TURING 图灵原创

丰生强/著

Android软件安全与逆向分析

国内第一本Android软件安全书

别让你的代码成为别人的炮灰！

eoe 全球最大中文Android开发者社区 (www.eoeandroid.com)

看雪论坛 (www.pediy.com)

安卓巴士 (www.apkbus.com)

联袂推荐

看雪版主非虫潜心力作

人民邮电出版社
POSTS & TELECOM PRESS

原创经典

TURING 图灵原创

Android 软件安全与逆向分析

丰生强 著

人民邮电出版社
北 京

图书在版编目（CIP）数据

Android软件安全与逆向分析 / 丰生强著. -- 北京：人民邮电出版社，2013.2(2013.3重印)
（图灵原创）
ISBN 978-7-115-30815-3

Ⅰ. ①A… Ⅱ. ①丰… Ⅲ. ①移动终端－应用程序－程序设计 Ⅳ. ①TN929.53

中国版本图书馆CIP数据核字(2013)第014823号

内 容 提 要

本书由浅入深、循序渐进地讲解了Android系统的软件安全、逆向分析与加密解密技术。包括Android软件逆向分析和系统安全方面的必备知识及概念、如何静态分析Android软件、如何动态调试Android软件、Android软件的破解与反破解技术的探讨，以及对典型Android病毒的全面剖析。

本书适合所有Android应用开发者、Android系统开发工程师、Android系统安全工作者阅读学习。

图灵原创

Android软件安全与逆向分析

◆ 著　　丰生强
策划编辑　陈　冰
责任编辑　傅志红

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：800×1000　1/16
印张：26.75
字数：632千字　　2013年2月第1版
印数：4 001－6 000册　　2013年3月北京第2次印刷

ISBN 978-7-115-30815-3

定价：69.00元

读者服务热线：(010)51095186转604　印装质量热线：(010)67129223
反盗版热线：(010)67171154

站在巨人的肩上

Standing on Shoulders of Giants

www.ituring.com.cn

推 荐 序

第一次看到生强的文章是在看雪安全论坛，他以“非虫”的笔名发表了几篇 Android 安全的文章。标题很低调，内容却极为丰富，逻辑清晰，实践性强，最重要的是很有“干货”。后来得知他在写书，一直保持关注，今日终于要出版了。

这本书的价值无疑是巨大的。

在此之前，即便我们把范围扩大到全球，也没有哪本书具体而系统地专门介绍 Android 逆向技术和安全分析技术。这可能有多方面的原因，但其中最重要的一点是竞争与利益。推动信息安全技术发展的，除了爱好者，大致可以分为三类：学术研究人员、企业研发人员、攻击者。

在 Android 安全方向，研究人员相对更为开放——许多团队开放了系统原型的源码，或者提供了可用的工具——但有时候他们也只发表论文以介绍系统设计和结果，却不公开可以复用的资源。近两年来，顶级会议对 Android 安全的研究颇为青睐，他们如此选择，可以理解。

在这个市场正高速增长的产业中，对企业而言，核心技术更是直接关系到产品的功能和性能，关系到企业竞争力和市场份额，许多企业会为了扩大技术影响而发布白皮书，但真正前沿的、独有的东西，极少会轻易公开。

攻击者则最为神秘，为了躲避风险，他们大都想尽一切办法隐藏自己的痕迹，低调以求生存。在地下产业链迅速形成后，对他们而言，安全技术更是非法获利的根本保障。

在这种情况下，刚刚进入或希望进入这一领域的人会发现，他们面临的是各种零散而不成体系的、质量参次不齐的、可能泛泛而谈的、也可能已经过时的技术资料，他们不得不去重复别人走过的路、犯别人犯过的错，将精力消耗在这些琐碎之中，而难以真正跟上技术的发展。

生强的这本书，无疑将大为改善这种局面，堪称破局之作。做到这一点颇为不易，这意味着大量的阅读、总结、尝试和创造。事实上，书中介绍的很多技术和知识，我此前从未在别的地方看到过。

另一方面，在 Android 这个平台，我们已经面临诸多的威胁。恶意代码数量呈指数增长，并且出现了多种对抗分析、检测、查杀的技术；应用软件和数字内容的版权不断遭到侵害，

软件破解、软件篡改、广告库修改和植入、恶意代码植入、应用内付费破解等普遍存在；应用软件本身的安全漏洞频繁出现在国内外互联网企业的产品中，数据泄露和账户被盗等潜在风险让人担忧；官方系统、第三方定制系统和预装软件的漏洞不断被发现，对系统安全与稳定产生极大的威胁；移动支付从概念逐步转为实践，而对通信技术的攻击、对算法和协议的攻击时常发生；移动设备正融入办公环境，但移动平台的攻击与 APT 攻击结合的趋势日益明显……更糟的是，随着地下产业链的不断成熟和扩大，以及攻击技术的不断发展和改进，这些威胁和相关攻击只会来势更凶。

