格，支持多种设备，改进安全性	

1.2.1 Nexus 系列

因为 Android 系统是 Google 出的，且 Nexus 手机也是 Google 的品牌，许多系统的更新我们只能在 Nexus 上看得到。图 1-1，就显示了 Google 近年来所推出的 Nexus 系列手机。

图 1-1 谷歌 Nexus 系列 Android 手机

1.2.2 国产定制系统

原本就很碎片化的 Android 系统，到了我国变得更碎片。从 ROM 到手机桌面，有许多个版本存在。

1.2.2.1　国产 ROM

在 Android 智能手机硬件大比拼的同时，Android 系统的开源也使得第三方定制 ROM 多种多样，给用户带来了多样化的体验。国产定制的 Android 系统有很多，每一个厂商都有自己的 ROM。

1.2.2.2　手机桌面

因为刷机的门槛比较高，而且会存在一定的风险，所以普通的用户在深受各种 ROM 骚扰下更喜欢的是装一个桌面。对于 Android 来说这其实就是一个 Launcher，一个系统的首屏的全套解决方案。因为其是一个入口级别的产品，所以各大商家也都推出了自己的桌面 App。但是，相对于手机 ROM 来说，手机桌面只能是用户首屏的一个整套解决方案，其安全优化与性能优化远不能和 ROM 相提并论。

1.2.3　Android 的开放与安全

“Android 不是为了安全设计的，它是为了开放而设计的”，这是 Google Android 业务掌门人 Sundar Pichai 在 MWC 大会上被问到“为什么 Android 上恶意软件泛滥”时做出的回应。Android 开放与安全的关系如图 1-2 所示。

图 1-2　Android 安全与开放关系图

这位 Google 高管表示，假如他是个恶意应用开发者的话，也会把 Android 作为首选平台。“我们不能保证 Android 是为了安全而设计的，它的设计目的是给用户提供更多的自由度。有人表示 90%的恶意软件都是针对 Android 平台的，他们忽略了这样一个事实，那就是 Android 现在是世界上最流行的系统。如果我有一家恶意软件开发公司，我也会选择攻击 Android 平台。”Pichai 说道。

确实，Google 一开始的战略就是希望 Android 变为最开放的操作系统，人们可以在上面任意地定制自己喜欢的东西。但这个并不意味着安全不重要，获得更高的安全性仍然是打造 Android 的初衷。Android 是一个开放的平台，很多人可以通过多种方式使用 Android，因此，就有一些合作伙伴制造了不同种类的 Android 设备。较早版本的 Android 操作系统会面临一些安全隐患，但并不表示 Android 本身不安全。GooglePlay 应用市场会从应用的生产源头，对数千个提交上架申请的应用进行扫描，以保证它不含有恶意程序。当然，只要用户的手机能够及时更新，那么 Android 操作系统会很安全。

虽然 Google 在 Android 的安全上也做了很多的改善与补救措施，但国内的很多 Google 服务是无法使用的，许多第三方应用商店监管不严，导致恶意软件泛滥的问题一直无法解决。

1.2.4　移动互联网的趋势

在网络技术迅猛发展的今天，各种移动终端层出不穷，大数据及云时代的到来更让网民大呼

网络发展快速。对于中国来说，移动互联网的时代已经完完全全的到来，移动设备的使用频率已经超过了 PC 端。正因为网民对移动互联网有如此大的需求，才能促进移动互联网的快速发展。对于移动互联网的明天，我们认为不应该仅仅是手机、Pad，而应该是涉及我们日常生活中的方方面面，如手表、衣服、眼镜等智能穿戴设备。移动互联网的发展趋势，应该会有以下几种特点。

- Android 将覆盖智能穿戴设备

移动互联网的发展也带动了智能穿戴设备的发展。如图 1-3 所示，手机、衣服、眼镜，甚至一些我们完全不敢想象的方向都会出现移动互联网的影子。

Android 的开源性以及其可定制性就会为各种嵌入式设备提供良好的系统环境支持，当然也会成为极客们针对智能穿戴设备设计使用的首选系统。

图 1-3 可穿戴式设备

- 手机将变为物联网的控制中心

从 2013 年开始，我们会发现虽然手机每年都会发布很多款，但是移动手持设备的创新与发展的脚步已经变得很慢了。因为大家都知道，目前的手机设备已经定型，希望在上面做更多的创新已经非常难了。更多的是制作其他的外置设备，如移动手环、手表，这些东西必须需要一个控制器或界面来承载它们的信息输入与输出，手机将会承载这一重要的职位。这也就造就了手机将会变为物联网的控制中心。

