Broadview®
www.broadview.com.cn

创建能够免遭黑客攻击和安全漏洞危害的应用

- 代码翔实，帮助读者直观学习
- 译注丰富，辅助读者透彻理解
- 补充附录B，扩展读者阅读视野

Android Apps Security

Android 应用程序安全

Android Apps Se

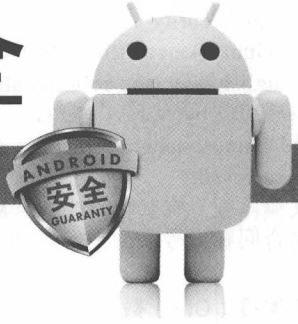
Sheran Gunasekera 著
王文君 董欢欢 译

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

Apress®

Android 应用程序安全

Android Apps Security



Sheran Gunasekera 著
王文君 董欢欢 译

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

内 容 简 介

本书是一本系统讲解 Android 应用开发安全的书籍。它首先介绍了 Android 系统的架构和安全机制，然后详细说明了 Android 应用中存在的安全风险，并提出如何实现相应的安全控制以保护用户的私密信息。同时，本书还深入讲解了数据加密、认证技术以及企业级安全等概念。通过本书的介绍，希望读者能够了解如何鉴别哪些是敏感数据、如何使用 Android API 保证数据的机密性和完整性、如何构建企业级安全的应用以及如何实现客户/服务端应用之间数据管理与传输的安全性等。

本书适用于 Android 应用开发人员、设计人员、测试人员、架构师、项目经理、安全咨询顾问等，是一本实用的讲解 Android 应用安全的教材和使用手册。

Android Apps Security
By Sheran Gunasekera, ISBN:978-1-4302-4062-4
Original English language edition published by Apress Media.

版权贸易合同登记号　图字：01-2013-5972

图书在版编目（CIP）数据

Android 应用程序安全 / 古纳塞克若（Gunasekera,S.）著；王文君，董欢欢译. —北京：电子工业出版社，2013.10
书名原文：Android Apps Security
ISBN 978-7-121-21383-0

Ⅰ. ①A… Ⅱ. ①古… ②王… ③董… 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（2013）第 209339 号

责任编辑：贾　莉
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
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：17.75　　字数：332 千字
印　　次：2013 年 10 月第 1 次印刷
定　　价：59.00 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。

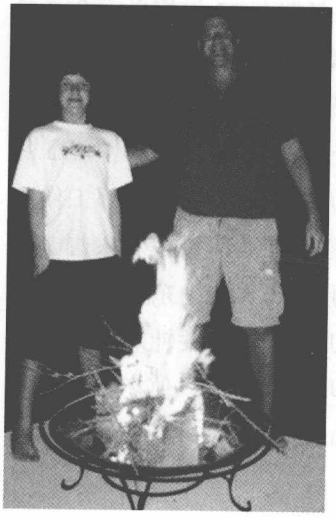
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件到 dbqq@phei.com.cn。

服务热线：（010）88258888。

关于作者

Sheran Gunasekera 是一名拥有 13 年信息安全经验的安全研究人员和软件开发者。他是 ZenConsult Pte.公司的研发主管，负责个人计算机和移动设备平台的安全研究。Sheran 一直积极致力于 BlackBerry 和移动 Java 的研究，并且是揭露首个企业认可的恶意应用内部工作原理的白皮书的作者，这些恶意软件被部署在阿联酋电信运营商签约用户的移动设备上。他曾在中东、欧洲和亚太地区的安全会议上发表演讲，提供有关针对移动设备的恶意软件分析，以及针对 Web 和移动设备的安全软件开发的培训。他还在其有关安全的博客上撰写并发表文章（http://chirashi.zenconsult.net）。

关于技术审阅者



Michael Thomas 拥有超过 20 年的软件开发的经验，其间做过独立开发者、团队负责人、项目经理和工程副总裁。Michael 拥有超过 10 年的移动设备相关的工作经验。他目前的工作重点是在医疗领域中通过使用移动设备加速患者和医疗服务提供者之间的信息传输。

