Broadview
www.broadview.com.cn

Mc Graw Hill
Osborne

安全技术大系

Mobile Application Security

移动应用安全

[美] Himanshu Dwivedi, Chris Clark, David Thiel 著
李祥军 罗熊 译

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

Mobile Application Security

移动应用安全

[美] Himanshu Dwivedi, Chris Clark, David Thiel 著

李祥军 罗熊 译

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

内 容 简 介

移动应用不仅仅是下一波技术浪潮，在不远的将来对于很多关键活动而言，它将成为默认的计算方式，如 E-mail、在线购物、游戏甚至娱乐等。本书介绍了手机、PDA 等移动设备面临的主要安全挑战以及一些移动应用安全开发中的技巧。以 Android、iPhone、Windows Mobile、BlackBerry 以及 Symbian 等操作系统为例，详细阐述了这些系统的安全功能以及如何利用这些功能来开发安全的移动应用，如防护缓冲区溢出、SQL 注入攻击以及部署私钥与公钥密码技术等。

针对当前的热点应用，本书还介绍了 WAP、蓝牙、SMS、MMS、移动地理定位等移动应用面临的安全威胁、自身存在的安全不足以及由此带来的安全风险，并介绍了针对移动平台的企业安全问题，以及不同系统的安全措施和安全防护手段。

Himanshu Dwivedi，Chris Clark，David Thiel
Mobile Application Security
ISBN：0-07-163356-1

北京市版权局著作权合同登记号： 01-2011-0634

图书在版编目（CIP）数据

移动应用安全 /（美）德维威迪（Dwivedi,H.），（美）克拉克（Clark,C.），（美）蒂尔（Thiel,D.）著；李祥军，罗熊译. —北京：电子工业出版社，2012.2
（安全技术大系）
书名原文：Mobile Application Security
ISBN 978-7-121-15440-9

Ⅰ. ①移… Ⅱ. ①德… ②克… ③蒂… ④李… ⑤罗… Ⅲ. ①移动通信－安全技术 Ⅳ. ①TN929.5

中国版本图书馆 CIP 数据核字（2011）第 255156 号

策划编辑：毕 宁 bn@phei.com.cn
责任编辑：贾 莉 白 涛
印 刷：北京东光印刷厂
装 订：三河市皇庄路通装订厂
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：21.5 字数：416 千字
印 次：2012 年 2 月第 1 次印刷
印 数：4000 定价：55.00 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。

关于作者

Himanshu Dwivedi

Himanshu Dwivedi 是 iSEC Partners 公司的创始人之一，作为一家信息安全公司，iSEC 致力于应用安全，详情请访问 www.isecpartners.com。Himanshu 负责 iSEC 公司的产品研发和市场营销。

Himanshu 还是业界知名的作家，已出版 6 本安全方面的著作：*Hacking VoIP*（No Starch Press）、*Hacking Exposed: Web 2.0*（McGraw Hill/Professional）、*Hacker's Challenge 3*（McGraw Hill/Professional）、*Securing Storage*（Addison Wesley）、*Implementing SSH*（Wiley）。此外，Himanshu 还拥有一项申请中的关于光纤信道安全的专利。

在创建 iSEC Partners 公司之前，Himanshu 是 stake 公司的区域技术总监。

Chris Clark

Chris Clark 是 iSEC Partners 公司的首席安全顾问，负责开发工具、实施渗透测试并担任 Windows 和移动安全专家。在其软件生涯中，Chris 专注于安全领域并协助一些大公司设计和开发安全软件。他带领几个团队完整实现了软件安全开发生命周期，以及开发安全产品所需的初始启动过程。通过在服务器、客户端及 Web 应用方面的工作，Chris 积累了广泛的安全经验。在加入 iSEC 之前，Chris 供职于 Microsoft，负责一个大型支付系统以及一款广泛部署的企业管理产品的安全。

