HZ BOOKS
华章科技

Mc Graw Hill Education

信息安全
技术丛书

黑客大曝光

移动应用安全揭秘及防护措施

[美] Neil Bergman Mike Stanfield Jason Rouse Joel Scambray 著
张普含 董国伟 王欣 邵帅 等译

Hacking Exposed
Mobile Security Secrets & Solutions

- 全球顶级移动安全顾问团队亲力打造，融合作者30余年Web安全从业经验，全面解读移动应用面临的各种安全问题，并提供有效解决方案
- 详细讲解移动网络、iOS和Android平台的细节，深入剖析威胁建模、安全编码和针对移动应用的特定软件维护实践方法，为移动应用开发者提供系统而实用的安全开发指南

机械工业出版社
China Machine Press

黑客大曝光

移动应用安全揭秘及防护措施

Hacking Exposed

Mobile Security Secrets & Solutions

[美] Neil Bergman Mike Stanfield Jason Rouse Joel Scambray 著

张普含 董国伟 王欣 邵帅 王眉林 时志伟 郝永乐 译

机械工业出版社

China Machine Press

图书在版编目（CIP）数据

黑客大曝光：移动应用安全揭秘及防护措施 /（美）伯格曼（Bergman, N.）等著；张普含等译 . —北京：机械工业出版社，2014.10
（信息安全技术丛书）
书名原文：Hacking Exposed: Mobile Security Secrets & Solutions

ISBN 978-7-111-48265-9

I. 黑… II. ① 伯… ② 张… III. 移动通信－安全技术 IV. TN929.5

中国版本图书馆 CIP 数据核字（2014）第 241727 号

本书版权登记号：图字：01-2014-0323

黑客大曝光：移动应用安全揭秘及防护措施

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）

责任编辑：吴　怡　　责任校对：殷　虹

印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2014 年 11 月第 1 版第 1 次印刷

开　　本：186mm × 240mm　1/16　　印　　张：14.5

书　　号：ISBN 978-7-111-48265-9　　定　　价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

The Translator's Words 译者序

随着信息技术的飞速发展，互联网日益成为人们生活中不可缺少的一部分，社交网络、微博、移动互联网、云计算、物联网等各种新技术、新应用层出不穷。但不管是 Facebook、Twitter 等新兴互联网公司的迅速崛起，还是 Android 日益成为智能手机市场的主流操作系统，信息安全一直都是永恒的话题。“震网病毒”和“火焰病毒”事件凸显网络武器的实际破坏能力，关键信息基础设施保护已成为世界各国网络空间防御的新重点；“维基泄密”事件彰显网络空间攻防双方的不对称性，百密难免一疏成为保密防范永远的痛；“斯诺登”事件更是把信息安全的威胁推到了风口浪尖。究其根源，所有这些信息安全事件都存在一个共同点，那就是信息系统或软件自身存在可被利用的安全漏洞。因而，漏洞分析和风险评估日益成为信息安全领域理论研究和实践工作的焦点，越来越引起世界各国的关注与重视。

为推动我国漏洞分析和风险评估工作的发展，提高国家信息安全保障能力和防御水平，中国信息安全测评中心长期跟踪和关注相关领域的理论进展和技术进步，有针对性地精选一些优秀书籍译成中文，供国内开发人员参考借鉴。

目前，移动设备中集成了丰富的应用和信息，这使得移动设备迅速普及，应用日益广泛，但同时也使得为其开发产品并保障安全更具挑战性。本书直接阐述了这些挑战，给出了移动网络、iOS 和 Android 平台与安全相关的细节，同时也为移动应用开发者开发安全的产品提供了详细的指导，并提出了从威胁建模逐渐深入到安全编码的软件维护实践方法。本书还覆盖了服务器端安全，以及与企业用户相关的话题。总之，本书对任何开发、管理移动应用的从业人员来说，都是一本重要参考手册。

