国际信息工程先进技术译丛

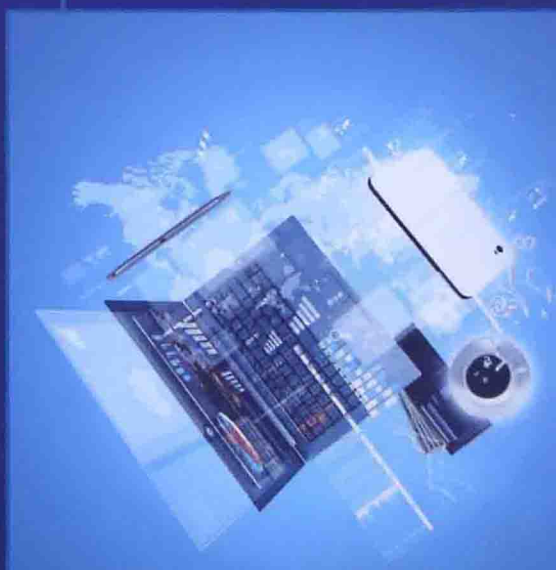
CRC Press
Taylor & Francis Group

Android系统安全与攻防

Android Security: Attacks and Defenses

（美） Abhishek Dubey
Anmol Misra 编著

王秋爽 郎为民 王大鹏 靳焰 等译



机械工业出版社
CHINA MACHINE PRESS

国际信息工程先进技术译丛

Android 系统安全与攻防

（美） Abhishek Dubey
Anmol Misra 编著

王秋爽 郎为民 王大鹏 靳 焰 等译

机 械 工 业 出 版 社

图书在版编目（CIP）数据

Android 系统安全与攻防/（美）杜贝（Dubey, A.），（美）米斯拉（Misra, A.）编著；王秋爽等译. —北京：机械工业出版社，2014.10

（国际信息工程先进技术译丛）

书名原文：Android security: attacks and defenses

ISBN 978-7-111-47721-1

Ⅰ.①A… Ⅱ.①杜…②米…③王… 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（2014）第 191821 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：张俊红 责任编辑：闾洪庆

版式设计：霍永明 责任校对：纪 敬

封面设计：马精明 责任印制：刘 岚

北京云浩印刷有限责任公司印刷

2014 年 10 月第 1 版第 1 次印刷

169mm × 239mm · 11.75 印张 · 222 千字

0001—3000 册

标准书号：ISBN 978-7-111-47721-1

定价：49.80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务		网络服务	
社服务中心：	（010）88361066	教材网：	http://www.cmpedu.com
销售一部：	（010）68326294	机工官网：	http://www.cmpbook.com
销售二部：	（010）88379649	机工官博：	http://weibo.com/cmp1952
读者购书热线：	（010）88379203	**封面无防伪标均为盗版**	

本书共分为10章。第1章介绍了移动设备的发展格局；第2章和第3章分别介绍了Android操作系统和应用程序的体系结构；第4章深入研究了Android系统的安全特性；第5~9章介绍了Android系统平台和Android应用程序安全问题的各个方面；第10章展望了未来移动设备安全威胁的发展格局。附录A和附录B分别讨论了Android权限的风险等级和JEB反编译器的用法；附录C演示了如何破解第7章中的SecureApp.apk应用程序，具体的破解方法和步骤，可在本书网站（www.androidinsecurity.com）上获得；附录D是本书出现的缩略语的中英文对照。

本书主要面向安全架构师、系统管理人员、企业软件开发周期主管、开发人员、白帽黑客、渗透测试人员、IT架构师、首席信息官、学生和普通用户。

译 者 序

随着信息技术的快速发展，信息已经成为人们日常生活和工作中的重要资源。围绕着信息资源的安全问题逐渐引起人们的关注，特别是利用移动设备和信息网络发起的各种非法和犯罪行为。例如，窃取企业信息资源、商业机密和个人隐私、网络钓鱼、网络间谍刺探等恶意行为。而且，随着智能移动设备日益普及，搭载各种智能移动操作系统平台的设备逐渐进入人们社会生活的各个层面（政府机关、企业团体、家居生活等），鉴于移动设备与生俱来的安全短板，信息资源的安全问题变得更加的复杂和严峻。

