TURING 图灵程序设计丛书

에이콘

Android恶意代码分析与渗透测试

【韩】赵涎元 等 / 著　金圣武 / 译　OWASP子明 / 审校

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

TURING 图灵程序设计丛书

Android恶意代码分析与渗透测试

【韩】赵涎元 等 / 著　金圣武 / 译　OWASP子明 / 审校

人民邮电出版社
北　京

图书在版编目（CIP）数据

Android恶意代码分析与渗透测试 /（韩）赵涎元等著 ；金圣武译. -- 北京 ：人民邮电出版社，2015.7
（图灵程序设计丛书）
ISBN 978-7-115-39593-1

Ⅰ. ①A… Ⅱ. ①赵… ②金… 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131406号

内 容 提 要

本书详细讲解了Android恶意代码的散播渠道，并针对开发者和用户介绍如何应对此类威胁。还从分析人员的角度出发，通过渗透测试方法查看如何对应用程序进行迂回攻击以获得敏感信息。这些都是安全咨询人员或安全负责人可以直接应用的诊断方法。

◆ 著　　[韩] 赵涎元 等
译　　金圣武
审　　校　OWASP子明
责任编辑　傅志红
执行编辑　陈　曦
责任印制　杨林杰

◆ 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
三河市海波印务有限公司印刷

◆ 开本：800×1000　1/16
印张：23.5
字数：555千字　　2015年7月第1版
印数：1－4 000册　　2015年7月河北第1次印刷
著作权合同登记号　图字：01-2014-5451号

定价：79.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第0021号

版权声明

推 荐 语

从业多年，我读过很多关于恶意代码分析的书籍。但是有关Android环境下的恶意代码分析，国内目前只有一本韩国的引进图书，也就是这本《Android恶意代码分析与渗透测试》。

本书完全从专业的技术手段进行分析，开始先讲原理——包括环境的搭建——接着通过具体的示例进行了详实的分析处理。最难能可贵的是，无论是安全方面的爱好者还是专业人员，都能参考本书。书中内容由浅入深，即使是刚刚从事分析工作的开发人员都可以轻松上手。诸多案例和第5章、第6章的多种专业工具都能手把手教会你如何分析，希望更多专业人士通过这本书进行系统化的学习。本书同时也可作为国际信息安全比赛移动分析部分的参考书，因为书中对每道试题都有十分具体的讲解。

应图灵公司之邀负责本书的审校工作，我感到非常荣幸。书中多次提及OWASP在移动安全开源方面的巨大贡献，作为“OWASP中国”的负责人之一，我向那些对Android环境下的恶意代码分析和研究感兴趣的人员强烈推荐本书。

OWASP子明

“OWASP中国”负责人、“知道创宇”信息安全培训负责人

作 者 序

赵涎元

不知不觉间，我们已经进入“移动设备就是必需品”的时代。除了工作或是编辑文档之外，我都通过移动设备搜索信息、管理网站、利用SNS与人联系。如今，移动服务的使用时间已经超过了PC台式机的使用时间。我们上下班途中或等人时，甚至和别人在一起的时候，手里也会拿着移动设备。可以说，人们现在的上网时间比以前翻了一倍。

针对台式机，特别是针对Windows用户的恶意代码攻击一直有增无减。经常访问的网站会突然变成恶意代码的宿主，在用户未能察觉的时候就感染到电脑，我们只能信任自己安装的杀毒软件。移动设备也暴露在同样的危险之中。众所周知，移动设备里保存的个人信息（公共认证书、照片、自动保存的服务账户信息等）比台式机里的更多，所以那些攻击者乐此不疲地向移动设备的用户发送大量恶意代码。每当出现重大的社会事件时，他们也会不知廉耻地利用这些新闻发送恶意代码。

韩国国内90%以上的移动设备用户都是Android系统用户，为了获取这些用户的信息，黑客们正在不分昼夜地进行研究。我们必须比这些人做更多研究以找出应对方案。

本书将详细讲解此类恶意代码会通过何种渠道散播，并针对开发者和用户介绍如何应对此类威胁。还会从分析人员的角度出发，通过渗透测试检验方法查看如何对应用程序进行迂回攻击以获得敏感信息。这些都是安全咨询人员或安全负责人可以直接应用的诊断方法。