毫无疑问，在 Android 安全上我们面临极大的挑战。在这个时候，生强的这本书起到的将是雪中送炭的作用。

安全技术几乎都是双刃剑，它们既能协助我们开发更有效的保护技术，也几乎必定会被攻击者学习和参考。这里的问题是，大量安全技术的首次大范围公开，是否会带来广泛的模仿和学习，从而引发更多的攻击？在这个问题上，安全界一直存在争议。1987 年出版的一本书中首次公布了感染式病毒的反汇编代码，引发大量模仿的新病毒出现。自此，这个问题成为每一本里程碑式的安全书籍都无法绕开的话题。我个人更喜欢的则是这样一个观点，在《信息安全工程》中，Ross Anderson 说："尽管一些恶意分子会从这样的书中获益，但他们大都已经知道了这些技巧，而好人们获得的收益会多得多。"

在生强写这本书的过程中，我们就不少细节有过交流和讨论。他的认真给我留下了非常深刻的印象。与其他的安全书籍相比，这本书在这样几个方面尤为突出：

实践性强。这本书的几乎每一个部分，都结合实际例子，一步步讲解如何操作。因此，它对刚入门的人或者想快速了解其中某个话题的人会有很大的帮助。事实上，缺乏可操作性，是 Android 安全方面现有论文、白皮书、技术文章和书籍最大的问题之一，很多人读到最后可能对内容有了一些概念，却不知道从何下手。但这本书则有很大不同。

时效性强。在交流中，我惊讶地发现，刚刚发布不久的 Santoku 虚拟机、APIMonitor 等工具，以及 Androguard 的新特性等，已经出现在了这本书中。这意味着，生强在一边写作的同时，还一边关注业界的最新进展，并做了学习、尝试和总结。因此，这本书将具有几乎和论文一样的时效性。

深度和广度适当。这本书涉及的面很广，实际上，仅仅是目录本身，就是一份极好的自学参考大纲。而其中最实用的那些话题，例如常见 C/C++代码结构的 ARM 目标程序反汇编特点，没有源码情况下对 Android 软件的调试技术等，都有深入的介绍。

此前，我曾写过一本叫 amatutor 的 Android 恶意代码分析教程，并通过网络分享，后来

由于时间和精力暂停了更新。这段经历让我尤其深刻地体会到在这样一个新的领域写出一本好书的不易。一直有人来信希望我能继续写，但自从了解到生强的这些工作，我就松了一口气，并向他们大力推荐这本书。同时，我也向周边的同事、同行推荐，我相信这本书的内容可以证明它的价值。

肖梓航（Claud）
安天实验室高级研究员
secmobi.com 创始人

看雪致序

移动平台逐渐成为人们上网的主要方式。随着 Android 应用的普及，安全问题日益突出。出于商业利益的考虑，Android 系统的所有者谷歌，一直回避公开讨论其安全性。国外用户一般是从谷歌应用商店下载应用，由于谷歌自身安全检测机制的保障，其安全性不太可能出现大的问题。但是，中国用户无法直接访问谷歌应用商店，大都是通过国内第三方 Android 市场下载应用，而谷歌无法控制第三方的应用商店。因此，国内的 Android 应用安全问题更加突出，安全威胁更高。

Lookout Mobile Security 移动杀毒软件公司预测：2013 年将有超过 1800 万台 Android 设备会遭遇某种形式的恶意软件的攻击。国内安全公司的数据也显示：流氓推广、恶意扣费、窃取用户数据等恶意软件增长迅速，危害日益严重。在黑色产业链中，骇客通过技术手段将非法 SP 提供的扣费号段植入到应用中，实现恶意吸费。手机骇客的攻击目标正在瞄准用户的手机支付与消费行为。为了更好地防范恶意软件和骇客带来的威胁，最好的办法是了解他们的攻击方法和工具，建立技术壁垒。

目前市场上研究 Android 安全相关问题的图书很少。因此当我拿到看雪论坛 Android 安全版版主“非虫”（丰生强）先生的倾力之作《Android 软件安全与逆向分析》的书稿时非常高兴，并认真通读了全文。我感到这是一本深入浅出、可以快速提升开发者 Android 安全技术水平的好书，其在注重实际操作讲解的同时，还特别重视一些原理的讲解，如 Dalvik 虚拟机与 Java 虚拟机的比较、APK 加载机理等内容。

据我所知，丰先生以前多年从事 Java 相关软件的开发，并对 Android 系统的全部源代码进行过深入的研究和分析，他有着很强的 Android 应用开发能力，尤其在安全相关专业领域经验丰富。他能够在繁忙的工作之余，耗费大量的时间和精力为读者呈现这样一部技术专著，并顺利出版，不仅是读者的幸运，也是看雪论坛的骄傲。在此，我对他表示由衷地祝贺，并期盼他今后为读者带来更多的技术成果和更大的惊喜。

