Android
应用程序安全

【美】Pragati Ogal Rai 著
秦双夏 罗平章 李远明 译

Android Application
Security Essentials

清华大学出版社

Android 应用程序安全

[美] Pragati Ogal Rai 著

秦双夏 罗平章 李远明 译

清华大学出版社

北 京

内 容 简 介

本书详细阐述了与 Android 移动应用程序安全相关的基本解决方案，主要包括 Android 安全模型、应用程序构建块、权限、定义应用程序的策略文件、加密 API、应用程序数据安全、Android 在企业的运用、安全测试等内容。此外，本书还提供了相应的示例、代码，以帮助读者进一步理解相关方案的实现过程。

本书适合作为高等院校计算机及相关专业的教材和教学参考书，也可作为相关开发人员的自学教材和参考手册。

北京市版权局著作权合同登记号 图字：01-2016-1656

图书在版编目（CIP）数据

Android 应用程序安全/（美）普拉加蒂·欧加尔·拉伊（Pragati Ogal Rai）著；秦双夏，罗平章，李远明译. —北京：清华大学出版社，2016
书名原文：Android Application Security Essentials
ISBN 978-7-302-43984-4

I. ①A… II. ①普… ②秦… ③罗… ④李… 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（2016）第 121882 号

责任编辑：钟志芳
封面设计：刘　超
版式设计：魏　远
责任校对：王　云
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　张**：10.75　　**字　　数**：221 千字
版　　次：2016 年 6 月第 1 版　　**印　　次**：2016 年 6 月第1 次印刷
印　　数：1～3000
定　　价：49.00 元

产品编号：061190-01

译 者 序

2009 年，世界上第一部 Android 手机诞生并搭载了 Android 系统。Android 系统是一个多用户、多任务、开源的操作系统，这极大地激发了开发者对基于 Android 系统应用的创新实践能力，同时，开源也带来了一些安全方面的问题。

本书结合实际操作的例子、图表和日常使用情况，深入研究从内核级到应用程序级的 Android 安全，并向读者展示如何保护 Android 应用程序和数据安全。通过本书，作者向读者展示了 Android 堆的整体安全架构，利用权限、安全加密等方法保护应用程序组件，让读者和开发者在今后的应用程序开发中，加强安全意识，保护应用程序和数据安全。

本书是一本较为全面的介绍从内核级到应用程序级，从 Android 安全模型、应用程序构建、权限、定义应用程序策略文件到保护用户隐私、加密算法等方面 Android 安全的书。读者在开发和编写应用程序时，可将本书作为参考。

本书的翻译由秦双夏组织完成，参与本书翻译的还有罗平章、李远明、吴骅、杨莉灵、王学昌、周娟、刘红军、王玲、郑正正、莫鸿强等，感谢这些同行。由于水平有限，译文中的不当之处在所难免，恳请同行及各位读者朋友不吝赐教。

译 者

序　言

20 世纪世纪 90 年代初，作者刚开始在 GO 公司工作时，当时最先进的移动计算机是一个 8 磅重、尺寸如剪贴板大小的设备，它的电池寿命极短，可以配备 9600 波特的调制解调器。不过，驱动这种设备的设想如今可以在最新安卓和 iOS 设备上很轻易地被实现：即期望拥有一种综合的、以任务为中心的无缝对接的计算平台。而在当时，我们认为这一设想将是拥有“从沙滩给某个人发送传真”的能力。后来，在 AOL 开发 AIM 过程当中（即时通信客户端服务，作为 iPhone App Store 2008 年首发软件之一），这一设想已逐渐成为了现实。但即便在那个时候（也就在几年前），我们当时也不可能预测到这些设备和其催生的应用程序生态系统会对我们的日常生活产生何等巨大的影响。