在当今众多的移动设备中，搭载 Android 系统的移动设备在智能移动市场份额上独占鳌头，几乎在每十部搭载智能移动系统的设备中，至少就有 6 部搭载 Android系统的设备。Android 系统自 2008 年 10 月第一次试水商用以来，经过短短的五年时间，迅速发展成全球最为普及和流行的、应用程序最为丰富的智能移动操作系统平台。据 2013 年统计数据，全球约 76% 的移动设备和约 80% 的智能手机，采用的都是 Android 操作系统平台。除此之外，Android 系统正在以迅猛的速度向更加广泛的应用领域扩张，包括智能家电、智能汽车电子、企业计算基础设施、智能定位导航终端、游戏机，甚至笔记本电脑等。Android 系统如此大的市场占有量、用户普及度，以及如此迅猛的发展势头，使得 Android 系统的信息安全问题直接牵动着移动设备信息资源领域的安全动向。同传统的台式机/笔记本电脑系统相比，搭载 Android 系统平台的智能移动设备，无论在设备屏幕分辨能力、安全软件成熟度，还是用户安全意识方面，都不及前者。而且，如今的智能移动设备发展迅速，设备本身配置各种功能模块，如 GPS、Wi-Fi、NFC、蓝牙，以及 Wi-Fi Direct 等，而这些技术/模块又为恶意攻击者提供更多的入侵设备的渠道。此外，Android 智能移动设备完善、丰富的功能，使得一部小小的智能手机几乎可以承担传统台式机/笔记本电脑处理的大部分个人日常业务，如日程安排计划、电子邮件收发、文档表格处理、网上银行个人支付、手机银行、股票理财等账户操作管理、网络账号登录、生活工作业务数据备份同步等，个人或企业用户在进行上述业务操作时，需要移动设备提供可靠的安全环境、企业制定规范的安全制度和用户树立良好的安全意识，否则，这些业务中涉及的数据将不可避免地成为恶意攻击者觊觎的目标。

本书在这一背景下，系统地介绍了 Android 系统的体系结构、Android 应用程序的组成架构与运行机制，深入地分析了 Android 系统的安全机制，概述了针对 Android 系统的威胁演化过程与发展格局。同时，结合近期出现的几例 Android 漏洞与恶意软件，系统地总结了 Android 系统的安全漏洞，并对恶意软件的特点进行

了深入的剖析。此外，本书最大的特点是从 Android 安全攻与防的角度出发，基于对各种针对 Android 信息安全的攻击方式的详细介绍，进行深入地剖析，并给出应对措施。并且，对几种主要的 Android 系统与应用程序的分析方法和工具进行了详细的介绍和归类，包括渗透测试、逆向工程等手段，为 Android 设备的普通用户、移动应用程序开发者、企业安全分析人员、企业安全管理员等人士，提供高效的分析工具和详实的测试指导。从而，便于上述人员能够有效地区分恶意 Android 应用、开发安全的 Android 应用程序、部署可靠的企业 Android 设备环境和制定完善、健全的企业安全规章。

本书主要由王秋爽、郎为民、王大鹏、靳焰翻译，天津师范大学的硕士研究生张敬瑜，解放军国防信息学院的张国峰、陈红、夏白桦、毛炳文、刘素清、邹祥福、瞿连政、徐延军、张锋军、陈于平、余亮琴、张丽红、王昊、陈虎参与了本书部分章节的翻译工作，和湘、朱元诚、高泳洪、周莉、蔡理金、王会涛绘制了本书的全部图表，李建军、靳焰、王逢东、孙月光、孙少兰、马同兵对本书的初稿进行了审校，并更正了不少错误，在此一并向他们表示衷心的感谢。同时，本书是译者在尽量忠实于原书的基础上翻译而成的，书中的意见和观点并不代表译者本人及所在单位的意见和观点。

由于译者水平有限，翻译时间仓促，因而本书翻译中的错漏之处在所难免，恳请各位专家和读者不吝指出。

郎为民

原 书 序

近年来针对移动设备的网络威胁始终在不断地增加。随着 Android 系统逐渐成为主流的移动设备系统平台，与该系统相关的安全问题也逐渐成为个人和企业客户关注的越来越多的问题。本书对 Android 系统及其功能特性的发展过程进行了深入的剖析、讨论了各种针对 Android 设备的攻击方法，为移动应用程序开发人员、安全架构师，以及其他各类专业人员，提供了掌握移动设备安全威胁防御手段所必需的各类基础知识，从而使读者树立良好的 Android 安全防御意识。