参与本书翻译的人员有：张普含、董国伟、王欣、邵帅、王眉林、时志伟、赫永乐。

本书的翻译工作得到中国信息安全测评中心“漏洞分析与风险评估”专项工程、国家自然科学基金项目（61100047、61272493）的支持。

序言 *Foreword*

从20世纪90年代中期开始，移动设备经历了戏剧性的变化，从庞大、单用途计算环境转变为通用计算环境。第一代数字移动电话是嵌入式系统，仅将极小的空间分配给第三方软件（third-party software）。随着1991年J2ME和2001年BREW的出现，移动电话的基带处理器开始将第三方软件应用处理作为自己的第二功能，消费者第一次可以选择在自己的手机上运行的应用软件。

移动设备从嵌入式系统到现代计算平台的演进经历了一个众所周知的过程，如同Daniel P. Siewiorek、C. Gordon Bell和Allen Newell在《Computer Structure: Principles and Examples》中描述的那样：从大型计算机到小型计算机再到台式计算机逐步演进。移动设备从单功能固件演化到可安装软件和鲁棒应用的环境，从只有低速处理器、受限内存和受限操作系统能力的单进程系统演化到拥有高速处理器、可扩展内存、专用协处理器和可同台式计算机相媲美的操作系统能力的多任务系统。现在的移动设备拥有和台式计算机相同规模的计算能力和网络吞吐率，以及匹配的音频和视频能力。可以证明的是，无处不在的3G和4G移动网络给移动电话提供了比台式计算机更加普遍的网络资源访问量。然而，移动设备拥有的一些能力和限制有其特殊性。

在移动设备上的用户界面是受限的。以前输入和显示的技术不够成熟从而限制了用户接口，而现在设备的物理尺寸是最大的限制，限制移动设备可以显示的信息数量以及可以对用户输入进行的操作。便携式计算机把人类视觉能力和典型的观看距离计算在内，可以显示十倍于移动电话的信息。触摸屏增加了屏幕控制目标的尺寸以弥补指尖自然尺寸给移动设备用户可操作范围带来的局限。

移动设备由于尺寸小在便携性方面有明显的优势，使得用户在任何时间都可以携带这些设备。这种设备从空闲状态到活跃模式可迅速转换，使用户可以立即访问计算机资源，用户与移动设备交互通常只需要几秒或者几分钟。移动设备的及时性和普遍性使我们能够在非常私人的空间里使用。我们的绝大多数个人通信都依赖于移动设备，并且在其中存储

绝大部分的个人信息。

移动设备拥有在其他计算机环境中不通用的一些硬件能力。触摸屏普遍存在，并且经常通过运动传感器来增强功能。无论是基于 GPS 还是基于网络的位置系统都由规章授权。环境传感器，例如温度、光度和距离也都是常见的。所有这些特性使得移动设备存储了可能是个人的且私有的额外数据。

在台式计算环境里，终端用户（或者是他们的 IT 部门）通常对计算操作系统的工作具有洞察力甚至对其负有责任。在台式计算机上，用户可以阅读日志文件，并且更改软件配置。移动环境通常对普通用户隐藏操作系统，这样用户通常不能监控它的行为。移动设备中的第三方软件通常在一个沙箱（sandbox）环境里运行，对操作系统功能的访问受到控制，并且与其他应用软件的通信也受到限制。与台式计算环境不同，中心应用分配器通常管理控制移动设备中第三方软件所占的盘区。

移动应用开发者面临的挑战是提供好的移动体验，同时保护好丰富的个人信息。由于用户越来越期待实时响应和从网络服务处获得不间断的信息流，因而移动应用需要充分利用移动平台具有的计算能力和便捷性。同时，应用开发者需要通过简化配置和默认处理错误条件的方式来对用户隐藏应用的复杂性。移动设备一般是面向消费者的平台，这使得企业开发者很难交付既满足企业需求又符合企业规则的应用。开发者最终对交付用户可信的服务和品牌负有责任。

