HZ BOOKS 华章IT

Mc Graw Hill Education

信息安全技术丛书

资深无线网络安全专家撰写，既包含当前常用网络的各种技术，也包含新型的无线技术的入侵，是利用和防御最新无线网络攻击的权威指南

以当前主流的Windows、OS X和Linux操作系统作为主要的描述对象，涵盖民用、工业和物联网及智能家居领域的无线通信，以实践为主，详化攻击过程和操作步骤，深入剖析各种技术

黑客大曝光

无线网络安全

（原书第3版）

[美] 乔舒亚·莱特（Joshua Wright） 约翰尼·凯诗（Johnny Cache） 著 李瑞民 译

HACKING EXPOSED WIRELESS

WIRELESS SECURITY SECRETS & SOLUTIONS

机械工业出版社 China Machine Press

信息安全
技术丛书

黑客大曝光

无线网络安全

（原书第3版）

[美] 乔舒亚·莱特（Joshua Wright） 约翰尼·凯诗（Johnny Cache） 著 李瑞民 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：无线网络安全（原书第 3 版）/（美）莱特（Wright, J.），（美）凯诗（Cache, J.）著；李瑞民译 . —北京：机械工业出版社，2015.12
（信息安全技术丛书）
书名原文：Hacking Exposed Wireless: Wireless Security Secrets & Solutions, Third Edition

ISBN 978-7-111-52629-2

I. 黑… II. ①莱… ②凯… ③李… III. 无线网 – 安全技术 IV. TN92

中国版本图书馆 CIP 数据核字（2015）第 314267 号

本书版权登记号：图字：01-2015-5223

黑客大曝光：无线网络安全（原书第 3 版）

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：李　艺　　责任校对：董纪丽
印　　刷：三河市宏图印务有限公司　　版　　次：2016 年 3 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：33.25
书　　号：ISBN 978-7-111-52629-2　　定　　价：99.00 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）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

The Translator's Words 译者序

在关于网络攻防技术的讨论中，常会遇到一个有趣的现象：一说起“攻”，大家马上就会认为这是“邪恶方”做的事，做这件事的人每天戴着墨镜，行为神神秘秘，目的不可告人；而一说起“防”，似乎就是“正义方”做的事，做这件事的人必须得西装革履，还要表情严肃，一脸正义。然而事实上并不是这样，也不需要这样。因为无论是攻还是防，都只是对网络安全性的一种设计和改进，二者没有谁正义谁邪恶之说。相反，将二者结合起来，反而会相互促进，使双方都能达到螺旋式地提高的效果。

这一点，在本书和现实中都体现得淋漓尽致。以我们的日常生活为例，拿出智能手机连接合适的 Wi-Fi 网络（即 SSID 网络），俨然成为“低头族”“手机控”每天的必修课。如果对网络再熟悉一些，那么我们还知道无线加密的技术有“ WEP 加密认证”“ WPA/WPA2 加密认证”“ WPA-PSK/WPA2-PSK 加密认证”等多种加密认证方式。为什么在短短的十几年时间内，无线路由器认证技术得到了这么快的发展？究其原因，就是“防”的一方，每有一种新技术被设计出来后，就被“攻”方破解，而要弥补这一技术的不足，避免被“攻”方再次破解，“防”方就不得不研发出更新、更安全的防守技术。于是，这种此消彼长的竞争，促进了双方的提高，也造就了越来越安全的系统。

越来越多的 IT 专业论坛都在预测 IT 行业的未来，民用无线通信、工业无线通信、物联网、智能家居都是当下研究的热点和重点，而这同样也是本书的重点。本书整体分为三个部分，每一部分又根据技术的分类分成了不同的章节。纵览全书，第一部分主要介绍的是民用无线通信，而第二部分主要介绍工业无线通信，第三部分则主要倾向于物联网和智能家居领域内的无线通信。从这里，我们也可以看到无线网络安全发展的一些理念变化，例如基于 Wi-Fi 的无线通信，普遍用于日常生活中，涉及百姓的生活安全，所以无疑会向大而全的复杂设计模式发展；而工业无线通信，更注重于低成本、低功耗、大范围推广的设计理念，因而第三代的工业蓝牙调整了自身的发展方向，不再追求大而全、面面俱到的设计模式，转向改