Chris 曾在 RSA 2009 以及 OWASP 纽约、新泽西、西雅图分会、SOA 高峰论坛等安全大会上进行演讲，并且担任 Black Hat Federal 大会的培训讲师。在 Black Hat Federal 大会上，他与 Immunity 以及 Microsoft 合作组织了旗帜保卫战培训。除公开演讲外，Chris 还针对那些致力于开发更加安全的产品的管理层与工程师设计和开办了一些培训班。

David Thiel

David Thiel 是 iSEC Partners 公司的首席安全顾问。他在计算机安全领域有着超过 12 年的经验，包括电子商务领域、政府领域、航空领域以及在线博彩领域的安全架构审计和设计。他擅长的领域包括 Web 应用渗透测试、网络协议、模糊测试、UNIX 以及 Mac OS X，

研究兴趣包括移动和嵌入式设备攻击、媒体软件漏洞以及新兴 Web 应用领域的攻击。他曾在 Black Hat USA、Black Hat EU、DEFCON、PacSec 以及 Syscan 等安全大会上做过演讲，并且还是 FreeBSD 项目的贡献者之一。

其他贡献者

Jesse Bruns 是 iSEC Partners 的创始人之一并且担任研究部的副经理。Jesse 被认为是移动应用安全和包括 Android OS 在内的移动平台领域的领军人物。除了移动安全研究之外，Jesse 还从事渗透测试、开发安全工具并领导公司内的独立研究。

Jesse 拥有超过 10 年的软件工程师和安全顾问的经验，并且协助许多业界最大的以及技术需求最迫切的公司满足其应用安全需求。另外，他带领过许多开发团队，设计和开发了基于 Windows 授权的企业号簿管理系统，研发了底层的安全工具，为美国一家大型经纪商建设了交易和支撑系统，为支持像 SSO 等安全特色进行架构设计以及设计了大规模框架。Jesse 也编写网络应用，如 web 爬虫、启发式分析程序等。在创建 iSEC 之前，Jesse 是 stake 公司的常务安全架构师。

Jesse 曾经在全美以及全球的一些地点进行过演讲，包括 Black Hat Briefing、Bellua Cyber Security、Syscan、OWASP、Infragard 以及 ISACA。他也会对他的许多安全咨询客户就广泛的技术问题进行专门的安全研究的演讲，包括加密方法攻击、fuzzing 技术以及新兴的 Web 应用威胁。

Jason Chan 是 VMware 公司的安全主管。在加入 VMware 公司之前，他是 iSEC Partners 公司的安全顾问，致力于 IT 基础设施和专业服务。Jason 已经在安全领域工作了至少 10 年，致力于网络、系统以及应用安全、合规性及风险管理等多个领域。

Alex Garbutt 是 iSEC Partners 公司的高级安全顾问。Alex 在安全咨询领域有着丰富的经验，他经常实施应用渗透测试、代码审计以及网络评估。他也进行相关的研究，最近的研究关注于 RTP 协议。他编写了 RTPInject 工具，这是一款很棒的攻击工具，能够在已经建立的 RTP 连接中插入任意的音频信息。Alex 曾经在 Black Hat 以及 iSEC 开放论坛上进行演讲。

在加入到 iSEC Partners 之前，Alex 在加州大学戴维斯分校学习，师从于在数字安全领域知名学者。他以优异成绩毕业于计算机科学和工程专业并获得学士学位。

Zane Lackey 是 iSEC Partners 公司的高级安全顾问。他研究的关注点包括移动手机安全、Ajax Web 应用以及 VoIP。Zane 曾经在包括 Black Hat、Toorcon、MEITSEC、YSTS 以及 iSEC 开放论坛等顶级的安全会议上演讲。另外，他是《黑客大曝光：Web2.0 安全》（McGraw-Hill/Professional 出版社出版）的作者之一，也是 *Hacking VoIP* (No Starch Press)

