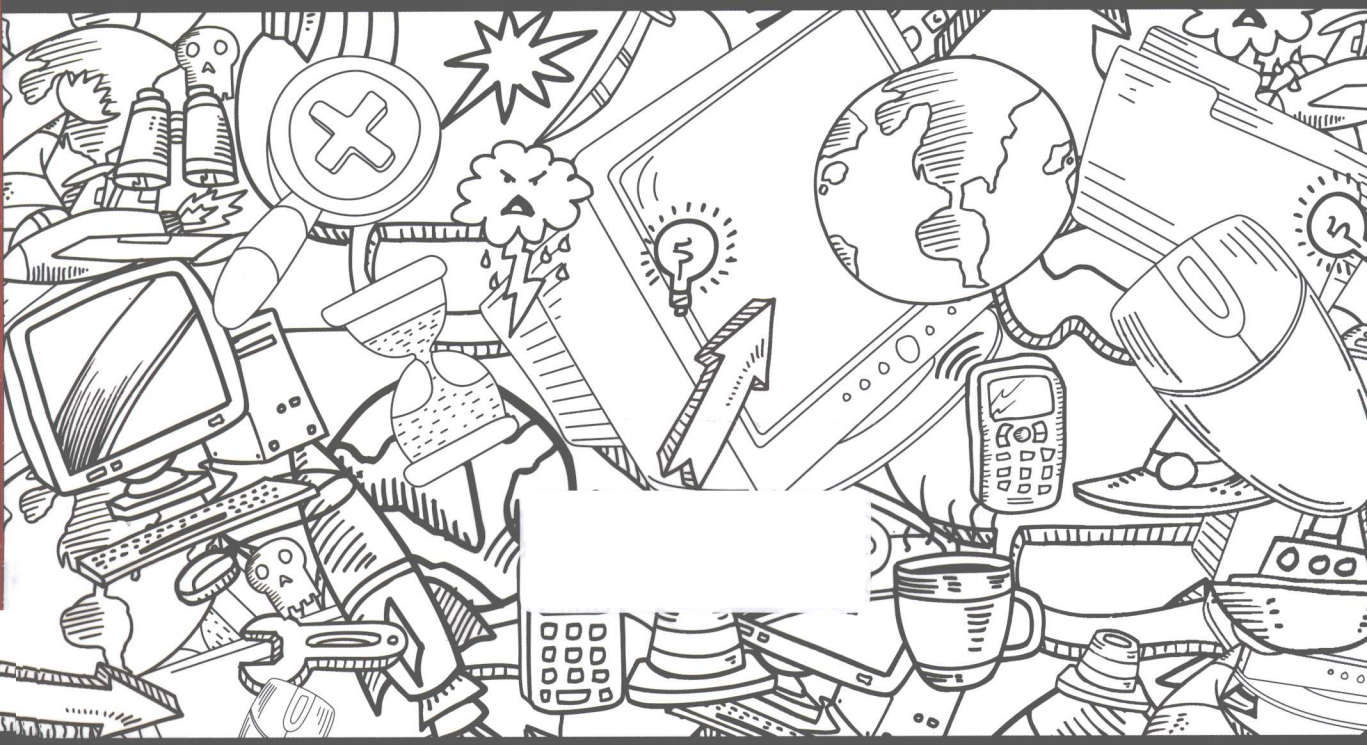
Broadview
www.broadview.com.cn

[PACKT] open source
PUBLISHING

安全技术大系

谷歌应用名人堂大牛手把手教会你Android安全攻防技术！

Android 安全攻防实战



Android Security Cookbook

[南非] Keith Makan
[英] Scott Alexander-Bown 著

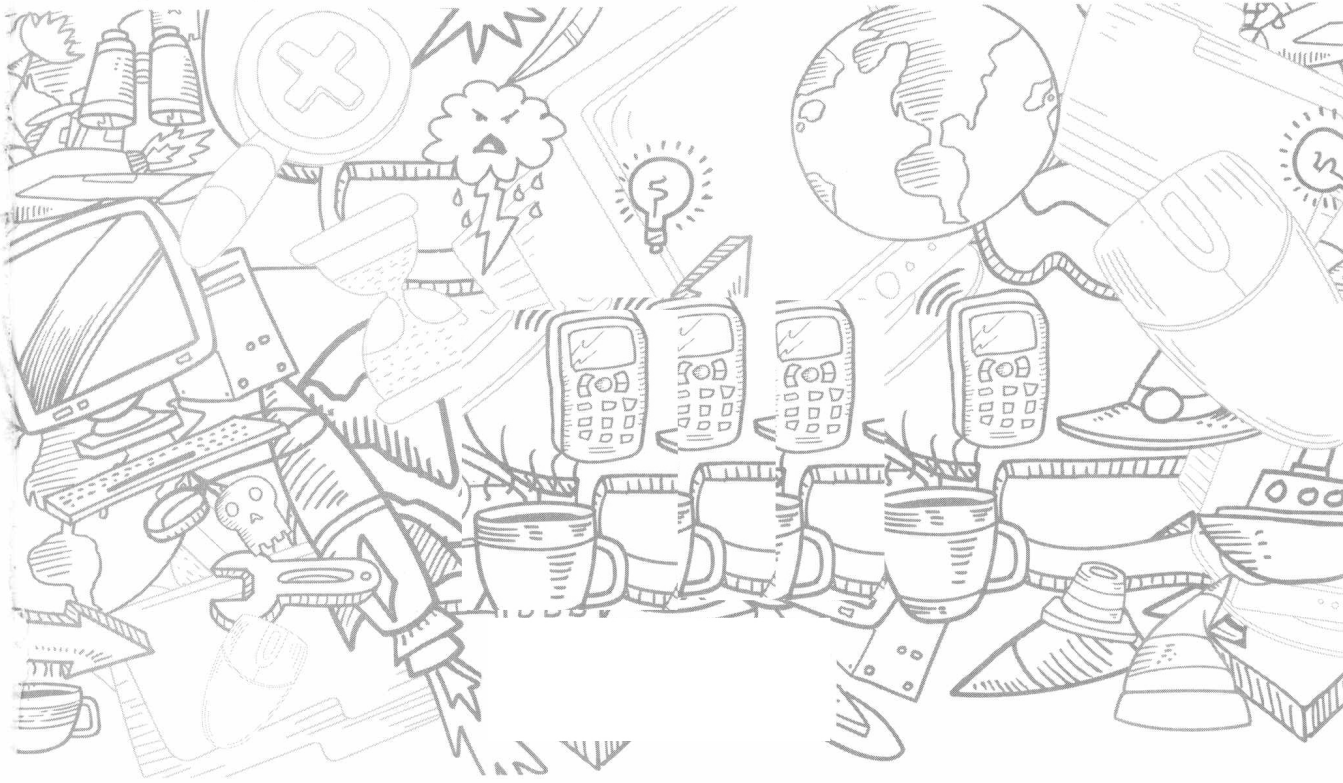
崔孝晨 武晓音 译

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

Android 安全攻防实战



Android Security Cookbook

[南非] Keith Makan
[英] Scott Alexander-Bown 著

崔孝晨 武晓音 译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

Android 是目前最为主流的移动设备操作系统，占据了全球近 84%的市场份额。因此，Android 系统中的安全问题也就变得十分重要。

本书通过大量极富针对性的实验，通过对常见的安全场景中解决方案的讲解，帮助读者全面掌握各种攻-防实用技能。因而，本书的实用性也很强，即使是一时不能完全理解其中的技术原理的新手，根据作者给出的方法，也能解决实践中遇到的大部分问题；而高手也能从中借鉴到一些好的做法。

全书共分九章，涵盖了基本的 Android 开发环境和工具；app 组件之间及它们与系统的交互方式；Android 安全评估框架“drozer”；app 及 Android 原生代码的逆向技巧；各类漏洞的利用及防护方式；使用 SSL 在网络通信中进行更有效的验证；利用第三方代码库或 Android 中新增的特性，通过加密和在开发时使用设备管理策略，加固 app 等内容。