为低功耗蓝牙的简单设计模式，呈现出向物联网靠拢的发展脉络。这种设计理念的差异和走向，体现了无线网络发展中的多样性。

很多人都有黑客梦，不为金钱，不为名利，只为“运筹键鼠之间，决胜千里之外”的成就感。然而真正的黑客寥寥无几。究其原因，就是黑客之路需要具备对新知识的快速接受能力、平时沉下心来做事的坚强毅力，还有可遇而不可求的好运气。不过，如果非要从每天日新月异的“技术堆”中找到一个终南捷径，那就是“取人所长，补己之短”，找对“良师益友”，直接从别人已得到的成果中学到方法，体会其成功之道，举一反三地应用到自己的实践中。而本书，恰是这样一本以实践为主，详化攻击过程和操作步骤的图书。更为难能可贵的是，书中还会讲到针对某一技术的使用历史，两种或多种工具之间攻击效果的对比。为了让读者对每种攻击方式有一个直观的了解，本书作者还独具匠心地将每种技术或漏洞根据其流行性、难易度、影响力、危险级四项参数分别进行定级，这样不仅可以使读者对该技术有新的了解，还能让网络安全人员对如何评价这种危险有所参考。值得一提的是，除了书中的内容，本书还提供了一些扩展章节和书中样例的附件文件，这些都可以从该书的配套网站上免费下载。

综合来看，本书既包含了当前常用网络的各种技术，也包含了前沿新型的无线技术的入侵和防护技术。绝大多数的技术细节都以当前主流的 Microsoft 的 Windows、Macintosh 的 OS X 和 Linux 操作系统作为主要的描述对象，这样既满足了各类操作系统用户的需求，也可以了解问题的普遍性。并且，正如本书作者所说，针对部分读者的建议，在本书第 3 版明显增加了在 Windows 操作系统下攻防技术和攻防工具方面的比重。这对于使用 Windows 系统较多的中国读者来说，无疑是一个不错的消息。

翻译的过程，是一个对自己掌握知识进行梳理、汇总的过程，是一个新知识、新动向的学习过程，也是一个与作者进行交流、探讨的过程，相信读者在阅读中也会有同样的感受。然而限于译者的水平和中西方文化的深层差异，书中难免会有曲解或错误，诚挚欢迎大家斧正。

李瑞民

2015 年 11 月

About the Authors 关于作者

· Joshua Wright

Joshua Wright 是 Counter Hack 公司（美国新泽西州的一家反黑客公司）的一名高级技术分析师，也是 SANS 研究所的高级讲师和作家。依靠渗入攻击测试工程师的经验，他同时为上百家移动设备、无线系统、开环信号产品和知名组织产品缺陷的攻击和防守工作。作为一名开源软件倡导者，Joshua 在软硬件安全评估通用工具方面进行最前沿的研究，这些工具应用于 Wi-Fi 网络、蓝牙网络、ZigBee 网络、Z-Wave 无线系统、智能网格部署、Android 和 Apple 公司 iOS 的移动设备平台。

· Johnny Cache

Johnny Cache 于 2006 年获得“美国海军研究生院”（Naval Postgraduate School）计算机科学专业硕士学位。他的论文主攻 802.11 指纹设备驱动程序，因其在计算机科学领域最具创新性而赢得了“Gary Kildall”[㊀]奖。Johnny 于 1988 年某一时间，在 Tandy 128K 彩色计算机上编写了他的第一个程序，从那时起，他曾在几个安全组织会议上发言，包括黑帽子组织[㊁]（BlackHat）、蓝帽子组织[㊂]（BlueHat），以及 Toorcon 组

㊀ Gary Kildall，微型计算机早期操作系统 DOS 的设计者之一。——译者注

㊁ 黑帽子组织，发起于美国的一个国际黑客组织，主要以“黑帽简报”的形式在世界各地举办技术性很强的信息安全会议。另外“黑帽”和“白帽”本身也是对黑客进行分类的一个代名词，其中“黑帽”黑客注重于恶意攻击，带有破坏性；“白帽”黑客注重于攻击技术和防守技术的研究，且从不进行破坏性实战。有时，还有“灰帽”一词，介于“黑帽”和“白帽”之间。——译者注