所有这些事情都给移动环境中的安全性提出了新的挑战，并且较其他计算环境而言在熟悉程度方面的挑战更大。移动应用依赖于客户端和服务器之间的频繁通信，并且极大地依赖于服务器存储和数据处理，这也就意味着个人信息会出现在移动设备和云中。移动设备硬件提供了个人的敏感信息，例如用户位置，而这些信息是需要适当保护的。由于操作系统一般是受保护且不可扩展的，并且故障修复周期更长，因此降低安全缺陷的机会是有限的。

移动设备的界面限制使得设计复杂安全的交互变得不切实际。如果发生错误，会使用有限的信息提示用户，而且对于用户来说很难发现问题或解决自身问题。在移动设备上，即使是常用的交互形式，如使用用户名和密码登录，都是冗余的。因为用户可能没有配置移动应用的能力。移动应用开发者必须代表用户做出安全决定，同时提高可用性。在受限环境下，用户必须信任应用开发者，破坏这种信任就会极大地破坏开发者的品牌。

移动设备具有丰富应用的平台和单机应用，这个新的计算环境已经在计算领域确立了相应的地位，极大地扩展由桌面和云提供的计算资源。这些特质使得移动设备有趣且易于

使用，同样也使得为其开发产品和保障其安全更具有挑战性。本书直接阐述了这些挑战，同时包括针对移动应用开发者的详细指导，还包括从威胁建模开始直至深入安全编码，以及针对移动应用的软件维护方法。本书提供移动网络、iOS 和 Android 平台的大量细节信息，来帮助开发者保障他们应用的安全性。本书也覆盖了服务器端安全和企业用户相关的主题。对任何开发、发布、管理或使用移动应用的人们来说，本书都是非常有用的资源，同时也是对于行业观察者的一个深度指导。

——Kai Johnson

Isis Mobile Commerce 首席架构师

Preface 前言

为什么写这本书

移动设备是伟大的技术革命，可与互联网的产生相提并论。当然，巨大的改革也会伴随着潜在的风险，那么有没有这样一个“银弹”来保护各处移动的手机呢？本书介绍最新的移动安全趋势，以及由全世界移动安全领域顶尖从业者提出的技术分析与解决方案。

谁需要阅读这本书

本书为使用移动设备的人们敲响了警钟。这些设备所传达的“世界就在你手中”的力量也具有黑暗的一面。本书将展示能帮助你发现自己正身处的许多黑暗面，以及如何从黑暗中走出来的方式。

本书主要针对以下读者：

- 移动 app 开发者
- 全体 IT 从业者
- IT 顾问
- 技术管理者和领导者
- 终端用户

这些人是我们每天都要打交道的人，他们可以识别和修复我们在后续内容中叙述的问题，所以很自然，本书面向能够直接或间接改变移动技术环境以提高安全性的那些人。

同时，我们也将集中讨论当前主流的两个移动平台：苹果的 iOS 和谷歌的 Android 移动操作系统。当下，这两大平台所占有的市场份额如此之大，以致我们很难想象一个完全不同的未来，所以我们努力提供对这两个平台来说最相关的技术分析。

这本书主要内容

回顾 1999 年，《黑客大曝光》系列图书就开始介绍如何轻松入侵计算机网络和系统的方法。尽管直至现在仍然有许多人没有实际接触安全问题，但大多数人开始认为有必要理解防火墙、安全操作系统配置、厂商补丁维护，以及许多其他以前晦涩的信息系统安全基本原理。

《黑客大曝光》系列图书后来分为两个方向，本书将重点应对移动安全挑战。

首先，我们为移动设备将面临的严重威胁分类，并详尽解释这些威胁的具体细节。我们如何知道这些就是最严重的威胁呢？因为我们受雇于世界上最大的公司来入侵他们的移动应用，我们每日使用基于这些威胁的攻击进行工作。并且多年来，我们一直在研究最新发布的黑客技术，开发自己的工具和技术，并结合我们认为最有效的方法来渗透现存的移动应用。