《Android 安全攻防实战》寓教于练，可供安全技术研究人员，软件开发人员，电子取证人员学习使用，对于各类高等院校中网络安全相关专业的师生也有较高的参考价值。

版权贸易合同登记号　图字：01-2014-8378

图书在版编目（CIP）数据

Android 安全攻防实战 /（南非）麦凯恩（Makan,K.），（英）鲍恩（Bown,S.A.）著；崔孝晨，武晓音译. —北京：电子工业出版社，2015.7
（安全技术大系）
书名原文：Android Security Cookbook
ISBN 978-7-121-26107-7

Ⅰ. ①A… Ⅱ. ①麦… ②鲍… ③崔… ④武… 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(2015)第 105458 号

策划编辑：刘　皎
责任编辑：徐津平
特约编辑：顾慧芳
印　　刷：北京京师印务有限公司
装　　订：北京京师印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×980　1/16　印张：20　字数：392 千字
版　　次：2015 年 7 月第 1 版
印　　次：2015 年 7 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

推荐序

想做一名优秀的英文技术资料译者实属不易，除了要有深厚的英文功底，还需要对所翻译的技术领域有深入的了解，同时还要译者有博大分享之心和躬耕不辍之志。拜读了小崔的最新译作《Android 安全攻防实战》后，我更是由衷地感到他对技术与文字的把握已相当娴熟，能受邀为其新作做一推荐也令我甚感荣幸。

我与小崔初识于 2003 年，彼时他尚在从事电子取证及数据鉴定领域的工作且颇具造诣，待到后来 Team509 成立，我们便成为了莫逆之交。当时团队的成员各有所长，但小崔一直是最勤奋的一员，其勤奋不仅仅在于对技术孜孜不倦的追求，也在于其不吝花费时间翻译大量的英文技术资料并乐于分享。想来他优秀的翻译功底便是那时练就的吧。之后，他翻译的“大部头”作品便陆续问世，且一部好过一部。

如今，这部新作的推出与当下的移动领域技术潮流匹配得恰到好处，本书可以作为初学者熟悉 Android 系统攻防的快速入门教程，其中的大量操作实例也可以为高手们提供一些值得借鉴的做法。此书的翻译忠实原意，对原著的意思把握得十分准确，语言生动活泼，令人读起来十分愉快。希望读者能够喜欢，并从中受益。

赵泽光

2014 和 2015 届 Pwn2own 黑客大赛 winner，Team509 创始人之一

* Pwn2own 是全球公认级别最高的黑客大赛

2015 年 5 月

译者序

这是一本 Android 安全的实训教材，你甚至可以把它当成参加一次专家手把手的专题培训！

自从 Android 操作系统成为移动平台上的两大主流操作系统之一后，Android 系统的安全性就受到了广泛的关注，确实也出版过几本 Android 安全方面专著，但是这些著作实在是太高大上了一些，一般都是要从高深的原理讲起，吓跑了许多对它感兴趣的爱好者。即使有人硬着头皮看下去，也如坠云里雾里，短期内无法把学到的知识，融会贯通地运用到实践中去。更别提那些只是不想让自己的代码沦为别人的“炮灰”的程序员了，他们确实学到了一些黑客知识，但是面对这些攻击时，又该怎样防护自己编写的代码呢？

本书的英文原名为《Android security cookbook》。其中的单词“cookbook”是“菜谱”的意思，也就是在给定场景下，如何进行操作的操作指南。顾名思义，书中的内容也就是针对典型的 Android 安全攻-防场景，通过实验来说明 Android 安全技术原理的。利用这种教学方法，能使学员快速上手，通过相对简短的培训，解决大部分实践中可能遇到的问题。由于本书同时也计划作为我校“网络安全与执法”专业“移动平台安全”课程的实训教材，所以我将书名直接译为《Android 安全实验教程》。