㊂ 蓝帽子组织，名称仿于黑帽子组织，由 Microsoft 创建，“蓝帽”会议每年举办两次，旨在通过与黑客之间的交流提升自己产品的安全性。——译者注

织[⊖]。他还发表了一系列与 802.11 安全有关的论文，同时也是许多无线工具软件的作者，还是 Cache Heavy Industries 的发起人和首席科学官。

关于参编作者

· Chris Crowley

Chris Crowley 是位于华盛顿特区的莫坦斯（Montance）咨询公司的所有人，从事渗入攻击测试、计算机网络防御、灾害事件响应、分析取证契约工作。作为 SANS 研究所的资深讲师，负责“移动设备安全”（Mobile Device Security）和“道德入侵”（Ethical Hacking）课程的讲授工作。Chris 为上千个组织工作，职责是帮助他们在移动和无线系统中鉴定和分析漏洞，以及定位致命缺陷等问题。空闲的时候，他还会用极限攀岩活动来缓解工作的压力。

· Tim Kuester

Tim Kuester 是马里兰州哥伦比亚市“战术网络解决方案”（Tactical Network Solution，TNS）组织的一名工程师。他有在“一站式工程”（turnkey engineering）的背景（该项目的范围从 CubeSats 卫星和 BioMed 生物医学设备研究，到间谍小配件和真空吸法器研究），平时喜欢嵌入式系统、无线通信、电路板等系统的入侵项目。除此之外，他还在 TNS 总部从事“软件无线收发”（software-defined radio）课程和“信号处理”（signal processing）课程的兼职讲授工作。工作之外，他还爱好业余无线电技术、步枪打靶射击、EMS 邮政特快专递服务等方面。Tim 特别感谢他的父母，以及他在马里兰大学巴尔的摩郡分校（University of Maryland，Baltimore County，UMBC）给予他悉心指导的工程教授。

关于技术审校人员

· Tim Medin

Tim Medin 是 Counter Hack 公司的一名高级技术分析师，也是 SANS 研究所的资深讲师。作为一名专业的渗透入侵测试人员，Tim 曾为数百个组织工作，这些组织包括财富 100 强企业，以及美国政府，其职责是在关键流程中，识别和使用系统弱点，进而保护关键网络。在创新的“网络战”（NetWars）程序方面，作为技术领先者，Tim 领导了一个信息安全的开发团队，学员从高中生到退休的美国退伍军人，主要研究那些对教育行业、评估行业、竞赛行业的挑战信息安全内容，并最终将这些人培养成才华横溢的分析师。只要不是正在那些遍布全

⊖ Toorcon，发起于美国加州圣迭戈市的一个相对较新的年度计算机黑客安全会议。——译者注

球的协议（如 Kerberos 协议）中查找致命漏洞，Tim 则喜欢和家人待在一起。

· Mike Ryan

Mike Ryan 是 iSEC Partners 组织的高级安全顾问（这是一个信息安全组织），主要从事渗透测试并专职红队的训练，同时兼顾网络渗透式入侵，嵌入式平台研究。另外，Mike 还研究蓝牙安全，在专门针对蓝牙低功耗模式进行攻击的“超牙”（Ubertooth）项目中，在超牙的性能增加方面取得骄人战绩。从 2002 年起，Mike 在安全领域，由先前的单一方式转换为另一种方式，如今已具备集各种技能、巧术，以及任何情况下将 Leet 语[㊀]带到台面上的能力。

· Jean-Louis Bourdon

Jean-Louis Bourdon 是一名固件工程师。在 Infineon 处理器的设计方面拥有十年工作经验，在嵌入式系统方面拥有五年软件开发经验。现在，他在位于英国的 Pektron 公司工作，从事超级汽车和顶级汽车的仪表组设计工作。他的爱好经常是与技术相关，如拆解那些可以拿在手中进行详细分析的最新产品。

㊀ 黑客界俚语的一种，非常像中国年轻网友中使用的“火星文”，是将要使用的字符用其他形似、反转的、拆分的、重要特征相像的字符代替。如“7”表示“T”，“15”表示“is”，所以“\0vv 15 7-3 71v3.”表示“Now is the time”。——译者注