我为写作本书付出了很多时间与努力。如果没有共同编写的同伴，我根本不可能完成这本书，非常感谢为了目标一直勇往直前的所有安全防范项目组成员。也非常感谢编写此书时一直在旁边为我加油的妻子金慧珍和儿子昊永，我爱你们。

朴炳旭

随着越来越多的用户开始使用Android系统的智能手机，一些不怀好意的人趁机对普通用户大肆实施短信诈骗，我也从这时起对Android恶意代码分析产生了兴趣。我现在也经常收到一些钓鱼短信，收到后并不立即删除，而是开始分析研究Android恶意代码，以了解恶意代码是怎样运行的。虽然刚开始有些辛苦，但随着分析的深入，逐步了解恶意代码的运行过程和损害用户利益的方法时，就好像拼图一样有趣。

目前也有很多人开始对Android系统的恶意代码分析和诊断感兴趣，想开始学习。为了让各

位也能像我一样从Android恶意代码分析中得到乐趣，本书包含了很多相关内容。

虽然书中没有收录所有Android恶意代码分析诊断相关内容，但已经包含了大量极为重要而核心的话题，希望能够指导各位的学习。

抚今追昔，这已经是我第三次写书了。虽然写作时感到艰难困苦，但是拿到成果时的兴奋真的无法言表。

感谢身边的家人和朋友，正因为有你们的不断支持，我才能体会这种难以言说的喜悦。

南大铉

这是我第一次写作者序，还生疏得很。虽然为技术杂志投过几次稿，但身为技术员，我感到写文章给别人看还是有些困难。

写这篇文章的时候我在想："读者能轻松理解我写的内容吗？"不记得从哪里听过（读过）："如果不能用一句话表达你想说的内容，那就说明你不了解这件事情。"我尽量用通俗易懂的表达方式对需要具体说明的地方展开了详细论述，但"这种程度应该都能理解吧"的想法也让我跳过了某些地方。当然，并不是所有人都能看懂全部内容。

移动环境已经占据了我们大部分的生活，也变成了一个重要的部分。无论怎样，我都希望自己写的内容能对学习移动恶意代码和移动安全的读者提供一点帮助。

感谢像亲人一样关心安全防范项目组成员的赵涎元先生，是他成就了今天的我。也感谢经常帮助我的江俊茂大哥和我深爱的妻子安正珠。

金衡范

2009年底，韩国国内引进了iPhone，之后的移动市场开始急速发展。无论男女老少，无论地铁、公共汽车、卫生间、办公室等何种环境，随时随地都可以利用无线接入网络。网民可以用移动设备使用银行服务、购买商品等，也有了越来越多使用移动设备处理公司业务的BYOD（Bring Your Own Device，自带移动设备）族。

高效与便捷使移动设备相关市场在短时间内急速增长，也因此暴露了很多安全漏洞。特别是Android系统，因为是开放性操作系统，所以变成了黑客的"游戏"平台。因此，国内外也提出了很多应对方案。OWASP（国际Web标准机构）也发表了"OWASP Mobile Top 10"安全威胁。

移动安全渐渐成为关注热点，我也对移动安全诊断产生了兴趣，并开始搜集资料学习相关技术。我怀着当时的热情和成员们一起编写了这本书，希望它能使更多人轻松进入移动分析和诊断领域。