实用性是本书最大的特色。除了常规工具外，作者还介绍了开源的 Android 安全评估框架“drozer”，利用这个工具，你不仅可以“敲一、两个命令”就能完成以前要花很大代价才能搞定的活。有经验的安全研究人员还能为自己定制开发一些针对特定问题的插件，让自己活得更滋润些。而且，由于这个框架能够暴露出 Android app 内部实现的许多细节，随着你越来越熟练的掌握这一工具，你对 Android 的理解也一定会越来越深入。

对于想要寻找代码加固方案的程序员来说，本书中更是针对常见的攻击方法，提供了详细且极富操作性的代码加固建议，其中不光有系统中自带的库或新增的特性的使用方法，也介绍了不少开源的库，通过对它们的使用，能把你的软件的安全性提高到一个新的级别。

本书的作者也不是光说不练的嘴把式，他们都是 Android 安全圈中的大牛，作者 Keith Makan 就是多个 0day 漏洞的发现者，数次入选谷歌应用安全名人堂（Google Application Security Hall of Fame）；而作者 Scott Alexander-Bown 也是移动 app 开发、逆向和加固方面的专家，在多个国际会议上做过演讲。

单词“application”在书中，既是指用 Java 语言编写的 Android 应用，也指使用 Android NDK 编写的原生（native）应用程序，显然，在翻译时，将它们不加区分的全部译为“应用”或“应用程序”是不合适的。为了表示其中的区别，在翻译中，我们将用 Java 语言编写的 Android 应用一律译为“Android app”，而用 Android NDK 编写的原生应用程序则全部译为“应用”。

全书由上海公安高等专科学校的教师教官翻译完成的，全书共九章，分工安排如下：

第一至第四章由武晓音同志翻译，第五至第九章由我翻译。全书翻译完成后由我统一审校。

本书中文版的面世，特别要感谢博文视点的各位编辑老师，特别是顾慧芳、刘皎老师，感谢你们对我的一贯支持和耐心的指导，使我从中获益良多！同时也感谢你们为本书的出版所花费的大量时间！此外，也要感谢 Team509 安全研究小组的朋友们在本书翻译时给予的宝贵建议！

由于翻译时间仓促，书中存在错误在所难免，敬请读者不吝指正。

崔孝晨

2015 年 2 月

前　言

Android 已经快速地成为了最主流的移动操作系统之一——这不光是对用户而言，也是对开发者和所有类型的公司而言的。当然也正是因为这个原因，它也成了恶意敌手眼里的一块肥肉。

自从 2005 年进入公众视线时起，Android 在功能和复杂性上都有了长足的进展。移动智能手机中一般都存有其使用者的非常敏感的信息，而且还能访问他们的电子邮件、短消息，以及公共网络和专门网络的服务。就像其他所有软件一样，在功能和复杂性增长的同时，也会增加安全风险。软件越强大，越复杂，人们就得越努力地应对和适应险恶的大千世界。

这一点还特别适用于移动智能手机上的软件。这些存放私人信息和隐私信息的温床，必然存在于我们十分关心的一个安全的上下文环境中，同时，我们也要在这一环境中解决问题。从一方面看，移动智能手机的安全上下文环境，与网上的或“云”中的服务器中的安全上下文环境是截然不同的。因为究其本质而言，网上的或“云”中的服务器是不会移动的。它们不会被轻易地搬走或偷走。我们可以同时强制执行软件的和物理的防护措施保护它们，使之未经许可就不能被访问。我们也可以一直监视它们，并及时响应各个安全应急事件。但是对于我们经常放在口袋或手提包里，带着到处跑，还会被落在出租车里的设备来说，游戏规则就完全变了。

Android 的用户和开发者需要持续关注他们的移动安全风险，而正是因为这一原因，对移动安全和风险评估专家和安全工程师的需求也一直是很旺盛的。本书致力于降低成为 Android 安全评估专家之初的学习难度，并希望成为经验丰富的 Android 安全专业人士手中的工具，帮助他们解决常见的 Android 安全问题。

本书的内容

第 1 章“Android 开发工具”介绍了安装和运行开发者用来编写 Android app 和

Android 平台上的原生级组件的工具。这一章也为那些想要了解如何搭建常用的 Android 开发环境和相关工具的新手做了一个大致的介绍。

第 2 章“实践 app 安全”介绍了 Android 操作系统提供的，专门用来保护 app 的组件。这一章里将讨论：（对 app 的）手工检查和一些用来保护 app 的安全相关的工具和服务的使用方法，以及用它们与操作系统交互的方法。