- 传统行业在移动互联网上将有突破

互联网快速聚集财富的能力让很多人加入其中。所以很多非互联网的传统行业当然也希望搭乘互联网的快车，尝到互联网带来的甜头。

- 移动开发将变得傻瓜化与复杂化

移动互联网的快速发展将会使得移动应用的开发供不应求，各类的跨平台与傻瓜式的开发平台将会出现，如拖曳式的编程、图形化的编程。开发一款 App 将不再是难事，任何一个人只要想学习 Android 应用程序开发都能够在几天之内学会。

当然，傻瓜似的工具并不能够真正地解决 Android 系统上存在的安全问题，对于底层安全以及设计架构上的需求必然会越来越大，这就使得移动开发将存在傻瓜化与复杂化并存的现象。

1.3 Android 和 iOS 系统对比

很多人喜欢拿 iOS 系统来与 Android 系统做比较。这是由于它俩是目前市面上最流行的手机操作系统。但是，我们只要从专业角度来看，会发现它们有许多不同点。

iOS 是由苹果公司开发的手持设备操作系统，最初是设计给 iPhone 使用的，后来陆续套用到 iPod touch、iPad 以及 Apple TV 等苹果产品上。它也是以 Darwin 为基础的，因此同样属于类 UNIX 的商业操作系统。

Android 是一种以 Linux 为基础的开放源码的操作系统，Android 操作系统最初由 Andy Rubin 开发，主要应用于手机平台。2005 年由 Google 收购注资，并和多家制造商组成开放手机联盟对其开发，逐渐扩展到平板电脑及其他领域上。至目前为止，Android 跃居全球最受欢迎的智能手机平台。

在便携式设备领域，iOS 和 Android 分别的优势和劣势也日益明显。

Android 采用的是 Java 技术，所有应用在 Dalvik 虚拟机中运行，Dalvik 是 Google 专门为移动设备优化的 Java 虚拟机。因此 Android 具有成熟、存在大量可重用代码的优点，也有占内存大、运行速度略低的缺点。

而 Apple iOS 的体系架构相对较为传统，但运行效率高，对硬件的要求低，成本优势大，在现有的硬件条件下，应用运行具有最好的顺畅感，也更加省电。系统架构朴实无华，但干净清晰，是目前最有效率的移动设备操作系统。

1.3.1　系统架构对比

表 1-2 就 Android 与 iOS 两个系统做了一个对比。

表 1-2　Android 与 iOS 系统对比表

对比项	Android	iOS
应用运行环境	运行在 Java 虚拟机（Dalvik）内	运行在原生系统上
应用收费标准	Google Play 上大部分可以免费获取 国内的市场都是免费的	App Store 上大部分需要付费（或者部分内容需要）
源码	开源	闭源
设备硬件要求	系统可以被匹配在各种不同类型设备	系统仅可以在平板和手机上使用
设备外设接口	可以兼容不同的外接设备	仅可兼容苹果认证的设备
设备价格	覆盖所有价格区间	专注高端市场
设备购买渠道	由各种厂商提供	仅由苹果公司提供

1.3.2　Android 和 iOS 安全对比

很多人都说，iOS 比 Android 安全，因为，Android 是开放性的，且 Android 系统的使用数量的基数大，即使系统漏洞的百分比再小，但是整体数量依然水涨船高。而 iOS 就个体而言，安全问题比较严重。由于整体数量、受众人群的关系，漏洞数还是无法赶超 Android。虽然 Android 漏洞数量居高不下，但是，必须透过现象看到数据安全的本质。

1.3.2.1　Android 系统安全性分析

其实，Android 的恶意应用比手机漏洞更可怕。而滋生恶意应用的土壤就是 Android 的开源性，由于应用的发布监管机制不够严格，很多应用的发布无需权威机构审核即可随意发布应用，而且很多应用都会申请一些与它本身功能并没有什么关系的系统权限。