其次，在介绍各种攻击之后，我们会告诉你如何阻止每种和每一次攻击。在不了解本书中信息的情况下部署一个移动应用就好比在驾驶一辆没有安全带的车去下一个很滑很陡的坡，绕过一个巨大的峡谷，没有刹车并且风门完全堵塞。

怎样使用本书

读者历来有这样的争论：是从第一页开始阅读还是跳到重要部分？我们说：两者皆可！

很明显，可以从头至尾地阅读这本书，以了解针对移动应用安全的包罗万象的内容。但是，《黑客大曝光》的写作模式是让每一章都能够独立存在，这样就可以以组建模块的形式来消化吸收这本书中的内容，适合于我们目标读者的疯狂计划。

我们严格坚持清晰、可读性好并且简明的写作风格，因此《黑客大曝光》系列图书获得了极大的读者反响。我们知道你很忙，并且需要最直接且没有模棱两可和冗余的术语的干货。一位《黑客大曝光》读者曾经写下这样的评论："读起来像小说，惊悚起来像地狱！"

我们认为从开始读到结尾很不错，但是用任何一种阅读方式均可。

本书组织结构

我们在第 1 章较为详细地叙述了本书目的：探索移动风险生态系统的最重要元素，面向这个领域的所有人员（移动 app 开发者、全体 IT 从业者、IT 顾问、技术管理者和领导者、终端用户）。基于作者多年亲身研究得到的移动安全经验，本书将包括的主题如下表所示。

章节	主题	描述
1	移动风险	移动恶意软件、BYOD、狮子、老虎与熊，天啊！移动安全从哪儿开始呢？我们将以一个关键移动利益相关者、资产、风险和趋势的广阔视角来尽量揭穿某些谎言
2	移动网络	就像物理攻击一样，如果你连接到一个恶意移动网络，那么你的移动设备便不再受你的操控
3	iOS 系统	苹果自我封闭式的商业策略是一个可靠的安全架构吗
4	Android 系统	谷歌强有力的技术和资金资源能够克服当前 Android 生态系统的原始边界吗
5	移动恶意软件	外部是一个快速进化的丛林。你能从简单或复杂的移动恶意软件所用的工具和技术中学到什么防御策略
6	移动服务和移动网络	不要被那些光鲜的设备所愚弄——安全中的真正问题在服务器端。学习移动服务需要采用的保证堡垒墙不被攻破的技巧
7	移动设备管理	MDM 为攻击者造成了多大的阻碍？相对于最有可能的攻击场景，对 MDM 的投资是否值得
8	移动开发安全	为想要证明其 app 具有安全性的开发者提供设计和实施指导
9	移动支付	类似于谷歌钱包的新服务展示了为敏感数据和交易而进行的首次大规模移动运用。我们能从设计、发布的漏洞及应对策略中学到什么
附录	其他	包括移动终端用户（消费者）安全检查表和一系列专业的移动应用渗透测试工具包

本书包括了很多来自全球顶级移动安全顾问的综合经验——你将如何使用它呢？

接下来介绍本书的其他一些特色，希望能有所帮助。

本书的基础构建模块：攻击和对策

本书是《黑客大曝光》系列图书之一，因此本书的基础构建模块与系列图书一致，每章讨论各种攻击和对策。

《黑客大曝光》系列图书的基础构建模块都类似，如下所示。

攻击图标

以这样的方式强调攻击，能使读者容易识别特殊的入侵检测工具和方法，并且为你提供某些强有力的信息，这些信息是你在说服管理者为你的安全创新措施投资时所必需的。

对策图标

这个图标应该引起读者对重要信息的注意。

其他图标

本书还有如下一些图标，提示读者。

这些图标用于强调那些经常易被忽视的小细节。

在线资源和工具

移动安全是一个快速发展的学科，我们承认纸质图书通常并不是跟踪该活跃领域所有最新动态的最充分媒介。

因此，我们创建了一个网站来跟进与书中讨论主题相关的最新信息，并包含整本书涉及的勘误表及公共流通工具、脚本和技术。网址是：http://www.mobilehackingexposed.com。