本书的重点内容——恶意代码分析不仅能满足对该领域感兴趣的读者的要求，而且能提高对操作系统的了解，也可以通过渗透测试掌握Android漏洞诊断的概念。

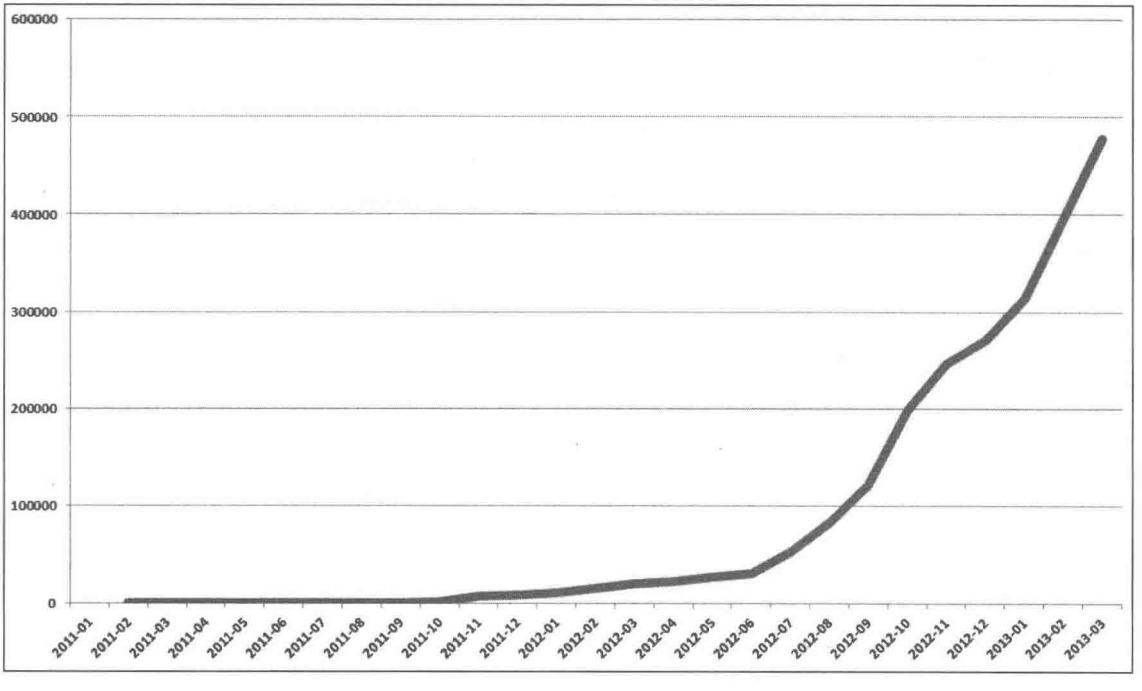
本书能使恶意软件分析的初学者体会到学习的乐趣，也会激发各位的热情。最后，感谢赵涎元先生和安全防范项目组允许我参与本书的编写工作。

前　言

韩国国内移动设备的普及时间并不长，但韩国网速极快，没几年时间，所有人都在使用智能手机。技术的发展需要以所有领域的高度发展为基础，而且要经过足够长的过程，但是过快的移动终端普及速度引发了移动领域的很多安全隐患。

移动终端的网络使用率已经超过了PC台式机的使用率，越来越多的个人信息安全问题得到关注。在PC端出现过的种种安全问题，也同样出现在了移动终端。

通过智能手机和平板电脑的普及，2013年的全球移动恶意代码比2012年增加了423%，特别在智能终端市场占有率非常高的Android系统中呈现增长趋势。每天新增的移动恶意代码数量也开始超过PC端。针对不熟悉手机操作人群的短信诈骗活动在日益增加，造成的损失也在不断扩大。



Android恶意代码增长示意图（2011年～2013年）（参考：安博士研究所（AhnLab）移动恶意代码统计资料）

与PC一样，移动设备也不能只依赖杀毒软件。新出现的恶意代码越来越智能，用户可以随时选择安装Android应用程序，所以只能自行防范恶意代码引发的威胁。

本书将讨论Android恶意代码的分析环境、分析方法、预防方法等所有领域，反映了截稿时[①]的所有最新信息，努力向有兴趣分析Android恶意代码的入门者和管理员提供更多信息。希望各位能通过学习本书有效应对恶意代码引发的威胁。

读者对象

本书面向移动安全分析领域的入门者和一线技术人员，同时适合以下读者。

- 想学习移动恶意代码分析技术的读者
- 想学习移动入侵/安全诊断工具的读者
- 想全面了解移动安全威胁的读者
- 想理解并实际运用移动服务诊断方法的读者

本书特色

近几年，移动应用发展迅猛，几乎覆盖了社会生活的方方面面，其安全性也越来越受到重视。本书从专业分析人员角度详细阐述了Android恶意代码的散播渠道及其引发的威胁，并从实战层面介绍了代码的分析环境、分析方法、预防方法等，读者不仅能通过渗透测试检验方法掌握Android漏洞诊断的基本概念，还可在多个项目中获得可直接运用于实际业务的技术和流程。