序　言 Preface

我第一次关注无线通信安全大约是2001年，那时针对“有线等效保密协议”（Wired Equivalent Privacy，WEP[⊖]）的攻击正大行其道。突然之间，数据网络通过空气传播，同样也是突然之间，这些网络的安全问题都深受其累。

对于无线网络的安全，总是存在大量激动人心的事情。无线网络的攻击不再需要以往的物理接入或网际互联！只要有一根好天线，监听者就可以从很远的距离监听一个网络！

随后的几年里，基于Wi-Fi的攻击工具和攻击技术变得越来越先进。尽管网络安全也在提高，但攻击者总能比防护者“领先一步”。这段时间以来，我对无线领域的安全越来越有兴趣，并从一些包括本书作者在内的802.11协议安全专家那里学到了一些重要的概念和技术。

最后，我将注意力转向其他无线通信协议。我很快意识到自己如果不动手开发一些发送和接收数字无线信号的工具集，那就意味着我几乎无所作为。Wi-Fi工具集便捷实用，并且功能异常强劲，这些工具使我受益匪浅，也让我学习了很多无线网络安全的通用原理。终于，借助工具集，在开始创建一些提供类似功能的工具以后，我就可以检测其他无线系统的安全了。

最初，我使用“软件无线收发”（Software-Defined Radio，SDR）开发平台来创建我自己的工具集。我是一个“软件独行侠[⊜]”（software person），极度热衷于“软件无线收发”SDR技术中，关于“允许无线电通信功能是生成到软件中，而不是生成到硬件中”的承诺，不幸的是，要达到这些目标，我发现我需要大量数据信号处理方面的背景知识。在最终掌握了这些知识后，我了解到实际上要设计这种对口工具，原本可以付出更小的代价。我所设计的一个平台是一个蓝牙测试工具，命名为“超牙一号”（Ubertooth One），可以在蓝牙设备处于“非可发现

⊖ WEP协议是对两台设备间无线传输的数据进行加密的方式，由于算法存在几个弱点，所以随后被WPA和WPA2协议所取代。但是不了解的用户常误将其选为当前协议，所以现在该协议仍然经常是被攻击的对象。详见本书第3章。——译者注

⊜ 软件独行侠就是软件开发过程中的设计、编码、测试、包装、发行都集于一身的人。——译者注

的”模式下仍然进行侦测。

如今，形形色色的无线技术在源源不断地开发出来，而无线通信领域的安全也比以往活跃。诸如对于 Wi-Fi 和蓝牙这些通行的技术，除了有那些专为针对它们的对口工具集之外，还有这些“软件无线收发”开发平台的通用工具集，并且后者正在变得更加廉价、易于使用。无线嵌入式系统正在迅速普及，新的无线通信协议似乎也在不断浮现，这导致我们永远难以找到合适的时间去探索这些系统中的安全问题。

在无线安全方面，这本书是我所知道的最佳参考。我希望那些学习无线通信系统的从业者可以好好读一读这本书。我也希望那些想获得更多安全知识的无线通信专家可以好好读一读这本书。尤其是对于那些数字无线电协议的设计者，我更推荐他们好好读一下这本书。因为对于了解一个新系统的安全来说，没有比通过实验成功地攻击之前的系统更行之有效的方法。

当我们快速开发一个新的无线通信协议时，那些已标准化的协议也更受欢迎。这些老系统中的安全问题，成熟得就像我们知道如何对抗那些熟知的攻击方式一样。Wi-Fi 通信协议在安全方面是一个最好的例子，这得益于该协议被开发人员长年累月地研究和完善。如今，搭建一个可以弹性抵御攻击的、基于 802.11 协议的网络是可能的，而部署一个几乎没有，或根本就没有安全可言的网络也是可能的。你甚至可以使用安全问题诸多的“有线等效保密协议”加密算法来配置一个的新网络，不幸的是，一些人还真仍在这么做。