第 3 章“Android 安全评估工具”介绍了一些主流（新的或即将发布的）安全工具和框架，Android 安全专业人士可以用它们来评估 app 暴露给用户的技术风险。在这一章里，你将学到如何安装、运行和扩展本书之后的这些章节中会使用到的黑客和逆向工程工具的功能。

第 4 章“利用 app 中的漏洞”介绍了针对 Android app 的目的漏洞利用技术的框架。这一章的内容涵盖了所有类型的 Android app 组件，从源码和 app 间上下文关系的角度，详述了如何检查这些组件的安全风险。另外，这一章里还将介绍在第 3 章“Android 安全评估工具”中介绍的工具的一些高级用法。

第 5 章“保护 app”的写作目的与第 4 章“利用 app 中的漏洞”的目的是完全相反的。这一章并不光讨论 app 中的漏洞，也讨论如何修补它们。它将引领读者学习那些开发者能够用来保护他们的 app，免受第 4 章“利用 app 中的漏洞”中详细描述的一些攻击危害的，有用的技术。

第 6 章“逆向 app”帮助读者学习如何破解 app 并教授他们 Android 逆向工程师用来检查和分析 app 时所使用的技术。你将会非常详细地学到 Dex 文件的格式，以及如何把 Dex 字节码解析成易于进行逆向工程的更有用的表示形式。这一章里也会介绍一些逆向工程师用来动态分析 app 和运行在 Android 操作系统上原生组件的新奇的方法。

第 7 章“网络安全”帮助读者深入研究一些 app 开发者能用来保护他们通过网络传输数据的实用方法。使用这些技术，你可以在安全套接字层（Secure Sockets Layer，SSL）通信中添加更有效的验证。

第 8 章“原生代码中漏洞的利用与分析”专门用来讨论关于 Android 平台上原生可执行程序的安全评估和测试技术。读者将会学到怎样去寻找能用于 root 手机和在 Android 系统中提权的安全漏洞——那些能用来对原生服务进行包括内存溢出攻击和利用竞争条件漏洞在内的底层攻击的漏洞。

第 9 章“加密与在开发时使用设备管理策略”将专注于如何正确地使用加密技术和避免一些常见的错误做法，以保护你的 app 中数据的安全。这一章中将给你使用

几个健壮的，帮助你节省开发时间的第三方库，来快速且安全地加固你的 app 的安全性的建议。为了使讨论内容完整，我们还将介绍如何使用 Android 设备管理 API，来实现和强制执行企业安全策略。

阅读本书时所需的软件

虽然，在阅读本书时需要使用一些软件，但是在本书的许多实验里，在真正下载和用这些软件做实验之前，都讨论了下载和安装它们的方法。

话虽如此，但在开始做实验之前，你可能还是最好先准备好下列软件：

- The Android Software Development Kit (SDK)；
- The Android Native Development Kit (NDK)；
- GNU C/C++ 编译器(GCC)；
- GNU 调试器(GDB)；
- Python，最好是 2.7，3.0 可能有时会无法正常工作；
- Virtual box；
- Ettercap (for Windows 版的或 Linux/UNIX 版的)；
- Dex2Jar；
- Objdump；
- Radamsa；
- JD-GUI；
- The Java Development Kit (JDK)；
- drozer，一个 Android 安全评估框架；
- OpenSSL 命令行工具；
- keytool 命令行工具。

这本书是写给谁的

本书中有些章节是专门用来讨论如何利用 Android app 中漏洞的，而另一些章节则讨论如何加固它们。本书的目标是：同时展示硬币的两面——攻击和防御。

安全研究人员，分析师和渗透测试人员会喜欢如何利用 Android app 中漏洞的部分。而想要学习更多安全方面知识的 app 开发者，将会从保护 app 免受攻击危害的部分中获得切实可行的建议。