本书结构

本书面向关注Android移动安全威胁的读者，由“恶意代码分析”和“移动服务诊断”两大主题组成。各章节包含了分析步骤，作者们还亲自编写了黑客大赛应用程序试题，读者可以借此复习学过的内容。

各章节内容如下。

- **第1章 Android的基本概念**：介绍Android的基本概念。构建恶意代码分析环境前，把握Android的整体概念和结构。本书重点不在于Android开发，所以只讲解必要的部分。只有掌握了基本概念，才能理解后面要讲解的分析阶段。
- **第2章 Android应用程序诊断环境**：介绍Android分析环境的构建方法。分析恶意代码或移动应用程序服务时，需要构建Android开发环境。谷歌提供了Android SDK、NDK等工具包，以及完美支持Java应用程序开发工具的诊断环境。详细介绍了分析所需工具及其使用方法。
- **第3章 Android App分析方法**：介绍诊断Android恶意代码应用程序或漏洞时必须掌握的分析方法。第3章内容会用于第4章、第5章和第7章，必须熟练掌握。

① 原书出版于2014年5月29日。——编者注

- **第4章　恶意代码分析**：本书亮点之一，详细介绍分析恶意代码时使用的在线分析服务及其意义、手动分析步骤等。希望读者能在介绍的多种操作方法中选择适合自己的方法。
- **第5章　Android移动服务诊断**：介绍诊断Android移动应用程序服务的方法。通过测试应用程序详细讲解可应用于实际业务的方法，以OWASP提供的标准为基础，展示各种诊断方法和相应的应对方案。
- **第6章　使用Android诊断工具**：介绍分析Android应用程序时用到的其他重要工具。通过数据包分析、漏洞分析、开源框架诊断工具等内容全面了解诊断方法。
- **第7章　Android黑客大赛App试题**：介绍Android黑客大赛的试题解析，以复习之前通过Android恶意代码分析与诊断而掌握的技术和工具。黑客大赛出现了很多移动应用程序诊断试题，想参加黑客大赛的读者也会获得有用的信息。

注意事项

本书写作目的在于，为想了解移动安全威胁的读者和想从事分析工作的入门者提供帮助。书中详细描述了如何在本地电脑搭建测试环境。严禁利用这些工具非法入侵未获授权的服务，由此产生的所有法律责任均由实施者本人承担。

目　录

第1章
Android 的基本概念

开始分析前，先通过本章简单了解一下Android的基本概念。很多开发相关书籍都涉及了Android概念，所以本书只会提及一些必要的内容。本书重点不是内核区域，而会针对恶意代码分析和应用程序诊断，从应用程序和服务角度进行说明。

1.1 Android 的架构

Android是由Android Inc.开发的基于Linux平台的操作系统。谷歌公司收购后对其进行了修改，使其更适合在智能手机、平板电脑、相机、机顶盒等触屏设备上运行。使用Android系统的用户在不断增加，韩国国内80%以上的用户都在使用Android系统。越来越多的人关注Android系统的同时，相应的安全威胁也呈现增长趋势。

学习Android应用程序的基本结构前，先简单了解一下Android的系统架构。本书不会逐一讲解系统架构，只简单介绍不同区域。图1-1是很多文档中常见的Android系统架构。