通过本书，你可以愉快地学到关于无线安全的一切内容，包括“ Wi-Fi 保护配置协议”（Wi-Fi Protected Setup，WPS）的弱点，以及诸如“蓝牙低能耗”协议等时髦的协议。你可以学到如何使用琳琅满目的基于“目的创建”的工具，也可以在 Wi-Fi 客户端系统中发现其多种多样的缺陷，还有就是通过重新定义部分无线电芯片目标的方法来攻击 ZigBee 网络与 Z-Wave 网络。在看过“软件无线收发”的产品部署以后，在使用其入侵无线协议的各个重要技巧上，你也可以获得一种跳跃式的提升。我甚至希望你借以破解一个或两个“有线等效保密协议”密钥。

总之，我希望你能愉快地探索令人振奋的无线安全领域。

Michael Ossmann

Great Scott Gadgets[⊖]团队的创始人

⊖ 这是一个着力于无线入侵技术研究的团队，主要研究内容是通过软件对无线收发信号进行定义，进而实现对无线数字信号的监听和入侵，团队主页为 http://greatscottgadgets.com/，软件开源，主要产品是 HackRF One、ANT500、Ubertooth One、Throwing Star LAN Tap，这些都将在本书中有所体现。——译者注

前　言 Preface

也就是一年以前，麦格劳－希尔教育出版公司的编辑找到我，谈及本书第3版的撰写事宜。当时，我们并不确定这是一件好事，因为当时每天的工作、会议计划，以及正在做的项目，使我们没有几乎没有时间投入到如此巨大的项目中。

现在回过头来看，我们很欣慰于当时做出了写作第3版的决定。首先，这是必须的！因为自从几年前本书第2版出版以后，黑客无线攻防技术变化非常之大。其次，我们可以将第2版出版以后研究的新协议、开发的新工具，通过本版与读者进行分享。再次，写这本书意味着这是一个保持信息共享的良好机会，因为无线是计算机网络安全的“瑞士奶酪（Swiss cheese）重叠孔”[⊖]。

关于本书

在开始写作之前，我们讨论了在本书第3版中要写什么。我们要写的应该是务实的、有用的、注重实践的内容，注意实践意味着读者可以通过该方法进行渗透式攻击的测试与安全评估。因此，每章开始的第一节都描述某个被黑客攻破的技术案例，并不是用大量并不重要的背景知识打乱你的头绪，而是介绍一些底层协议以方便理解其原理。随后，在必要的背景介绍之后，每章都会介绍一些可行的攻击技术，这些技术足以用于攻击你的目标。

我们也清楚需要请专家在相应章节中为我们答疑解惑。在第11章和第12章中，我们幸运地请到了Tim Kuester和Chris Crowley。无论是广度，还是深度，这两人在各自领域内都造诣颇深。当然，我们并没有让二位在两章中直接代笔，而是让他们作为技术审校人员提供技术支持。Tim Medin作为本书大部分章节的技术评审，Mike Ryan在最具挑战的、与蓝牙技术

⊖ “瑞士奶酪模型”是James Reason提出的，即在多层奶酪片中，每一层都有不规律分布的孔，如果有光穿透奶酪，则穿透部位的每一层都在该位置有重叠孔，反之，只要有一层没有重叠孔，光就透不过来。这句话的意思是：如果将计算机安全分成一个个层，那么各层中与无线相关的部位将组成重叠孔，成为整个系统的公共弱点。——译者注

相关的第 7 ~ 10 章中提供了宝贵的见解，Jean-Louis Bourdon 则在第 14 章中提供了专家的视角，在 Z-Wave 领域，目前还没有几个人敢自称为安全专家。

对于本书第 2 版，我们也尽所能地找到读者的评论，花了大量时间来阅读（包括每一条正面和负面的评论）。对于正面的评论，我们会确保在写这些章节的时候继续保持。对于负面的评论，如果是非常有价值的，我们会悉心接受。例如有一些读者抱怨缺少在 Windows 操作系统上运行的黑客工具，再如在一个非常重要的话题，即针对“全球移动通信系统”（Global System for Mobile Communication，GSM）网络的入侵中，缺少必要的内容涵盖。我们希望在这次大规模更新版本中会对这些批评所涉及的不足进行修正。