致谢

感谢各位编辑、审稿人以及 Apress 的工作人员，他们不知疲倦的工作帮助了这本书的出版。他们是这本书背后的驱动力，感谢他们的耐心与包容，我则不是一个称职的作者。

同样要感谢我的朋友和同事，Michael Harrington 和 Shafik Punja，没有他们我就没有机会出版这本书。感谢你们，这是一段很棒的经历。

——Sheran Gunasekera

译者介绍

王文君

王文君现就职于惠普软件上海研发中心，担任多个产品的安全架构师和安全讲师。现为 OWASP 上海区负责人之一，作为演讲嘉宾参加过 2011 年 OWASP 亚洲峰会以及 2012 年 OWASP 中国峰会，并且是 CWASP 认证专家组成员，同时也是 2013 年出版的《Web 应用安全威胁与防治——基于 OWASP Top 10 与 ESAPI》作者之一，拥有 CISSP、 PMP、 ITIL 等认证。王文君于 2002 年毕业于上海交通大学，拥有电气工程硕士学位和电气工程/涉外会计双学士学位。

董欢欢

董欢欢毕业于上海复旦大学，拥有计算机信息技术管理学士学位。现就职于惠普软件上海研发中心，担任研发工程师。拥有 7 年的软件研发经验，在移动开发和设计方面有着丰富的经验。2009 年至今，从事 Android 应用程序设计和开发，对 Android 有较深刻的理解，开发有 AltiGen MaxMobile Communicator、SkyDrive Assistant 等 Android 应用。

译者序

2012 年的秋天，我收到了电子工业出版社贾莉编辑的电话，问我对 *Android Apps Security* 一书有没有翻译的兴趣。我正好带领一个团队做过手机应用，对这个课题很感兴趣，并在 Amazon 网站上搜索了 Android 应用安全方面的书籍，得到的结果只有这么一本，于是毫不犹豫地答应了。

不可否认，现在的手机应用无论是在个人领域还是企业应用领域都变得举足轻重，而其中，Android 的份额最大。但是 Android 应用一直以来都有一个为用户所诟病的问题，就是其安全性，因而构建一款成功的 Android 应用，安全的重要性不言而喻。所以作为一名开发人员，需要了解 Android 的安全风险有哪些，如何构建安全控制以规避这些安全隐患，而本书写作的主要目的正是为了说明这些问题。

本书有几大特点。首先，这是一本完全基于 Android 系统讲述应用安全性的书籍。目前有关移动应用安全的书籍很多，但是具体讨论 Android 系统安全性的却很少。其次，本书内容不仅具备理论性，还提出了具体的设计指导，全书以实际的代码介绍来讲解抽象的理论知识，相信对于读者而言，会具有很强的可操作性。

回想过去的几个月，几乎所有的空余时间都在做此书的翻译工作，我们对书中的内容做了严格的考证，并实际运行了书中的实例。比如在作者写作本书时候的 Google Play，现在已纳入了 Google Now；而现在的 Google App Engine 相比作者写作之时，地址和界面都已发生了变化，等等，所有的这一切我们都添加了译者注。为了使读者更容易理解和上手，对于第 7 章“企业级应用开发安全”，我们就补充了原书中没有提及的服务器端源代码，帮助读者直接参考。在本书翻译的最后阶段，我们两人在星巴克一坐就是一整天，喝着咖啡，吃着面包，一起热烈讨论书中的细节，现在想起来，还是回味无穷。

感谢李详青女士为本书译稿做审核，你严谨的工作态度和精湛的外语底蕴使我们受益匪浅。

感谢电子工业出版社参与编审的老师们，正是你们认真的职业态度，使得我们几易其稿，方而敲定。

感谢HP Software上海的领导黄晓辉先生对软件安全一直以来的大力支持和鼎力推广，同时感谢李维纲、朱征宇、姚靓、伍文冰，陈立浩、金卫国、谢黎等领导一直以来对软件安全工作的支持。

Many thanks to my team —— HP Software Security&Trust office, I really enjoy working with these talent people, including but not limited to Tomer Gershoni, Gabi Joseph, Uri Shamir, Elena Kravchenko, Yaniv Toledano, Yaniv Simsolo and Ori Troyna. All of you are definitely the security expert that everyone wants to be.