如今，移动设备无处不在。它们为我们提供娱乐，帮助我们打发闲暇时光；当然，也帮助我们保持联系（通过收发传真保持联系也许不常用）。由 Google 推出的 Android 操作系统是这一革新背后的推动力之一，这一操作系统已被数以百计的设备供应商所采用，并安装在全球近十亿的设备上。但是，随着这些移动设备遍及我们生活的方方面面，保持设备和其用户的安全就变得至关重要。这正是本书如此重要的所在。

相比移动设备，病毒、木马和恶意软件可能还是更流行于桌面平台环境。但手机市场的增长意味着恶意软件的大幅上涨，反病毒厂商 Kaspersky 报告每个月检测到数以千计的新程序。今天的智能手机和平板电脑对于潜在的攻击者而言，等同于一个不可抗拒的蜜罐，个人信息、财务数据、密码和社交图谱，甚至是最新的位置定位数据，对于消费者而言这些设备的一切宝贵之处也成为恶作剧和数据窃贼的诱人目标。作为开发人员，管理好用户信息是应有的责任。Android 系统的开放性和集成性意味着我们每个人要各尽其责以确保应用程序和服务的安全，这一点尤为重要。

安全不能只当作可有可无的选项，或进行事后弥补。它必须成为程序设计的一部分，始终贯穿应用程序的执行过程。我相信本书作者 Pragati Ogal Rai 必定深谙此理，因为她从操作系统和应用程序开发者两个角度解决过安全问题，所以正是撰写此书的不二人选。她能总览 Android 系统全局（从设备到内核，再到应用程序），并提出清晰可行的操作步骤，供开发人员依循，以保护应用程序和数据的安全。同时，作者亦提供源代码作为使用的示例，以及测试其有效性的方法。此外，作者并不局限于比特和字节的基础层面，进一步探索能平衡开发者使用个人信息和用户保护个人信息两种愿望的安全策略和最佳做法。

功能强大的移动设备与无处不在的社交媒体相结合，具有传输、存储和消费大量数据的能力，在论及手机安全性时这给每个人增加了风险。但是，安全就像我们所呼吸的空气，直到它消失我们才会真正去考虑并重视这一问题，而到那时往往为时已晚，来不及保护我们的用户，来不及保护开发者的声誉和业务。因此，对于每一位 Android 开发者而言，了解在这复杂多变的境况下保护用户安全所扮演的角色是极其重要的。

作为开发人员和用户，我很感激本书作者 Pragati 耗费时间写出一本如此全面而翔实的指导书籍帮助我们通行于网络空间中，我很希望她的经验教训能使各地的 Android 开发者们提供我们所渴望的迷人创新的应用程序，同时维护保障我们期待并应得的安全和信任。

Edwin Aoki
PayPal 技术研究员

作 者 简 介

Pragati Ogal Rai 是一位在移动操作系统、移动安全、移动支付和移动商务领域里拥有超过 14 年经验的技术专家，从 Motorola Mobility 平台安全工程师，到 PayPal 移动服务的设计和开发，她在移动技术的方方面面皆拥有广泛的经验。

Pragati 拥有计算机科学的双硕士学位，并教授、培训不同层次的计算机科学专业的学生。在国际技术活动中是位公认的权威发言人。

我真诚感谢全体 Packt 出版团队为此书面世所付出的努力，特别感谢 Hardik Patel、Madhuja Chaudhari 和 Martin Bell 在此书撰写过程中的辛勤努力，以及对我疯狂的进度表的包容。感谢 Alessandro Parisi 为改善此书质量所提的坦诚意见和建议。

感谢蓬勃发展、充满活力的 Android 系统的开发者们，他们正是撰写此书的动力所在。

感谢所有的朋友和家人鼓励我写这本书。特别要感谢 Khannas 和 Kollis 两家人，你们是我写书期间的强有力支柱。特别感谢 Selina Garrison 给予的指导和无时无刻的帮助。最后，也最为重要的是，我要感谢我的丈夫 Hariom Rai 和我的儿子 Arnav Rai 以他们独有的方式不断地鼓励、支持和鼓舞我，倘若没有他们，此书不可能完成。