对黑客来说，本书意味着：无论你是想点到为止，看看就行；还是牛刀小试，尝试“入侵”；或者是以全新的方式探索网络安全，以便达到以前已成文的技术所未曾到达的深度。动机你自己来选，只是我们可以很容易地看到，无论是在你的下一个无线入侵测试的过程中，还是你在重新审视以前对无线技术的使用方式上，又或者是在选择保护下一代嵌入式无线系统的资源上，本书就是你的绝佳参考。

本书涵盖了对无线安全进行攻击的很多内容，其意义在于通过了解黑客技术入侵到无线系统的技术，进而提高无线系统的安全。尽管 Wi-Fi 已成为无处不在的互联网接入技术，但许多其他无线协议也在使用，而本书所涵盖的协议是从安全角度出发，我们认为在日常使用中最重要的无线通信协议。包括从 Wi-Fi 协议到先进的“软件无线收发”协议，后者是目前无线通信协议中前所未有的。也包括“传统蓝牙”通信协议到“低能耗蓝牙”（Bluetooth Low Energy，BLE）通信协议。还包括苹果发布的 iBeacon 协议。对于“关键任务业务”和“家庭控制系统”，也包括 ZigBee 协议和 Z-Wave 协议。我们每天都在使用这些协议，所以了解它们的安全缺陷，保护它们免受攻击至关重要。

快速索引

在本书中我们使用“黑客大曝光”特有的格式进行编写，该格式已注册。

攻击图标

这个图标表示特定的渗透测试技术和工具。图标后面是技巧或者攻击技术的名称。在本书中你会看到传统的“黑客大曝光”危险分级表。

流行性	我们预计这种攻击方式在现实中会发生的频率。表示的方法很简单：1 表示最罕见，10 表示普遍
难易度	实施攻击所需要的技术等级：10 表示使用广泛流传的傻瓜式工具或者同等水平的技术，1 表示需要自己编写新的入侵程序，5 表示需要攻击者对目标系统或者协议有一定的了解，来使用比较难掌握的命令行工具

（续）

影响力	攻击实施后会产生的潜在危害，同样从 1 到 10。1 表示泄露设备或者网络上一些无足轻重的信息，10 表示获取权限或者能够重定向、嗅探、修改网络流量
危险级	即上面三项值的平均值

应对措施图标

大部分的攻击都有对应的应对措施图标。应对措施表示我们可以采取的一些措施，使用它们可以缓解对应攻击所带来的威胁。

我们同样使用特殊标记（即注意、提示、警告）来强调我们认为必要的特定细节和建议。

配套网站

为了方便读者，作者为本书开发了一个相应的网站，即 http://www.hackingexposedwireless.com。在网站上，读者可以找到本书中描述的许多资源，包括源代码、脚本、高分辨率的图片、资源的链接等。

网站上同样包括了 802.11 网络和蓝牙网络的补充介绍资料，还有一整套有关“射频低电平”（low-level radio frequency）的完整材料，它影响着所有的无线通信系统。

在本书出版之后，我们确定了一张勘误表，在配套网站上读者也可以找到这些更正，所以请经常访问配套网站确保与无线入侵领域的发展保持同步。

本书使用指南

阅读这本书，有几种不同的方法。第一种方法，随便翻到哪一页，找到“攻击图标”，就可以学到一种特定的技术，通过该技术可以查到一种具体的无线安全技术。第二种方法，随便翻到某一章的开始，可以学到一个具体的无线通信协议的重要操作特征。第三种方法，从头到尾，一章一章地读完。此外，我们希望这本书能作为一本有价值的参考书，能多年后仍然保存在你的书架上（或保存在你的数字阅读器里）。

本书共分成三个部分。第一部分专门讨论针对 Wi-Fi 的破解，本部分开始介绍如何入侵 IEEE 802.11 网络（第 1 章），随后详细介绍了扫描和发现 802.11 网络（第 2 章）。第 3 章主要介绍针对 Wi-Fi 网络的通用攻击。第 4 章则将这种攻击目标扩展到了流行的“ Wi-Fi 保护访问”WPA/WPA2（“ Wi-Fi 保护访问”版本 1 或版本 2）保护的 Wi-Fi 环境中。第 5 章在深度上介绍了如何入侵无线用户的客户端。第 6 章则主要介绍通过“架桥过隙”技术，借助于一个中间被攻陷的主机去攻击一个远端无线网络。