王文君　董欢欢

2013 年 8 月

目 录

第 1 章

Android 架构

Google 以拥有数亿资产的公司才负担得起的大手笔进入了手机市场：直接收购一家公司。2005 年，Google 公司收购了当时还鲜为人知的 Android 公司，尽管 Android 公司的四位创始人都是相当成功的人士。该公司自 2003 年由 Andy Rubin、Rich Miner、Chris White 和 Nick Sears 创建以来，就一直没有显山露水，潜心研发一款针对手机设备的操作系统。为了能够开发出更符合用户需求的智能手机，这支隐藏在 Android 操作系统背后的团队一直在保密状态下工作。对外他们只承认正在研发针对手机设备的软件，对 Android 操作系统的实质始终只字未提，这一情形一直持续到 2005 年公司被收购。

凭借 Google 的大力支持，Android 的开发进度迅猛提升。到 2011 年第二季度，在用户已使用的移动操作系统的比例中，Android 已赢得近 50%的市场份额。收购后四位创始人继续留在公司，Rubin 则作为 Google 移动部高级副总裁领导着整个团队。2008 年 9 月 23 日，Android 1.0 版本正式发布，运行该系统的首个硬件设备则是绿白之梦 HTC Dream（见图 1-1）。

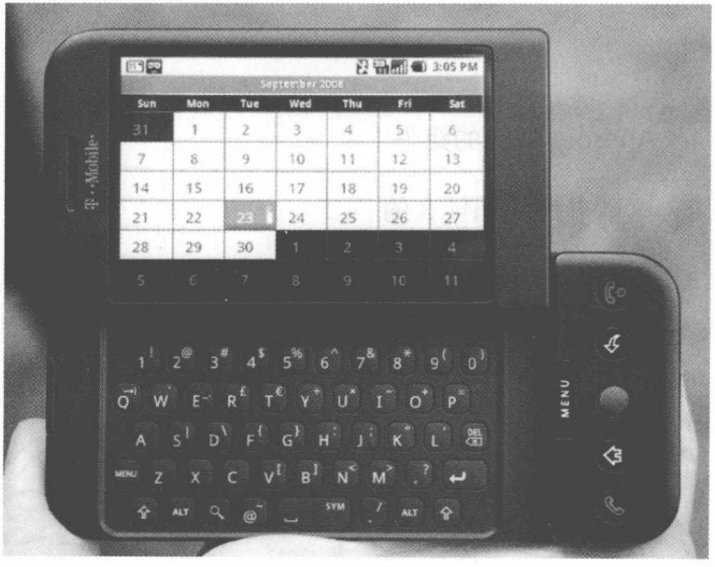


图 1-1　HTC Dream（图片由迈克尔·奥利提供）

Android 操作系统的一个独有特点，即将二进制文件和源码作为开源软件发布，使其得以快速成长。你可以下载完整的 Android 操作系统源代码，约占 2.6 GB 的磁盘空间。理论上，这就允许任何人设计和制造出一部运行 Android 系统的手机。但是这一开源软件的想法只持续到 Android 3.0 版本，Android 3.0 及其之后的版本则采用了闭源方式。在接受彭博商业周刊（*Bloomberg Businessweek*）采访时，Rubin 说版本 3.x 代码库采用了众多捷径，以确保快速向市场发布，并且系统只能运行在某些特定的硬件上。如果其他硬件厂商采用这一版本的 Android 系统，就有可能出现一些负面的用户体验，而这正是 Google 所力图避免的。[1]

1.1 Android 架构的组件

Android 架构可划分为如下四个主要组成部分：

- 内核
- 类库和 Dalvik 虚拟机
- 应用程序框架
- 应用程序（本书中也常简称为“应用”）

[1] 彭博商业周刊，“Google Holds Honeycomb Tight”，阿什莉万斯和布拉德•斯通，*www.businessweek.com/technology/content/mar2011/tc20110324_269784.htm*，2011 年 3 月 24 日。