在当今世界移动设备大量普及的背景下和移动设备的广泛领域中，Dubey 和 Misra 开始关注 Android 系统的崛起和该系统平台所面临的各种安全挑战。他们超越了传统的被应用程序开发者熟知和掌握的基本安全概念，致力于解决更加重要和高级的安全课题。例如，攻击对策、企业内部 Android 系统整合，以及与之相关的企业监管与合规风险。通过本书，任何对移动安全感兴趣的人，都可以快速地熟悉 Android 系统平台，并且在保护个人和企业客户免于遭受日益增长的移动设备安全威胁方面，获得独特的安全策略视角。这对于安全架构师和安全顾问，以及从事移动设备与应用程序的企业安全管理人员来说，是一种必须具备的能力。

卡内基·梅隆大学信息网络研究所主任兼 CyLab 网络实验室教育、培训、外联主任

Dena Haritos Tsamitis 博士

Dena Haritos Tsamitis 博士领导的信息网络研究所（Information Networking Institute，INI），是卡内基·梅隆大学工程学院的一个全球性的、跨学科的部门。她主管着信息网络研究所的研究生专业，包括信息网络专业、信息安全技术与管理专业和信息技术专业。在她的带领下，信息网络研究所将其专业推广到了全球各个地区，并力主同卡内基·梅隆大学硅谷校区合作，将信息安全、移动与软件管理学科打造成“美国双海岸”共建专业。Dena 博士还主管卡内基·梅隆大学 CyLab 网络实验室的教育、培训和外联事务。她是 NSF（National Science Foundation，国家科学基金会）资助的两个信息安全教育项目（CyberCorps 奖学金计划[⊖]和信息安全保障能力构建计划）的主要研究者，同时还是 DOD（Department

---

⊖ CyberCorps 奖学金计划，用于资助实施“网络空间人才”（CyberCorps）计划，鼓励高等院校开设计算机安全专业、开展专项课题研究，并为志愿从事计算机安全工作相关专业的大学生提供奖学金。——译者注

of Defense of the United States，美国国防部）资助的信息安全保障基金项目的主要研究者。她曾荣获过2012年度卡内基·梅隆大学Barbara Lazarus奖，以表彰其在研究生和青年教师的指导上所作出的贡献。此外，她还被Alta联合公司和CSO杂志提名，荣获2008年度女性影响力奖，以表彰她在信息安全和教育领域的成就。

原书前言

2007年苹果公司推出iPhone手机，开启了移动设备和移动应用程序领域的新纪元。随后，Google公司的Android系统平台也成为移动设备市场中的重要成员，并且到2012年，搭载Android系统的移动设备的出货量首度超越了苹果公司的iPhone手机。随着移动设备逐渐成为主流，针对移动设备的威胁也在不断地演化。如今，Android系统的大量普及，已经引起了众多恶意攻击者的注意。可以看到，近年来针对Android系统平台的攻击案例数量正在不断地攀升。

关于本书

本书从安全问题和威胁的角度，对Android系统平台和应用程序进行了分析。所有对Android系统安全或对Android在安全方面的优势和劣势感兴趣的人士，都属于本书的读者群。书中介绍了Android操作系统和应用程序的体系结构，分析了Android系统平台提供的各种安全特性。随后，本书又介绍了分析和测试Android平台和应用程序安全问题的各种方法和工具。最后，本书还介绍了企业环境下Android设备存在的各种安全隐患，以及增强Android设备和应用程序安全性的措施和步骤。尽管本书主要关注的是Android系统平台的安全问题，但是书中论述的很多问题和原则，同样适用于其他主流的操作系统平台。

假设

本书假设读者熟悉操作系统的相关知识并拥有一定的安全概念。如果读者掌握有关渗透测试、威胁建模和常见的Web应用程序与浏览器漏洞的相关知识更好，不过如果读者没有掌握这些知识，在本书的阅读上也是没有问题的。

读者

本书主要面向安全架构师、系统管理人员、企业SDLC（Software Development Life Cycle，软件开发周期）主管、开发人员、白帽黑客[⊖]、渗透测试人员、IT架构师、CIO（Chief Information Officer，首席信息官）、学生和普通用户。如果你想

⊖ 白帽黑客（white-hat hacker），又称白帽匿名者、白帽子，是指利用黑客技术测试网络和系统的性能，从而判定它们能够承受入侵的强弱程度，和网络安全工程师的性质有点相同。通常他们被企业聘请来攻击他们自己的系统或客户的系统以便进行安全审查。——译者注