段钢

看雪安全网站站长

www.pediy.com

2013 年 1 月 15 日于北京

前　言

近几年，Android 在国内的发展极其迅猛，这除了相关产品强大的功能与丰富的应用外，更是因为它优良的性能表现吸引着用户。2011 年可谓是 Android 的风光年，从手机生产商到应用开发者都纷纷捧场，短短几个月的时间，Android 在国内红遍了大街小巷，截止到 2012 年的第一个季度，Android 在国内的市场份额就超过 60%，将曾经风靡一时的塞班系统远远的甩在了身后，与此同时，它也带动了国内移动互联网行业的发展，创造了更多就业的岗位，国内 IT 人士为之雀跃欢呼。

随着 Android 在国内的兴起，基于 Android 的平台应用需求也越来越复杂。形形色色的软件壮大了 Android 市场，也丰富了我们的生产生活，越来越多的人从起初的尝试到享受再到依赖，沉浸在 Android 的神奇海洋中。事情有利也总有弊，即使 Android 如此优秀也会有怨声载道的时候，各种信息泄露、恶意扣费、系统被破坏的事件也屡见不鲜，Android 系统的安全也逐渐成为人们所关注的话题。

如今市场上讲解 Android 开发的书籍已经有很多了，从应用软件开发层到系统底层的研究均丰富涵盖，其中不乏一些经典之作，然而遗憾的是，分析 Android 软件及系统安全的书籍却一本也没有，而且相关的中文资料也非常匮乏，这使得普通用户以及大多数 Android 应用开发者对系统的安全防护及软件本身没有一个全面理性的认识。因此，笔者决定将自身的实际经验整理，编写为本书。

内容导读

本书主要从软件安全和系统安全两个方面讲解 Android 平台存在的攻击与防范方法。

第 1 章和第 2 章主要介绍 Android 分析环境的搭建与 Android 程序的分析方法。

第 3 章详细介绍了 Dalvik VM 汇编语言，它是 Android 平台上进行安全分析工作的基础知识，读者只有掌握了这部分内容才能顺利地学习后面的章节。

第 4 章介绍了 Android 平台的可执行文件，它是 Android 软件得以运行的基石，我们大多数的分析工作都是基于它，因此这部分内容必须掌握。

第 5 章起正式开始了对 Android 程序的分析，对这部分的理解与运用完全是建立在前面

章节的基础之上。这一章详细讲述了Android软件的各种反汇编代码特征，以及可供使用的分析工具，如何合理搭配使用它们是这章需要学习的重点。

第6章主要讲解ARM汇编语言的基础知识，在这一章中，会对ARM汇编指令集做一个简要的介绍，为下一章的学习做铺垫。

第7章是本书的一个高级部分，主要介绍了基于ARM架构的Android原生程序的特点以及分析它们的方法，读者需要在这一章中仔细的体会并实践，鉴于此类程序目前在市场上比较流行，读者在阅读时需要多进行实践操作，多动手分析这类代码，加强自己的逆向分析能力。

第8章介绍了Android平台上软件的动态调试技术，动态调试与静态分析是逆向分析程序时的两大主要技术手段，各有着优缺点，通过动态调试可以让你看到软件运行到某一点时程序的状态，对了解程序执行流程有很大的帮助。

第9章详细介绍了Android平台软件的破解方法。主要分析了目前市场上一些常见的Android程序保护方法，分析它们的保护效果以及介绍如何对它们进行破解，通过对本章的学习，读者会对Android平台上的软件安全有一种“恍然大悟”的感觉。

第10章介绍了在面对软件可能被破解的情况下，如何加强Android平台软件的保护，内容与第9章是对立的，只有同时掌握了攻与防，才能将软件安全真正地掌握到位。

第11章从系统安全的角度出发，分析了Android系统中不同环节可能存在的安全隐患，同时介绍了面对这些安全问题时，如何做出相应的保护措施。另外，本章的部分小节还从开发人员的角度出发，讲解不安全代码对系统造成的危害，读者在掌握这部分内容后，编写代码的安全意识会明显提高。

第12章采用病毒实战分析的方式，将前面所学的知识全面展示并加以应用，让读者能彻底地掌握分析Android程序的方法。本章的内容详实、知识涵盖范围广，读者完全掌握本章内容后，以后动手分析Android程序时，便能够信手拈来。

为了使读者对文中所讲述的内容有深刻的认识，并且在阅读时避免感到乏味，书中的内容不会涉及太多的基础理论知识，而更多的是采用动手实践的方式进行讲解，所以在阅读本书前假定读者已经掌握了Android程序开发所必备的基础知识，如果读者还不具备这些基础知识的话，请先打好基础后再阅读本书。