字体风格约定

在这本书中，你会看到一些不同排版风格的文字——这些不同的排版风格是用来

区分各类不同的信息的。下面是一些排版风格的样例及对其所表示的意思的解释。

文字中的“代码字体”的部分，表示数据库中表的名字、目录名、文件名、文件扩展名、路径、URL 和用户的输入。比如：“上一步中你选中的系统镜像的 ID 可以用-t 参数来指定”。

代码块是像下面这样表示的：

```
from drozer import android
from drozer.modules import common, Module
class AttackSurface(Module,common.Filters, common.PackageManager):
```

如果我们希望你注意代码块中的某些部分，那么相关的行或语句就会被加粗：

```
from drozer import android
from drozer.modules import common, Module
class AttackSurface(Module,common.Filters, common.PackageManager):
```

命令行窗口中的输入或输出，则被表示成这样：

```
sudo aptitude update //如果你已经装好了 aptitude
```

第一次出现的术语和**重要的单词**会被加粗。在正文中，你会在屏幕上，菜单栏或对话框中看见的文字，也会像这样出现：“当你同意了用户许可协议之后，你可以单击“**安装**”按钮，收集你的文档和 API”。

警告或重要的提示会出现在这样的地方。

小窍门或小技巧会这样显示。

读者反馈

我们总是欢迎你——亲爱的读者提出宝贵的意见。请让我们知道你对本书的看法——无论你喜欢还是不喜欢。反馈意见对我们今后出版你真正最需要的东西是非常重要的。

如果只是一般的意见，请给 feedback@packtpub.com 发送电子邮件，并在主题中注明书名即可。

如果你对某个主题特别有研究，或者你有兴趣写一本书或投稿，请移步我们的作者指南页面 www.packtpub.com/authors。

售后服务

你现在已经是尊贵的 Packt book 的客户了。我们愿意为你的购买提供全面的服务，使你获得更多东西。

下载示例代码

你可以在网站 http://www.packtpub.com 你的账户中，下载所有你已经购买了的 Packt books 的示例代码。无论你是在哪里购买这本书的，你都可以用你的电子邮箱注册一个账号，访问 http://www.packtpub.com/support 页面。

勘误

尽管我们已经非常仔细地校对了稿件，但错误仍然是不可避免的。如果你在我们的书中发现了错误——不论是文字，还是代码错误——都请告诉我们，我们将感激不尽。这样做，你不仅可以帮助其他读者免受错误的困扰，也能帮助我们改进这本书后续版本的质量。如果你发现了任何错误。请访问 http://www.packtpub.com/submit-errata 网页，选中你的书籍，单击“**errata submission form**”链接，并输入你发现的错误的详细信息，把它告诉我们。一旦你报告的错误被确认之后，你的意见将会被接受，该错误也会被发布在我们的网站上，或被添加到一张该书籍的勘误表中。在 http://www.packtpub.com/support 网站中选中您的书目，就能看到所有目前已知的错误。

版权

互联网上，可复制媒体的版权保护问题是个一直困扰着所有媒体的问题。在 Packt，我们是非常严肃地对待版权保护和用户许可协议问题的。如果你在网上发现任何非法复制我们的书籍的情况——无论是以何种形式，请立即通过我们公司的地址或网站联系我们，以便我们采取补救措施。

请通过邮箱 copyright@packtpub.com 联系我们，并附上疑似盗版材料的链接。

我们感谢你为保护我们的作品而提供的帮助，并且我们也将尽我们的所能，向你提供物质回馈。

疑难解答

如果你对本书的任何方面有所疑问，请通过邮箱 questions@packtpub.com 联系我们，我们将尽力去解决它。

作者简介

Keith Makan

以前他是计算机科学和物理学专业的学生，现在是狂热的业余爱好者和安全研究员。他把绝大多数业余时间都用在了阅读源码、逆向工程、fuzz 测试和编写 Web 应用技术中的相关漏洞的利用代码上。