我们还提供一个论坛可直接与作者沟通。我们希望大家在阅读这些章节的过程中能够经常浏览该网站以查看最新的材料，获取那些我们所提到工具的简单访问权限，并不断跟进移动安全始终变化的一面。否则，你将不会知道哪些最新发展成果可能在你还未防御之前就威胁你的移动设备。

结束语

我们为这本书倾注了所有的心血，真诚地希望所有的努力能够为你在保护移动基础设施和应用方面节省宝贵的时间。我们认为投入移动应用的安全领域就是勇敢而超前的决定，但是，正如你将会在本书中发现的一样，在应用程序上线的这一刻你的工作才刚刚开始。不要惊恐，开始翻阅本书并从中得到安慰，当下一个巨大移动安全灾难降临时，你甚至不会眨眼。

About the Auther 作者简介

Neil Bergman

Neil Bergman 是 Cigital 公司的资深安全顾问。他已经领导和组织了针对业界顶尖财经和软件公司内关键应用的渗透测试、代码审查和架构风险分析。他不仅组织了针对 Web 服务、Web 应用、活跃客户端的大量评估，也主导了许多移动平台安全评估，例如 Android、iOS 和 RIM。他的主要研究领域包括移动和 Web 应用的漏洞发现与挖掘。他毕业于 James Madison 大学并获得计算机科学硕士学位，于 North Carolina State 大学获得计算机科学学士学位。

Mike Stanfield

Mike Stanfield 是一名安全顾问，于 2012 年加入 Cigital 公司，该公司是企业软件安全咨询公司。作为 Cigital 移动安全实践的一部分，Mike 专门从事针对 iOS、Android 和 Blackberry 平台的应用安全评估和渗透测试，并且参与 Cigital 移动软件安全培训课程的开发和传授。他在移动支付平台，包括 GlobalPlatform/Java Card applet 的安全和开发等方面，都有相关的工作经验。在加入 Cigital 之前，他是 Indiana 大学学生事务部门的信息技术主管。同时，他也作为 Indiana 大学科研管理办公室的授权分析家，参与了开源项目 Kuali Coeus 的开发。Mike 现在居住在 Manhattan，在 Indiana 大学学习安全信息学，并且获得 Indiana State 大学的人类学学士学位。

Jason Rouse

Jason Rouse 在安全方面拥有数十年的亲身经验，这些经验都是从他为全球诸多顶尖公司服务的实践中得来的。现在，他是负责 Bloomberg LP 产品和服务安全团队的成员之一，同时还在探索如何能够重新开发可信计算和怎样将可信计算应用于普遍存在的生物测量学中。Jason 对于安全领域充满激情，他参与了提高 Bloomberg 安全效能和全球极其重要的安全项目上。基于他专业的贡献，他

还担任面向移动安全的金融服务技术组织委员会的主席，该委员会致力于提高移动安全性。在加入 Bloomberg 之前，Jason 是 Cigital 公司的首席顾问。他在 Cigital 参与了很多项目，包括创建移动和无线安全实践，实施架构评估，并且是全球一些超大型开发机构的可信顾问。在加入 Cigital 之前，Jason 与 Carnegie Mellon 的 CyLab 安全研究室合作创建了下一代移动验证和授权平台并扩展了计算机安全行业的状态。Jason 现在居住在 Manhattan，获得了加拿大 Dalhousie 大学计算机科学学士和硕士学位。