要了解 Android 系统的安全特性、潜在的安全攻击，以及防御这些攻击的办法，你会发现书中的每一章，对你来说都可以成为实用的出发点。我们的目标是为读者提供充足的信息和所有 Android 平台的基础知识，以及背后相关的安全问题，从而使读者能够快速了解 Android 系统并驰骋于 Android 系统安全领域。如果你是一名 Android黑客，或者你已经相当精通 Android 平台的安全问题了，那么本书并不适合你。

支持

本书的勘误表和相关资源可从 CRC 出版社的网站，以及我们的网站 www. androidinsecurity. com 上获得。在我们的网站上，有其他用户创建的应用程序和工具，可以提供给读者下载。本书作者编写的示例应用程序，可以在我们网站的资源部分获得。读者可以结合书中内容，使用下述账号和密码，从我们网站上下载相应的 apk 文件进行练习。

用户名：android

密码：1439896461（本书的 10 位 ISBN[⊖]）

本书结构

本书共分为 10 章。第 1 章介绍了移动设备的发展格局；第 2 章和第 3 章分别介绍了 Android 操作系统和应用程序的体系结构；第 4 章深入研究了 Android 系统的安全特性；第 5 ~ 9 章介绍了 Android 系统平台和 Android 应用程序安全问题的各个方面；第 10 章展望了未来移动设备安全威胁的发展格局。附录 A 和附录 B 分别讨论了 Android 权限的风险等级和 JEB 反编译器的用法；附录 C 演示了如何破解第 7 章中的 SecureApp. apk 应用程序，具体的破解方法和步骤，可在本书网站（www. androidinsecurity. com）上获得。

⊖ 此为英文原版书的 10 位 ISBN。

作者简介

Anmol Misra

Anmol 是《Defending the Cloud: Waging War in Cyberspace》[⊖]一书的特约作者，擅长移动设备与应用程序安全、漏洞管理、应用程序与基础架构安全评估，以及代码安全性审查。

Anmol Misra 现在是思科外部关键业务安全组（Critical Business Security External team，CBSE）的项目主管。CBSE 是思科信息安全组（Information Security Team，InfoSec）的一部分，主要负责思科云托管服务（Cisco's Cloud Hosted Services）的安全问题。在加入思科之前，Anmol 是安永会计师事务所（Ernst & Young LLP）的高级顾问。他的职责主要是为财富 500 强企业提供有关明确和改善企业信息安全计划和措施的建议。他曾帮助过一些大型企业，通过改善他们的安全状况，降低企业 IT 安全风险并符合安全规范的要求。

Anmol 拥有卡内基·梅隆大学信息网络专业硕士学位，同时还拥有计算机工程专业工学学士学位。他曾担任过卡内基·梅隆大学校友会旧金山湾区分会的校友联络处副主席。

在 Anmol 闲暇的时间里，他喜欢在旧金山的海滩上漫步。Anmol 是一名狂热的社科类书籍爱好者，尤其是历史和经济类的书籍。同时，他还是一位有抱负的摄影师。

Abhishek Dubey

在信息安全方面，Abhishek 有着广泛且丰富的经验，包括逆向工程、恶意软件分析和漏洞检测。目前，他是思科公司安全服务与云运维组（Security Services and Cloud Operations team，SSCO）的首席/高级工程师。在加入思科公司之前，Abhishek是 Webroot 软件公司高级威胁研究小组（Advanced Threat Research Group，ATRG）的高级研究员。

Abhishek 拥有卡内基·梅隆大学信息安全与技术管理专业硕士学位，以及计算机科学与工程专业科技学学士学位。目前，他正在攻读斯坦福大学战略决策与风险

⊖ 《Defending the Cloud: Waging War in Cyberspace》，译为《云防御：网络空间作战》，2011 年 12 月由 Infinity Publishing 出版公司出版。——译者注