关于技术审校

Alessandro Parisi 是一位企业软件架构师和白帽黑客，作为一名从业近 20 年的 IT 顾问，他一直热衷于尝试用非传统的途径解决复杂多变的动态环境中的问题，将新技术与横向思维和整体解决方案融合在一起。

他是 InformaticaSicura.com 的创立者、专业 IT 安全顾问、informaticasicura.altervista.org 博客的 Hacking Wisdom 专栏的负责人。

他也是 Sicurezza Informatica e Tutela della Privacy（《信息安全和隐私政策》）一书的作者，该书于 2006 年由意大利政府印刷局发行。

在此我要感谢 Ilaria Sinisi，衷心感谢她所给予的支持和耐心。

前　言

在当今这个精于技术的时代，人们的生活日益数字化。所有这些信息都可以使用移动设备随时随地访问，有成千上万的应用程序供用户下载和使用。使用移动设备上的应用程序可以轻松地访问大量信息，其最大的挑战是保护用户的私人信息和尊重他们的隐私。

第一台 Android 手机诞生于 2009 年，在这之后移动生态圈发生了变化。Android 平台是一类开放性和较少限制的应用程序模型，在开发者社区引起了兴奋并培养了创新实践能力。但是，正如每个硬币有正反两面一样，Android 平台的开放性也不例外。Android 平台刺激了所谓的破坏者的想象力。Android 为他们提供了完美的测试平台试验他们的想法。不管是作为开发者还是消费者，懂得 Android 的安全模型，以及如何明智地使用它来保护消费者是非常重要的。

本书结合实际操作的例子、图表和日常使用情况，深入研究从内核级到应用程序级的 Android 安全。向读者展示如何保护 Android 应用程序及数据的安全。在开发应用程序时，它会作为技巧和提示以馈赠读者。

读者将会学习 Android 堆的整体安全架构。使用权限、在清单文件中定义安全性、安全加密算法等方法来保护组件，Android 堆协议、安全存储、安全测试和保护设备上的企业数据也会详细介绍。读者也将学习在整合新的技术和使用类似 NFC 和移动支付到 Android 应用程序上时，如何变得有安全意识。

内容概要

第 1 章，Android 安全模型——整体，主要讲述 Android 堆的整体安全，从平台安全到应用程序安全的方方面面。本章将是学习后续章节的基础。

第 2 章，应用程序构建块，介绍应用程序组件、权限、清单文件以及从安全角度着手的应用程序签名等内容。这些 Android 应用程序的基本组件和关于这些组件的知识对于构建 Android 安全知识很重要。

第 3 章，权限，讨论 Android 平台的既有权限、如何定义新的权限、如何使用权限保护应用程序组件安全以及在定义新的权限时给予分析。

第 4 章，定义应用程序的策略文件，深入剖析作为应用程序策略文件的清单文件的

机制。讨论加强策略文件的提示和技巧。

第 5 章，尊重您的用户，包含了妥善处理用户数据的最佳实例。这对于依赖于用户评论和用户关注度的开发者的声誉来说是重要的。开发者也应谨慎处理用户的私人信息，以免落入法律的陷阱。

第 6 章，您的工具——加密 API，讨论 Android 平台提供的加密功能。它包括对称加密、非对称加密、散列、加密模式和密钥管理。

第 7 章，应用程序数据安全，是关于所有在休眠和传输过程中的应用程序数据的安全存储。讨论如何利用应用程序将私有数据沙箱化，如何安全地存储数据到设备、外部存储卡、硬盘和数据库中。

第 8 章，Android 在企业的运用，讨论 Android 平台提供的设备安全构件以及它对应用程序开发者的意义。企业应用程序开发者对于本章将会特别感兴趣。

第 9 章，安全测试，专注于以设计和开发为安全重点的测试用例。

第 10 章，展望未来，讨论即将到来的移动领域的用例，以及它是如何影响 Android 的，特别是从安全的角度。

阅读本书所需基础

如果您有一个已搭建好的 Android 环境并且可以实际操作在本书中讨论的概念和例子，那么本书将会非常有价值。请访问 developer.android.com 获得关于搭建环境和开始 Android 开发的详细说明。如果读者对内核开发感兴趣，请访问 source.android.com。