Joel Scambray

Joel Scambrary 是 Cigital 公司的主管经理。在过去的 15 年里，他帮助大量公司（从新近崛起的初创公司到财富 500 强企业）解决所遇到的信息安全问题，帮助公司抓住难得的机遇。Joel 的身份包括主管、技术顾问和企业家。他联合他人创建了信息安全咨询公司 Consciere，并在 2011 年 6 月 Cigital 收购 Consciere 之前，一直担任 Consciere 领导。他还是微软公司的高级主管，一直领导着微软在线服务和 Windows 部门安全方面的工作。他还联合创建了安全软件和服务新兴公司 Foundsone，该公司于 2004 年被 McAfee 收购。在此之前，他担任 Ernst & Young 的经理、微软 TechNet 的安全专栏作家、InfoMord 杂志的编辑，以及某主营商业实体房产公司的信息技术部门主管。

Joel 是信息安全方面一位广为人知的作家和演讲家。他参与完成了十几本信息技术和软件安全方面的著作，很多都是全球畅销书。他在很多大会和组织中进行过演讲，包括 Black Hat 等会议，IANS、CERT、CSI、ISSA、ISACA、SANS 等组织，私有公司，FBI 和 RCMP 之类的政府机构等。

他拥有加利福尼亚大学 Davis 分校的理学学士学位、UCLA 的文科硕士学位，以及信息系统安全专业认证（CISSP）。

参与者简介

Swapnil Deshmukh 是 Visa 的信息安全专家。他之前是 Cigital 公司的安全顾问，在此期间他帮助客户建立安全移动实践。他的职责包括：设计实施移动威胁建模、实施安全编码实践、执行源代码分析、二进制应用软件逆向工程和移动渗透测试。在加入 Cigital 之前，他在 MyAppSecurity 担任移动威胁分析师，在那里他设计和实现了一个移动威胁模型生成器。他获得了 George Mason 大学的计算机网络和通信理学硕士学位。

Sarath Geethakumar 是 Visa 的首席信息安全专家。他专门从事移动平台和应用安全，在移动安全研究中十分活跃。他的研究活动对于发现移动设备管理方法与平台安全能力有关的大量安全漏洞非常有效。除此以外，他在安全移动应用开发和 Visa 道德入侵方面都做

了大量工作。他曾任安全专家、安全顾问、首席架构师、软件开发者等。在加入 Visa 之前，他是美国万国宝通银行的信息安全专家和 Red Team 成员。作为咨询顾问，他还担任许多金融机构和财富 500 强公司的咨询专家。在形成跨机构的移动安全实践和培训移动安全专业人员方面，他都起到了至关重要的作用。

Scott Matsumoto 是 Cigital 公司的首席顾问，他拥有超过 20 年的软件安全和商业软件产品开发经验。在 Cigital、Scott 负责公司的移动安全实践，并且通过直接咨询、项目监督、培训以及软件开发，促成了 Cigital 的美国西部生意。他与许多 Cigital 的客户在安全架构方面进行合作，例如移动应用安全、云计算安全、SOA 安全、细粒度授权系统和 SOA 管理。Scott 在此之前完成了基于组件的中间件、性能管理系统、图形 UI、语言编译器、数据库管理系统和操作系统内核等的开发工作。现在，他是云安全联盟（CSA）的创始者之一，并且积极参与该联盟的可信计算计划。

Mike Price 现在是 Appthority 的首席架构师。作为架构师，他完全关注于移动操作系统和应用安全的研究与开发。他之前是位于 Santiago 的 McAfee 实验室的高级操作经理。在此期间，他与 Chile 以及拉丁美洲的外包组织合作，负责办公的平稳操作，并且广泛推广跨团队和领域的技术优势以及创新。他作为 Foundstone Research 团队成员长达 9 年。最近，他负责 McAfee Foundstone 公司漏洞管理产品的内容开发。在此期间，他与一个全球的安全研究人团队合作并管理他们，负责软件检查，用来远程探测操作系统和应用是否存有漏洞。他在信息安全领域有着丰富的经验，并且在漏洞分析和与信息安全相关的 R&D 领域工作接近 13 年。Mike 是一位作家，对《 hacking Exposed ： Network Security Secrets & Solutions》第 7 版中的 iOS 安全和 Sockets、Shellcode 及套接字编码和代码可移植性方面的 Porting & Coding 都作出了贡献。Mike 同时也是该书“计算机安全会议”的共同创建者，该会议每年在 Chile 的 Santiago 举办一次。Mike 也是本书的技术评论员。