再者，Android 存在各类第三方 App 碎片化问题，很多 App 开发者由于缺少审核机制，恶意软件开发商可以轻易地发布一些仿冒的产品，因此山寨应用在 Android 平台上层出不穷。有很多恶意产品甚至直接修改国内、外知名 App 产品，在其中增加恶意代码后便在论坛或某些软件商店发布。对于普通用户来说，分辨难度极大。

最后，Android 系统上的许多应用无需 Root 就能够替换掉一些系统的核心应用，诸如输入法、市场、通信录等。这类应用是最敏感的，它们能直接记录用户的隐私。不法分子通过山寨版的 App 轻易地就能获得用户的隐私信息，轻则做广告的个性化推荐，重则直接盗取。因此，开放就是一把双刃剑，把握不好则会伤到自己。

1.3.2.2 iOS 系统安全性分析

iOS 应用的审核上架是由苹果公司负责，应用的收益、支付、分成都有一套完整的体系。虽说审核周期较长，但从根本上杜绝了恶意、山寨应用的滋生。

除此之外，苹果对涉及系统核心层的应用都采取封闭的措施。禁止了第三方应用市场的使用，目前的第三方应用程序只能通过用户打开“开发者模式”才能安装到手机上（当然，这样安装的应用经常会出现闪退）。如果用户希望使用一些高权限的应用，如手机管家类的应用，则必须通过“越狱”后才能正常使用。

就因为这样，iOS 给广大用户留下了“比 Android 系统更安全”的印象。但是，无可否认苹果在杜绝恶意应用这一方面确实做得比 Android 出色，因为这些是导致系统不稳定的最大因素。但从客观的技术检测与架构上来看，iOS 系统本身也存在有不安全的因素。

第 2 章 Android 地下产业链分析

目前 Android 设备已经遍布全球，人们就会想着各种方法从这海量的用户里面捞取利益。创业者们会想着如何做出一款让大家都喜欢的、解决大家实际问题的 App；游戏开发商们想着如何让 Android 用户将自己的碎片时间都用在玩自己所开发的手机游戏上；手机制造商们想着如何让自己所生产的 Android 手机销量更好；而黑客们，却想着怎么样用自己的技术通过非正常手段获取利益。

如果你还认为黑客们的手段就是拨打欺诈电话、发送欺诈短信，那你就落伍了。黑客们攻击的手段层出不穷，有些手段你可能未曾听说，有些也许你已习以为常。本章就从 Android 黑色产业链的盈利模式开始，向读者解读为什么这么多人愿意冒着巨大的风险从事这“见不得光”的事业。

2.1 钱从哪里来

你们的盈利模式是什么？你们从哪里赚到钱的？这些都是人们对互联网行业的疑问，那就更别提黑客们怎么赚钱了。图 2-1 所示就是一个移动互联网行业地下盈利模式，从图 2-1 中可以发现，

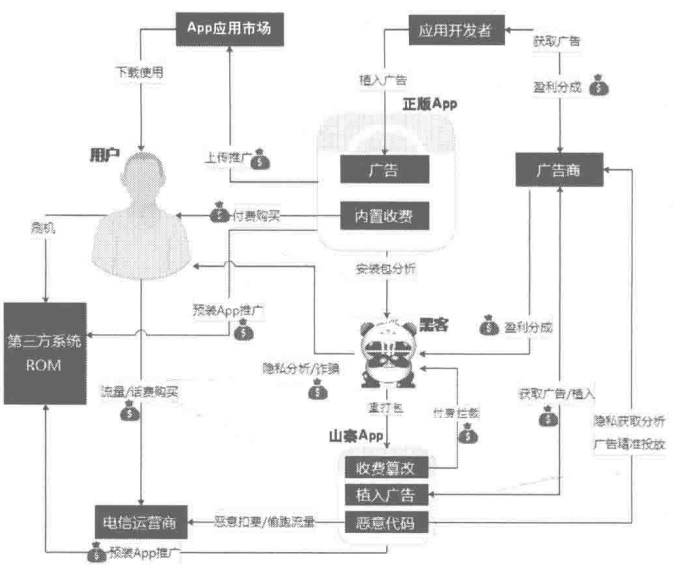


图 2-1 Android 地下产业链盈利图