第二部分主要介绍蓝牙网络的破解，既包括传统蓝牙支持，又包括低功耗模式的蓝牙技术。第 7 章主要介绍在蓝牙传统模式下，扫描和侦测时所用的工具和技术。随后的第 8 章则是蓝牙在低功耗模式下的扫描和侦测。第 9 章是蓝牙侦听和嗅探过程中所用的攻击技术，囊括了前面的传统模式和低功耗模式。第 10 章则是组合所有的技术，攻击传统模式和低功耗模式的蓝牙网络，以及使用这些技术所涉及的协议。

第三部分主要介绍的是除了 Wi-Fi 协议和蓝牙协议之外，其他无所不在的网络无线技术及其所支持的网络。第 11 章介绍了通过软件无线收发技术入侵的精彩内容，该技术令黑客“如虎添翼”，使其可以方便地访问以往无法访问的无线网络。第 12 章着眼于“蜂窝网络”的破解，包括二代（即 2G）、三代（即 3G）、四代（即 4G）网络及 LTE[⊖]安全。第 13 章探讨改进 ZigBee 的黑客技术，主要介绍工业控制系统和其他重要无线部署。最后的第 14 章关注之前从未出版过的 Z-Wave 智能家居网络破解的相关知识。

本书可以作为参考手册备用，帮你在下一个渗透测试中，进行脆弱性评估时，或在审计时，或在政策审查时，或道德入侵约定中使用。保有本书，可以在洞察复杂的无线协议时，将其作为参考。最后，在你发现某无线安全漏洞的时候，及时向全世界同行进行分享，因为只有公开披露，世界才会实现显著的变化。

Joshua Wright

⊖ LTE，Long Term Evolution，即长期演进，是由 3GPP（The 3rd Generation Partnership Project，第三代合作伙伴计划）组织制定的 UMTS（Universal Mobile Telecommunications System，通用移动通信系统）技术标准的长期演进。——译者注

致　谢 *Acknowledgements*

感谢约翰逊·威尔士大学技术学院（Johnson & Wales University School of Technology）的全体教职员工，即使我毕业多年，他们仍然一如既往地继续为我提供教育上的服务。本书的每一章都是我在那里受教后的反馈，从程序编写到逻辑设计，从电路理论到数字信号处理，从嵌入式系统到单片机的逻辑分析，我的教授们给我留下了不可磨灭的印象，他们教我怎样从失败中吸取教训，那就是不停地自问“这件事应该怎么做”，这使我可以克服任何困难，进而投入激情做更伟大的事情。特别感谢 Al Benoit、Frank Tweedie、Jim Sheusi、Ron Russo、Al Colella、Al Mikula 和 Sol Neeman，感谢他们送给我的特殊礼物。

感谢我在 Counter Hack 公司的同事们，他们在我利用一些学术间隙从事本书写作的时候，给予了帮助和支持。感谢本书的编辑组成员 Brandi Shailer、Meghan Manfre、Janet Walden 和 Amanda Russell，在整个繁杂的编审流程中，每到稿件的重要时间节点，他们都提供悉心指导和灵活的处理。这次，我再次幸运沾了 LeeAnn Pickrell 超凡编辑技巧的光，对此我非常感激。同时感谢技术编辑 Tim Medin、Mike Ryan 和 Jean-Louis Bourdon，他们为本书增辉不少。感谢 Matt Carpenter、Chris Crowley 和 Tim Kuester 所给予的宝贵支持和技术诀窍，感谢我的合著者 Jon，在一年前就同意与我同舟共济，共担此任。

最后，感谢我的孩子 Maya 和 Ethan，他们使我想成为一个更好的人。感谢我的妻子 Jen，她帮我变成了这样的人。

——Joshua Wright

我要感谢许多有超凡才华的个人和团体，我有幸与之共事多年。这些个人和团体包括（但不仅限于）#area66、serialbox、trajek、Rich Johnson、Matt Miller、hlkari、geo、linnox、spoonm、Skywing、hdm 和 Pusscat。如果不是你们，我可能永远不会使用 ATDT 9884227 这个网名。

——Johnny Cache

Contents 目　录