Keith 工作起来就像是一个 IT 安全评估专家一样专业。他的个人研究已经使他多次入选“谷歌应用安全名人堂”（Google Application Security Hall of Fame）。他还编写了谷歌 Chrome 的 WebKit XSSAuditor，火狐浏览器的 NoScript 插件中漏洞的利用代码。此外，他还数次报告了 WordPress 插件中的漏洞，并写出了相应的利用工具。

我要感谢我的妈妈、爸爸以及其他支持我疯狂的想法，并总是给我极大鼓励的家人们。

Scott Alexander-Bown

他是一名在金融服务，软件开发和移动 app 客户端开发方面有着丰富经验的研发高手。他一直沉湎于 Android 之中，热爱移动 app 安全。

Scott 目前是一位高级开发人员，专长于移动 app 的开发、逆向工程以及 app 加固。他也热衷于发表与 app 安全相关的演讲，活跃在多个国际移动 app 开发者大会上。

最重要的，我要感谢我的妻子 Ruth，没有你的爱和鼓励，我将一事无成。我爱我们的儿子 Jake，他的笑声和可爱的笑脸是我前行的动力。

此外，我还要感谢以下诸公：

Keith, Barbara，Kirk Bown，Mhairi 和 Robert Alexander ，感谢你们给予我的爱和支持。

Andrew Hoog 和 viaForensics 小组的成员，感谢你们在移动安全领域的支持、洞察力和经验。

Mark Murphy, Nikolay Elenkov, Daniel Abraham, Eric Lafortune, Roberto Tyley, Yanick Fratantonio, Moxie Marlinspike, the Guardian Project 和 the Android 安全团队，你们博客中的文章、论文、演示和/或示例代码对于学习 Android 安全是很有趣且非常有用的。

感谢 Keith Makan 的热心和指导，在你的带领下，我才能完成本书的编写。

感谢本书的各位技术审校对细节的关注和极具价值的反馈意见。最后，感谢您——亲爱的读者——我希望，您能从本书中获益，并由此写出更安全的 app。

审稿人简介

Miguel Catalan Bañuls 是一名年轻的工程师，他唯一的梦想是希望自己的努力能为世界的改变做出贡献。他是一名软件开发人员，也是一名团队的带头人。

他拥有工业工程学士学位，是 Geeky Theory 的合伙人。他还是 Miguel Hernandez 大学（西班牙分校）的 IEEE 学生分会的副会长。

我想感谢我的妻子与父母，感谢他们对于我工作的理解与宽容。

Seyton Bradford 是一名在移动设备安全和取证上有着超过 10 年经验的软件开发人员和工程师。

目前，他在 viaForensics 任高级软件工程师，主攻 app 和移动设备的安全性。

他的作品在全球各地均有出版，同时还是多部学术期刊的评审。

感谢我的家人及朋友对我事业与工作的支持。

Nick Glynn 目前受聘担任技术培训师和顾问，在英国和世界各地提供关于 Android、Python 和 Linux 的课程和专业知识。他在许多领域，无论是主板启动代码、Linux 驱动程序开发和系统开发，还是全栈部署、Web 应用程序开发，以及 Linux 和 Android 平台的安全强化，都拥有丰富的经验。

我要感谢我家人给我的爱，感谢我漂亮的宝贝女儿，是你照亮了我的生活。

Rui Gonçalo 就读于葡萄牙布拉加的 Minho 大学，他现在正在完成 Android 安全领域的硕士论文。他正在开发一项新功能，旨在使用户能以非常细的粒度，控制互联网连接。他对移动安全的浓厚兴趣源于大学里“密码学”和“信息系统安全”这

两门课程，在几次有关的活动中他得到了这一领域里葡萄牙最重要的公司的支持。他建议渴望成为安全领域专家的 Android 安全初学者把这本书作为必读书目。

我要感谢 Packt 出版社负责此书的工作人员，是你们让我完全相信，对移动安全的研究会占满我对探索软件世界的所有好奇心。

Elliot Long 从小在硅谷长大，2005 年起就编写了多个移动 app。他是移动旅游线路生成软件 mycitymate SL/GmbH 的共同创始人。2009 他加入了 Intohand 有限公司，负责 Android 和黑莓开发。

目　录