在撰写本书的时候，Jelly Bean（Android 4.2，API level 17）是最新的版本。笔者已经在这个平台上测试了所有的代码。自从 2009 年第一个版本 Cupcake 发布以来，Google 公司一直在不断提高后续版本的安全性。例如，在 Android 2.2（API level 8）中加入了远程擦除和设备管理 API，这使得 Android 更加吸引商业界。每当有相关信息时，笔者会引用该版本支持的特定功能。

本书适合的读者

本书对喜欢移动安全的人来说是一份优秀的资源。开发者、测试工程师、工程经理、产品经理和架构师，在设计和编写他们的应用程序时可以本书为参考。高级管理员和技术员可利用本书拓宽在移动安全领域的视野。拥有一些 Android 堆栈开发知识是可取的，但不是必需的。

体例

在本书中，将会发现一系列用来区分不同信息的文本风格。以下是这些风格的一些例子和关于它们含义的说明。

文本表示如下：“使用 PackageManager 类处理安装和卸载应用程序的任务”。

代码块设置如下：

```
<intent-filter>
  <action android:name="android.intent.action.MAIN" />
  <category android:name="android.intent.category.LAUNCHER" />
</intent-filter>
```

当希望读者注意特殊代码段时，相关的行或者条目会被设置成粗体：

```
Intent intent = new Intent("my-local-broadcast");
Intent.putExtra("message", "Hello World!");
LocalBroadcastManager.getInstance(this).sendBroadcast(intent);
```

命令行输入或输出写成如下格式：

```
dexdump -d -f -h data@app@com.example.example1-1.apk@classes .dex > dump
```

新术语和关键词以粗体显示。例如，读者在屏幕、菜单或对话框看到的字体，将会像这段文字一样出现：“单击下一步按钮切换到下一页”。

注意：以此格式在对话框中显示警告或重要的消息。

提示：以此格式显示提示和技巧信息。

读者反馈

我们一直欢迎读者反馈。让我们知道读者对本书的观点——喜欢的或者不喜欢的。读者反馈信息对于我们改进内容是十分重要的。

提交给我们的一般反馈，只需发送电子邮件到 feedback@packtpub.com，并注明反馈信息对应的书名。

您如果有专业知识的话题，并有兴趣撰写或者促成一本书，那么可以在 www.packtpub.com/authors 查阅作者指南信息。

用户支持

现在，您已经是 Packt 图书的用户，我们有许多的方式可以帮助您满足您的需求。

勘误表

虽然我们已经尽力确保本书内容的准确，但是错误难免会有。如果您发现我们书中的错误（文本错误或代码错误）并将错误反馈给我们，我们将不胜感激。这样，您可以避免让其他读者阅读到这个错误并帮助我们改进本书的后续版本。如果您发现了任何勘误内容，请访问 http://www.packtpub.com/submit-errata 网站，选择书名，单击 errata submission form，然后输入具体勘误内容反馈给我们。一旦通过验证，您的勘误内容将被采纳并上传到我们的网站，或者根据主题添加到现有勘误表的列表中。任何现有的勘误表都可以访问 http://www.packtpub.com/support 网站，选择主题查看。

版权声明

互联网上充斥着版权材料的盗版，所有媒体对此问题的报道一直没有间断过。在 Packt 公司，我们严格保护版权和许可。如果发现我们著作在互联网上的任何形式的非法副本，请立即向我们提供地址或者网站名称，让我们能够采取补救措施。

请通过 copyright@packtpub.com 网站与我们联系有关疑似盗版物的链接。

我们感谢您对保护作者，以及对我们提升为您带来更有价值内容的能力的帮助。

问题

如果对本书有任何疑问，您可以通过 questions@packtpub.com 网站联系我们，我们将会竭力解决您的问题。

目　录