管理专业。他也曾担任过卡内基·梅隆大学校友会旧金山湾区分会运营与联合处副主席，该校友分会拥有5000多名校友。

在Abhishek闲暇的时间里，他是一名狂热的长跑和摄影爱好者。同时，他还喜欢攀岩，并且还是一名美食家。

原书致谢

写书不是一个人的事情，离不开他人的支持和帮助。首先，我们要感谢我们的编辑——CRC 出版社的 John Wyzalek，感谢他对本书的编写所给予的耐心和不变的承诺。我们还要感谢 Derryfield 出版公司的制作团队——Theron Shreve 和 Marje Pollack。在本书的制作过程中，Theron 自始至终给予我们极大的指导。在本书多次修订的过程中，Marje 始终非常耐心地帮助我们，将这本记录式的书稿制作成一部读者手上令人兴奋的书籍。

我们要感谢 Dena Tsamtis（卡内基·梅隆大学信息网络研究所主任兼 CyLab 网络实验室教育、培训、外联主任）、James Ransome（McAfee 公司产品安全高级总监）和 Gary Bahadur（Razient 公司 CEO），多年来给予我们的帮助和指导。我们还要感谢 Nicolas Falliere（JEB 反编译器的创作者），让我们在第一时间接触到了 JEB 反编译器。同时，我们还要感谢其他那些在我们前进的道路上帮助过我们的人们，这里不可能将他们的名字一一列出。

——Anmol 和 Abhishek

借此机会，我要向我的导师 David Veach（思科公司高级主管）和 Mukund Gadgil（Engineering-Upheels. com 网站副总裁）致以诚挚的感谢，感谢他们一直以来给予我的示范和指导。这些年来，从你们身上，我学到了很多的东西。同时，我还要由衷地感谢我的朋友们——Anuj、Varang、Erica 和 Smita。这些年来，是你们不断地鼓励我实现目标，并始终陪伴着我同甘共苦。在我眼中，你们都是最棒的！最后，我要感谢我的妈妈、爸爸，还有我的姐姐——Anubha，感谢你们对我所做的每一件事情都不曾有丝毫质疑的支持。正是因为有你们的支持，才有我所获得的成绩。

——Abhishek

我要感谢 Bill Vourthis（安永会计师事务所高级经理）、David Ho（思科公司经理）和 Vinod（Jay）Jayaprakash（安永会计师事务所高级经理）多年来给予我的指导和鼓励。我还要由衷地感谢我的导师 Nitesh Dhanjani（安永会计师事务所执行主任）给予我的指导和鼓励。同时，我要感谢我的家庭——妈妈、爸爸，以及我的兄弟——Sekhar 和 Anupam，感谢你们对我事业的支持，并始终与我同在。妈妈、爸爸——你们是家庭的支柱，我获得的所有成绩都源自于你们的鼓励和支持。我知道你们对我繁忙、紧张的时间安排难以忍受。现在，我已经完成了这本书，我保证从现在开始一定及时地回复你们的电话和电子邮件。