适合的读者

本书适合以下读者：

Android应用开发者、Android系统开发工程师、Android系统安全工作者。

本书约定

为了使书中讲述的知识更加容易理解，思路更加清晰，本书做了如下约定：

- 本书在讲解部分内容时，可能会对Android系统与内核的源码加以引用，如文中无具体说明系统版本，则统一为Android 4.1的系统，Linux 3.4的内核。
- 本书不介绍Android系统源码的下载方法，假定读者已经自行下载好了Android系统源码。
- 本书在引用Android系统源码时，为了避免代码占用过多篇幅及影响主体的分析思路，在不影响理解的情况下，对摘抄的内容进行了适量的删减。
- 本书在列举实例代码时，为了方便读者阅读与理解，对代码中的关键部分采用加粗显示。
- 本书中在给出命令的格式用法时，为了醒目起见，采用斜体显示。
- 对于部分操作容易发生错误或理解上造成歧义的地方，本书会在下面加上文本框注解。如：

注意　Smali代码的语法与格式会在本书第3章进行详细介绍。

本书源代码

下载地址：

http://www.ituring.com.cn/book/1131

点击“随书下载”即可看到本书源代码的下载链接。

本书正文中提到的“随书的附图x”也一并打包在源代码中。

致谢

首先，要感谢本书的编辑陈冰先生。在编写本书时，陈冰先生对书中每个章节的细节都严格把关，并多次耐心地教导我写作的技巧，是他对书稿质量的严格要求，以及对工作的一丝不苟，才使得本书得以顺序出版。

感谢我的父母，是他们养育了我，给了我生命，他们永远是我心中最伟大的人。

写作本身是一件很辛苦的事，尤其是每天还要被生活中的琐事困扰。在这里，我要感谢

这半年多来对我无言支持的大哥与大嫂，大嫂可口的饭菜补充了我每天写作所需的营养，而大哥更是帮助我解决了很多烦心的琐事，让我在写作时无后顾之忧。

好书总能给人带来心灵上的震撼。感谢美女作家李沉嫣，是她那扣人心弦的文字感染了我，给了我创作的最初源动力。

感谢那些共享 Android 安全技术的组织与个人，如果没有他们前期的奉献，笔者现在可能还处在独自探索的阶段，不可能有机会与大家分享如此前沿的技术。

看雪学院是国内最具权威性的软件安全研究论坛。感谢看雪学院站长段钢先生对本书内容上的肯定与支持。

最后，感谢那些关注本书、为本书提过意见的朋友，你们的支持是我写作本书最大的动力。

作者：丰生强

2012 年 11 月 2 日

编辑的话

每一本书的诞生，都有让人记住的事情。在这本书的出版中，我印象深刻的是三点：

一，作者丰生强在第一次给我交来样稿时，其粗糙不规范的写书格式和读起来不是那么顺溜的语言表达让我囧了一下，我耐心地（也或许是有些耐着性子的？）在QQ上边截图边详细地告诉了他有哪些地方的格式被他忽略了，有哪些地方的话说得不够清楚。

我说完后，他说他会认真修改好后再次给我发来。但说实话，我心里没指望他第一次就能把格式给改好，因为对于第一次写书的作者来说，这种情况几乎不曾出现过。我做了继续指导第3、4次的心理准备。让我没想到的是，几天后他第二次交来的稿件就相当靓仔，让我多少有些不相信自己的眼睛，格式规范美观，语言流畅清楚，很难相信这是同一个人仅相隔几天后的作品。他跟我说他是一个字一个字地来阅读和修改每句话的。

二，他是很少的按时且保质保量完成书稿的。对于作者，不管水平高低，大多都擅长干一件事情——拖稿，而策划编辑不得不被迫干另一件事情——催稿。但丰生强以实际行动打破了这一魔咒，他努力工作，在合同规定的期限内按时交来了全稿。作为对作者拖稿见怪不怪的一名策划编辑来说，纵然不至于说是老泪纵横吧，那也是感触良多啊。

但从另一角度说，那些能完全视合同交稿期限为无物的作者也着实让人不敢小觑，这得有多强大的心理素质才能做到这一点呢，就这么心平气和地跨过了最后期限。真心让人纠结。

三，在整个写作过程中，在谈及技术时，丰生强所表现出的那些热情、专注和乐观。我一直信奉的一点是，如果一个作者不能在他所钻研的领域体会到乐趣和幸福，那这样的作者写出来的东西是不值得一读的。好的内容就像好的食材，而那份热情和乐趣则是烹饪的手法。

现在，书已经打开，希望你会喜欢。

本书策划编辑 陈冰

2013年1月15日

目　录