的贡献者以及技术编辑。他在加州大学戴维斯分校获得经济学学士学位，并且辅修计算机科学专业。

Luis Miras 是一个独立的安全研究人员。他曾经供职于安全产品设备商以及业内领先的安全咨询公司。他的领域包括安全漏洞研究、二进制分析和硬件/软件逆向工程。过去他在数字设计和嵌入式编程领域工作。他在 CanSecWest、Black Hat、CCC Congress、XCon、Recon、Defcon 以及全球其他的大会上做过演讲。

技术编辑

Chris Topher Chung 于 1997 年加入 Intuit，并且是公司信息安全（Corporate Information Security，CIS）团队的员工信息安全分析师（Staff Information Security）。Topher 为 Intuit 产品和服务进行应用安全评估。在 2006 年之前，Topher 是 Quicken for Windows 以及 Quicken Health Care 等产品的高级软件工程师以及安全工程师。

Topher 拥有埃默里大学数学与计算机科学学士学位以及俄勒冈大学计算机信息科学硕士学位，在俄勒冈大学攻读硕士学位期间，他进行移动/普适计算/可穿戴计算领域的研究。

在工作之余，Topher 喜欢高尔夫、烹饪、自酿酒品、滑雪以及与爱妻 Mary Ann 和儿子 Connor 在一起享受时光。

谨以此书献给我的儿子，Shalin Dwivedi！

他的到来是我完成此书的最大动力。感谢 Shalin 那安静的、优雅的举止，以及之后那灿烂和调皮的笑容。

本书也同样献给我的女儿，Sonia Dwivedi，她略有急躁的性格以及对任何事物都抱有的无法估量的热情到目前为止，对一个父亲而言，是最大的动力。

另外，特别感谢我的妻子，Kusum Pandey，你为我付出如此之多，但很多我却不知情。你的不合常规的但是异常杰出的能力使我向行家不断前进，而这是我所低估的并且是重要的一种财富。

最后，既然这是我计划写作的最后一本书，我必须要感谢我的妈妈，Prabha Dwivedi，她的无形的但是可信赖的支持这么多年以来一直是我动力的源泉。从早前的学前时期到后来的大学时期，您一直以来的支持让我无法言谢。感谢您，妈妈，为您所付出的一切！我爱您！

——Himanshu Dwivedi

谨以此书献给给予我支持、鼓励和指导的家人以及 Kathryn。

——Chris Clark

致　谢

首先要感谢本书最重要的作者之一，Chris Clark，感谢他在本书编写过程中付出的巨大努力。本书是在 Chris 的带领下才拥有极高质量、严谨性及专业性。若没有 Chris 的付出，本书就不可能完成，因此，本书的出版主要归功于他。谢谢，Chris！

也要感谢本书的其他作者以及特约作者，是他们使本书如此完美、实践性强（从移动应用到移动平台）而又兼具技术深度。感谢 David Thiel、Alex Garbutt、Jason Chan、Zane Lackey、Luis Miras 以及 Jesse Burns。

此外，还要感谢出版社的 Jane Brownlow 和 Joya Anthony，由于他们的耐心、坚持以及灵活，本书的创作过程一直很愉悦。

最后，要感谢 iSEC Partners 的创立者创建了大量移动应用安全方面的资料，这些资料不仅帮我完成了相关章节，而且还帮我联络到了本书的最佳作者。

——Himanshu Dwivedi

感谢 iSEC Partners 公司提供了绝佳的环境，在解决富有挑战性的问题之时可以进行实验以及深入研究。感谢 Townsend Ladd Harris 和 Brian Hernacki 协助完成了 WebOS 相关章节。