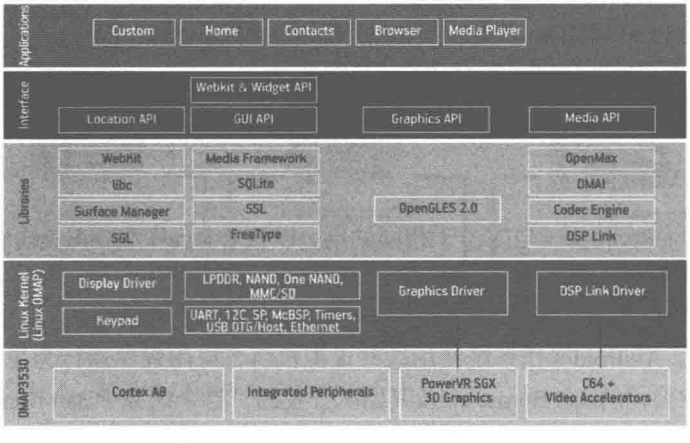


图1-1 Android系统架构

（出处：http://www.techdesignforums.com/practice/technique/android-for-the-rest-of-us）

1.1.1　Linux 内核

最底层由Linux内核构成。Android系统以部分结构微调后的Linux 2.6内核版本为基础，该层由相机、声卡、Wi-Fi、键盘等多种驱动程序构成。Android的安全、内存管理、进程管理、网络协议栈、驱动模型等主要系统服务都依赖于Linux。内核会在硬件和软件栈的剩余部分起到抽象层的作用。

用户在应用程序启动后运行的Windows或Linux等传统平台上工作。例如，用户安装并运行软件时，软件的执行权限与用户权限相同。假如该软件是恶意软件，其访问或窃取用户计算机中的敏感信息时，都会得到操作系统的许可。因为Windows和Linux都会在相同的用户权限下运行所有进程。

1.1.2　库

Linux内核的上层是Android的本地库，这些库是用C/C++语言编写的。库会使用Android系统的多个组件，通过Android应用程序框架（库的上层）展示给程序员。这些库也会在Linux内核中以进程方式运行。

库只是告知设备多种数据处理方式的命令集合。比如，媒体库支持录制或播放音频、视频格式。一部分重要的库如下表所示。

库	说　明
系统C库	嵌入式Linux设备专用，是继承了BSD而实现的标准C库
SQLite	可在所有应用程序中存储数据。虽然小，但是一个功能强大的关系型数据库引擎（渗透测试时可用于查看数据库中的所有敏感数据）
WebKit	提供网页检索工具的浏览器引擎（渗透测试时用于查看所有敏感页面缓存）
Surface Manager	负责设备屏幕上的图形图像
OpenGL	在屏幕上绘制2D或3D图形图像
媒体库	播放或录制音频、视频格式（mp3、mpeg4、jpg、png等）
3D库	基于OpenGL API，是硬件3D加速软件
SGL	支持2D图形图像

1.1.3　Android 运行时

Android运行时（Runtime）与库位于相同的层，以核心Java库和Dalvik构成。核心Java库用于开发Android应用程序。

众所周知，虚拟机是拥有操作系统的虚拟环境。Android使用Dalvik虚拟机概念，这样可以有效运行多个虚拟机。Android操作系统使用这些虚拟机将各应用程序运行为自己的进程。

Dalvik是由谷歌公司的Ban Bornstrein及其团队开发的，这个词源于Ban Bornstrein的祖先居住的一个冰岛村庄。Dalvik虚拟机的构建过程与JVM（Java Virtual Machine，Java虚拟机）类似，但前者使用Dex编译器进行转换，生成位元码后运行，如图1-2所示。这是考虑到当时的移动环境而设计的