John Steven 是 Cigital 公司的 CTO，他有超过 15 年的行业经验。John 的专业知识主要涉及威胁建模、架构风险分析、静态分析（强调自动化）和安全测试。作为首席顾问，John 为很多跨国公司提供策略指导。作为 CTO，John 指导 Cigital 公司的安全实践，他最大的兴趣在于将 Cigital 技术始终保持在顶尖地位。

技术审校简介

Gabriel Eacevedo 是 Cylance 的一名安全研究人员，与一个有多名安全专家的精英团队合作，来保护现实世界并以简单得体的方式解决每天遇到的繁琐复杂的问题。在加入 Cylance 之前，Gabriel 是 McAfee 实验室的安全研究人员。在此期间，他对 Microsoft Windows、Mac OS X、Unix Platforms、移动设备、安全应用和其他系统中的漏洞进行分

析。他的团队致力于软件检查的设计和实现，用以检测远程系统里的安全缺陷。在 McAfee 工作期间，他带领移动安全工作团队对嵌入式系统的安全性进行了分析研究。同时，他在 LTAM 中也是 McAfee 的发言人。他发表了由 McAfee 出版的重点关注 Chilean 全球电视和无线程序的白皮书和文章。同时，他也是发表于软件工程第 33 届全球会议上的科技论文《 Transformation for Class Immutability 》合著者，该论文由计算机机械协会出版。他的研究兴趣主要是信息安全研究、iOS 和 Mac OS X 内核，以及软件工程。

Acknowledgements 致谢

本书的顺利出版离不开许许多多人的支持、鼓励、投入与贡献。我们尽可能在此列出所有参与人员，并向那些由于我们的疏忽而遗漏的人们表示深深的歉意。

首先，衷心感谢我们的家人和朋友数月以来对我们研究和写作的支持。他们的理解和支持对于本书的顺利完成至关重要。希望完成另一本著作后就去陪伴他们。（我们对此承诺！）

其次，我们要感谢同行作者、合作作者和同事对这本书的贡献。特别感谢 Sarath Geethakumar、Mike Price、John Steven 和 Scott Matsumoto 对于本书严格的技术审阅和超乎预期的实质性贡献。

当然，十分感谢不辞劳累的 McGraw-Hill 出版团队，感谢他们为这本书所付出的一切，包括我们的编辑 Amy Jollymore、管理人员 Amanda Russell，他们使各项工作有序进行，还有艺术顾问 Melinda Lytle 和项目编辑 LeeAnn Pickrell。所有这些人员在面对十几位具备各自独特风格、方法和创造性机制的合作作者所完成的各种各样的内容时，都保持了冷静的头脑。

我们也要感谢 Gary McGraw、Sammy Migues、John Wyatt 和 Cigital 整个团队的许多人，他们为本书中讨论的大量主题提供了材料和指导。另外，我们衷心感谢 Bloomberg 的同事所给予的源源不断的支持。

衷心感谢 Kai Johnson 的长期支持、对于原稿的反馈意见以及他在前言中的杰出评论，同时还要感谢为本书草稿慷慨提供评论的所有同事。

我们一如既往地向全球有洞察力和创造力的黑客们，尤其是那些定期通信反馈的黑客们致敬，他们持续地进行创新并不断地向《黑客大曝光》系列书籍提供原材料。

最后，深深地感谢所有《黑客大曝光》书籍的读者朋友，正是由于你们的不断支持才使得所有的辛苦工作都是值得的。

——全体作者

目录 *Contents*