——Chris Clark

前　言

移动计算已然来临。几十年了，一直说有一天计算机最终将变为手掌大小，而今这一天来到了，如今的移动设备具备了桌面机/笔记本电脑的功能。这一变革的第一步就是智能手机，也称为 PDA 电话，它内置有微操作系统，可供用户阅读邮件及访问互联网。阅读邮件和访问互联网是很重要的功能，但毫无疑问，推动移动手机从只是笔记本电脑的延伸到逐步替代笔记本电脑的关键是手机上的移动应用。与 19 世纪 80 年代相似，那时主要推动因素不是桌面机上的硬件，而是在其上能够应用的不同类型的软件。之所以应用移动设备，主要是因为其所支持的应用程序，而不是因为它有台式机的功能。Apple iPhone 就是一个非常好的例子，用户转向使用这款移动设备，是因为它上面有许多应用，而不是仅仅因为它能够用来检查邮件和访问互联网。除了 iPhone，还有 BlackBerry，它们将许多商务功能扩展到了用户的手中，包括美国第 44 任总统。除了 iPhone 和 BlackBerry，市面上还有一些新的力量，例如 Google Android，一些熟悉的面孔，如 Windows Mobile，以及 Symbian 系统，它几乎随处可见。

除移动应用外，移动革命的另一个重要催化剂是通信技术的不断发展，特别是带来了具有广阔的无线自由的高带宽技术。举例来说，802.11 不久前在移动设备上得以支持，给用户带来了带宽，但并没有给用户在离开家庭/办公室时仍能保持连续连接的自由，而这则是真正移动性的重要部分。具有高带宽的真正的端到端自由所带来的通信模式是移动设备取得成功非常关键的一部分。例如，在轻量级的硬件上内置轻量级操作系统实现时相对容易，但是集成无线宽带功能却用了较长的时间。在此之前，用户虽然也能够同步数据，但是因为速度很慢，这种功能很快就变得无人问津。一旦“移动通信模式”能够提供足够高的带宽，给用户一个持续在线的模式，用户对这些移动设备（以及为这些设备编写的应用程序）的接受程度就会显著增加。这种转变给数据带来的是非常实在的特性，将令其“无处不在”。

本书概览

至此，我们已经回顾了移动设备面临的一些挑战，下面介绍本书如何来解决这些挑战。

本书分为两个部分，第一部分是移动应用平台，包括第2～8章。这些章节讨论了移动设备上的主要操作系统平台，包括 Google Android、Apple iPhone、Windows Mobile、RIM BlackBerry、J2ME 以及 Symbian。这些章节主要讨论如何应用这些平台来开发安全的应用。例如，在其中解决了第一章中列举的 15 大问题中的许多个，包括安全存储、应用隔离以及恶意软件线程。对于那些对利用这些平台的安全模型感兴趣的应用程序开发人员而言，这些章节应该看做是一份操作指南。许多内容在各章节之间是共享的，因此，可以在阅读关于 Google Android 应用程序隔离的章节时，将之与 Apple iPhone 和微软 WinMobile 部分中相同的章节进行对比。操作系统的几章包含了许多相同的内容分类，例如应用程序隔离、应用签名以及更新升级，因此读者可以在它们之间进行对比和比较。同时，也有具体针对某一平台的内容分类，例如应用程序商店的具体实现方式。在阅读了所有这些操作系统基础章节之后，一定要看一下第 13 章，该章精炼地概括了这些移动平台。

本书的后半部分内容更加多样，讨论了第 1 章中提到的 15 大问题中的一些具体攻击类型，也介绍了新的关注领域，例如 SMS 和蓝牙的相关安全问题。这些章节并不一定和移动应用直接相关，但是随着许多移动应用开始利用蓝牙、SMS 或者 GPS，这使得这些章节也成为了相关的部分。这些章节将帮助读者完全掌握 15 大问题中的许多技术问题，以及一些新的问题。例如，虽然 SMS 并不是一个移动应用，但它在许多移动应用程序中大量应用，甚至是用于安全目的。用户向某一特定短信号码发送请求短信，在确定短信来自某一手机号码之后，许多银行网站会向用户发送一些银行账户信息（详细讨论见第 8 章）。这种融合将移动手机上的 SMS 功能/不足与移动 HTML 关联到了一起，并使得讨论 SMS、蓝牙、GPS 以及其他与应用层融合的手机功能变得重要。

目　录

第 1 部分　移动平台