性能，也是因为被Sun公司的Open Java（Open JDK和Apache Harmoney项目）替代了的缘故。

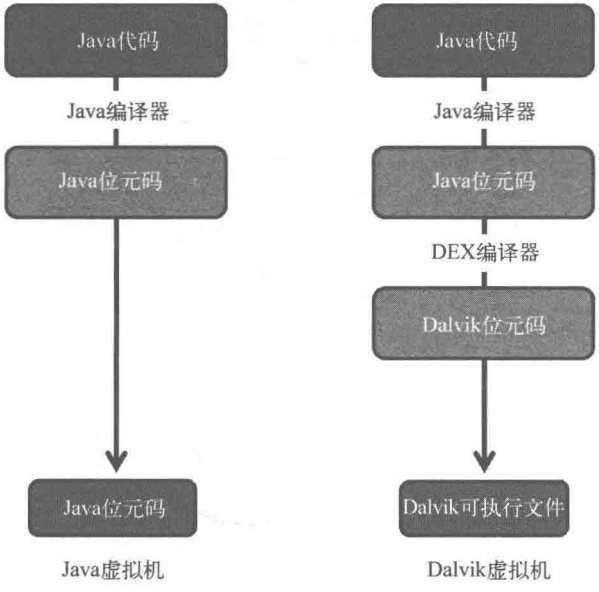


图1-2 Java VM与Dalvik VM的区别

Dalvik虚拟机的主要特点如下。

- 优化内存管理。
- 各应用程序未授权时不可干涉其他应用程序。
- 支持threading。

图1-3以图片形式表示Android环境。各Android应用程序在各自的虚拟实例中运行，每个应用程序会获得分配好的固定用户ID。

图1-3 赋予各应用程序固定的用户ID（出处：Google Market）

从图1-4可以看到设备中安装的工具包，并能看到以app_为前缀赋予了用户ID。简言之，就是每个进程都有一个Linux用户。

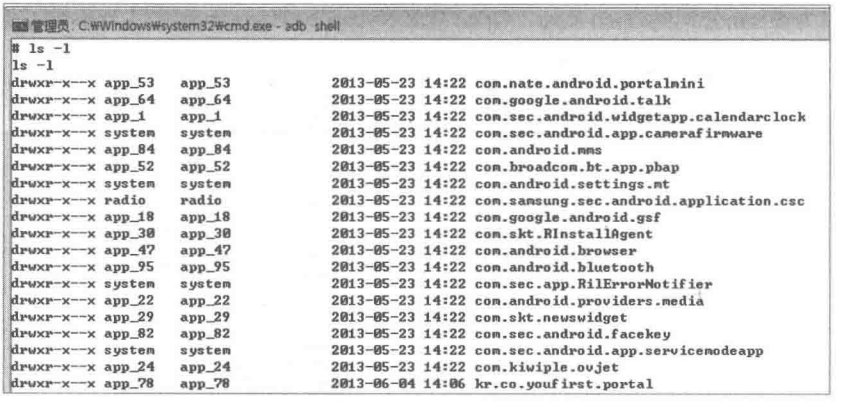


图1-4　赋予各应用程序固定的用户ID：在设备中查看

输入ps命令查看进程信息时，可以看到最左侧每个进程持有的用户权限。

```
# ps | more
... (略) ...
system    271   200    261244 70524 ffffffff afd0b7ec S system_server
system    354   200    152524 31240 ffffffff afd0c63c S com.android.systemui
system    362   200    147524 21920 ffffffff afd0c63c S
com.samsung.sec.android.inputmethod.axt9
radio     366   200    159304 25128 ffffffff afd0c63c S com.android.phone
app_22    367   200    155084 20816 ffffffff afd0c63c S android.process.media
bluetooth 375   200    135844 16056 ffffffff afd0c63c S com.broadcom.bt.app.system
app_1     382   200    210036 50772 ffffffff afd0c63c S com.sec.android.app.
twlauncher
app_18    427   200    207524 26392 ffffffff afd0c63c S com.google.process.gapps
app_1     439   200    142628 19428 ffffffff afd0c63c S android.process.acore
system    447   200    147540 25404 ffffffff afd0c63c S com.android.settings
app_40    477   200    137076 16700 ffffffff afd0c63c S com.sec.android.
provider.badge
app_1     486   200    135976 16076 ffffffff afd0c63c S
com.sec.android.provider.logsprovider
system    510   200    135940 15436 ffffffff afd0c63c S com.android.server.
vpn:remote
... (略) ...
```

1.1.4　应用程序与框架

库之上的层是应用程序框架，包含资源分配、语音通话等管理智能手机基本功能的程序。程序员使用此框架API开发更加复杂的应用程序。

该框架的一部分重要的“块”管理资源管理器，谷歌地图和GPS等定位服务、应用程序生命周期的Activity管理、语音通话管理、应用程序之间共享的数据管理内容提供商等均属此类。

栈的最上层是应用程序。与邮件地址、SMS账户、地图、浏览器等通过Android市场开发并发布的应用程序一样，也包含随Android系统一起提供的应用程序。