——Anmol

目　录

译者序

原书序

原书前言

作者简介

原书致谢

第1章　引言 …… 1

1.1　选择 Android 系统的原因 …… 1

1.2　移动设备的威胁演化 …… 6

1.3　Android 概述 …… 8

1.4　Android 应用软件市场 …… 10

1.5　小结 …… 12

第2章　Android 体系结构 …… 13

2.1　Android 体系结构概述 …… 13

2.1.1　Linux 内核层 …… 13

2.1.2　标准库层 …… 19

2.1.3　Android 运行时环境 …… 20

2.1.4　应用程序框架层 …… 20

2.1.5　应用程序层 …… 21

2.2　Android 系统启动与 Zygote …… 21

2.3　Android SDK 及开发工具 …… 22

2.3.1　Android SDK 下载与安装 …… 22

2.3.2　Eclipse 和 ADT 开发环境 …… 23

2.3.3　Android 工具 …… 25

2.3.4　DDMS …… 26

2.3.5　adb …… 27

2.3.6　ProGuard …… 29

2.4　“Hello World” 应用程序详解 …… 30

2.4.1　认识 “Hello World” 程序 …… 31

2.5 小结 …… 34

第3章 Android 应用程序体系结构 …… 35

3.1 应用程序组件 …… 35

3.1.1 Activity …… 35

3.1.2 Intent …… 38

3.1.3 Broadcast Receiver …… 41

3.1.4 Service …… 43

3.1.5 Content Provider …… 44

3.2 Activity 生命周期 …… 45

3.3 小结 …… 50

第4章 Android 安全机制 …… 51

4.1 Android 安全模型 …… 51

4.2 Linux 权限机制 …… 52

4.3 Android Manifest 权限 …… 54

4.3.1 权限请求 …… 55

4.3.2 权限组合使用 …… 58

4.4 移动设备安全问题 …… 61

4.4.1 设备 …… 61

4.4.2 漏洞修补 …… 62

4.4.3 外部存储 …… 62

4.4.4 键盘 …… 62

4.4.5 数据隐私 …… 62

4.4.6 应用程序安全 …… 62

4.4.7 遗留代码 …… 63

4.5 近期主要的 Android 系统攻击事件 …… 63

4.5.1 DroidDream 变种程序分析 …… 63

4.5.2 Zsone 手机木马程序分析 …… 65

4.5.3 Zitmo 手机木马程序分析 …… 65

4.6 小结 …… 68

第5章 Android 渗透测试 …… 69

5.1 渗透测试 …… 69

5.1.1 外部渗透测试 …… 69

5.1.2 内部渗透测试 …… 70

5.1.3 渗透测试方法 …… 70

5.1.4 静态分析 …… 70

5.1.5 Android 系统和设备渗透测试步骤 …… 71
5.2 Android 渗透测试工具 …… 71
5.2.1 Nmap …… 72
5.2.2 BusyBox …… 72
5.2.3 Wireshark …… 73
5.2.4 Android 操作系统的漏洞 …… 76
5.3 Android 应用程序渗透测试 …… 76
5.3.1 Android 应用程序 …… 76
5.3.2 应用程序安全 …… 83
5.4 其他问题 …… 85
5.4.1 内部、外部以及云端的数据存储 …… 85
5.5 小结 …… 85

第 6 章 Android 应用程序逆向工程 …… 86
6.1 逆向工程 …… 86
6.2 恶意软件 …… 87
6.3 识别 Android 恶意软件 …… 88
6.4 Android 应用程序逆向工程方法 …… 89
6.5 小结 …… 103

第 7 章 无需源码修改 Android 应用程序行为 …… 104
7.1 概述 …… 104
7.1.1 添加恶意的行为 …… 104
7.1.2 清除恶意的行为 …… 104
7.1.3 绕过特定的功能 …… 105
7.2 DEX 文件格式 …… 105
7.3 案例研究：修改应用程序行为 …… 108
7.4 实例 1：Google Wallet 漏洞 …… 114
7.5 实例 2：Skype 漏洞（CVE-2011-1717） …… 115
7.6 防范策略 …… 115
7.6.1 代码混淆 …… 116
7.6.2 服务器端处理 …… 118
7.6.3 迭代散列与使用盐值 …… 118
7.6.4 选择恰当位置存储敏感信息 …… 119
7.6.5 加密技术 …… 119
7.6.6 结论 …… 119
7.7 小结 …… 120

第 8 章 入侵 Android …… 121
8.1 概述 …… 121
8.2 Android 文件系统 …… 121
8.2.1 挂载点 …… 122
8.2.2 文件系统 …… 123
8.2.3 目录结构 …… 124
8.3 Android 应用程序数据 …… 126
8.3.1 存储方式 …… 126
8.3.2 /data/data …… 126
8.4 Android 设备的 root 处理 …… 128
8.5 制作 Android 系统镜像 …… 130
8.6 访问应用程序数据库 …… 131
8.7 从 Android 设备上提取数据 …… 133
8.8 小结 …… 135

第 9 章 企业环境 Android 系统的安全问题 …… 136
9.1 企业的 Android 系统 …… 136
9.1.1 企业 Android 系统的安全问题 …… 136
9.1.2 终端用户的安全意识 …… 140
9.1.3 合规/审查事项 …… 140
9.1.4 移动设备安全措施推荐 …… 141
9.2 强化 Android 安全性 …… 142
9.2.1 安全部署 Android 设备 …… 142
9.2.2 设备管理 …… 146
9.3 小结 …… 148

第 10 章 浏览器安全与未来威胁格局 …… 149
10.1 移动 HTML 安全 …… 149
10.1.1 跨站点脚本攻击 …… 151
10.1.2 SQL 注入攻击 …… 151
10.1.3 跨站点伪造请求攻击 …… 151
10.1.4 网络钓鱼 …… 152
10.2 移动浏览器安全 …… 152
10.2.1 浏览器漏洞 …… 152
10.3 未来移动设备威胁发展格局 …… 154
10.3.1 手机变身间谍/跟踪装置 …… 155
10.3.2 通过移动设备操纵企业网络与设备 …… 155