21世纪信息安全大系

无线网络安全

Chris Hurley, Brian Baker, Christian Barnes, Tony Bautts,
Darren Bonawitz, Randy Hiser, Jan Kanclirz Jr.,
Andy McCullough, Jeffrey A.Wheat 著

杨 青 译

How to Cheat at
Securing a Wireless Network

How to Cheat at

Securing a Wireless Network

无线网络安全

Chris Hurley
Brian Baker
Christian Barnes
Tony Bautts
Darren Bonawitz
Randy Hiser
Jan Kanclirz Jr.
Andy McCullough
Jeffrey A. Wheat

著

杨 青 译

科 学 出 版 社

北 京

图字：01-2008-2613 号

This is a translated version of
How to Cheat at Securing a Wireless Network
Chris Hurley, et al.

ISBN: 1597490873

图书在版编目（CIP）数据

无线网络安全/（美）赫尔利（Hurley, C.）等著；杨青译. —北京：科学出版社，2009

（21 世纪信息安全大系）

书名原文：How to Cheat at Securing a Wireless Network

ISBN 978-7-03-024338-6

Ⅰ.无… Ⅱ.①赫… ②杨… Ⅲ.无线电通信-通信网-安全技术
Ⅳ.TN92

中国版本图书馆 CIP 数据核字（2009）第 048661 号

责任编辑：田慎鹏 霍志国／责任校对：张 琪
责任印制：钱玉芬／封面设计：耕者设计工作室／封面图片：徐 湛

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

骏走印刷厂印刷
科学出版社发行 各地新华书店经销
*
2009 年 4 月第 一 版 开本：787×1092 1/16
2009 年 4 月第一次印刷 印张：21 3/4
印数：1—4 000 字数：515 000

定价：56.00 元
（如有印装质量问题，我社负责调换〈环伟〉）

致　谢

Syngress 出版社非常感谢下列人士为本书提供的协助和支持。

Syngress 出版的图书目前由 O'Reilly Media 公司负责在美国和加拿大地区的发行。O'Reilly 公司的人员表现出了惊人的工作热情，我们感谢下列人士为本书的成功发行付出的时间和精力：Tim O'Reilly、Laura Baldwin、Mark Brokering、Mike Leonard、Donna Selenko、Bonnie Sheehan、Cindy Davis、Grant Kikkert、Opol Matsutaro、Steve Hazelwood、Mark Wilson、Rick Brown、Tim Hinton、Kyle Hart、Sara Winge、Peter Pardo、Leslie Crandell、Regina Aggio Wilkinson、Pascal Honscher、Preston Paull、Susan Thompson、Bruce Stewart、Laura Schmier、Sue Willing、Mark Jacobsen、Betsy Waliszewski、Kathryn Barrett、John Chodacki、Rob Bullington、Kerry Beck、Karen Montgomery 以及 Patrick Dirden。

我们感谢 Elsevier Science 出版社的勤奋团队，包括 Jonathan Bunkell、Ian Seager、Duncan Enright、David Burton、Rosanna Ramacciotti、Robert Fairbrother、Miguel Sanchez、Klaus Beran、Emma Wyatt、Krista Leppiko、Marcel Koppes、Judy Chappell、Radek Janousek、Rosie Moss、David Lockley、Nicola Haden、Bill Kennedy、Martina Morris、Kai Wuerfl-Davidek、Christiane Leipersberger、Yvonne Grueneklee、Nadia Balavoine 以及 Chris Reinders。他们让本书的编写具有了全球视野。

我们还要感谢 Pansing Distributors 图书发行公司的 David Buckland、Marie Chieng、Lucy Chong、Leslie Lim、Audrey Gan、Pang Ai Hua、Joseph Chan、June Lim 和 Siti Zuraidah Ahmad。他们在收到本书后表现出了极大的热情。

最后我们要感谢 Woodslane 公司的 David Scott、Tricia Wilden、Marilla Burgess、Annette Scott、Andrew Swaffer、Stephen O'Donoghue、Bec Lowe、Mark Langley 以及 Anyo Geddes。他们负责本书在澳大利亚、新西兰、巴布亚新几内亚、斐济、汤加、所罗门群岛及库克群岛的发行。

技术编辑和合著作者

Chris Hurley（也被同行称作 Roamer） 是在 Washington. DC 地区工作的一名高级渗透测试人员。他是 WorldWide WarDrive 活动的创办者；该活动每四年举办一次，由 INFOSEC 组织相关领域的专家和爱好者参加，旨在促进人们对无线网络不安全因素的了解。他同时也是 DEFCON WarDriving 竞赛的主要组织者。

Chris 目前的主要关注领域是渗透测试，他对于漏洞评估、入侵取证和事件响应也拥有广泛的经验。Chris 在安全领域的许多会议上都发表过主题演讲，并且发表了大量白皮书，涵盖 INFOSEC 的诸多主题。Chris 是《*WarDriving: Drive、Detect、Defend*》一书的主要编写者，同时也是《*Aggressive Network Self-Defense*》、《*InfoSec Career Hacking*》、《*OS X for Hackers at Heart*》和《*Stealing the Network: How to Own an Identity*》等书的供稿作者。Chris 拥有计算机科学专业的学士学位。他与妻子 Jennifer 和女儿 Ashley 一起居住在 Maryland。

作 者 简 介

Brian Baker 是在华盛顿特区为美国政府工作的一名渗透测试人员。Brian 几乎在 IT 行业的各个领域都工作过：从服务器管理员到网络基础架构的支持，再到目前的安全领域。Brian 一直把关注重点放在无线技术和最新的安全技术上。

我要感谢自己的妻子 Yancy，还有孩子 Preston、Patrick、Ashly、Blake 和 Zakary。我也要向 GTN 实验室的 Chris、Mike 和 Dan 大声说：谢谢你们！

第 2 章献给我的母亲 Harriet Ann Baker，谢谢你给予 3 个孩子的慈爱、奉献和鼓励，使我们能够在一个单亲家庭里成长起来。安息吧，有一天我们会再见……

Christian Barnes（拥有 CCNA、CCDA、MCSE、CAN 和 A+认证） 是在堪萨斯州 Overland Park 地区为 Lucent Technologies 工作的一名网络顾问。他在 IT 行业的最初工作是在 Western New York 为一家大型银行的 NT 和 NetWare 服务器以及 NT 客户端提供支持。不久之后，他转向为高级工程师和 LAN 及 WAN 管理员提供支持，协助他们处理故障和设计网络。后来他又转为一名网络顾问。Chris 与妻子和 4 个孩子生活在一起。

Tony Bautts 是 Astech Consulting 公司的一位高级安全顾问。他目前为旧金山湾区的客户提供安全建议和架构咨询服务。他擅长的领域包括入侵检测系统、防火墙的设计和集成、入侵取证、防御主机和安全架构设计。Tony 在安全领域拥有丰富的经验，曾为美国多家财富 500 强公司提供过服务，并在日本从事了两年安全咨询工作。他也是BerkeleyWireless.net项目的参与者；该项目旨在为加利福尼亚州 Berkeley 地区的居民建立区域性的无线网络。

Darren Bonawitz 是 Lucent Worldwide Service 部门的一位网络系统工程师。Darren 最初在电子商务领域创业。在 2001 年 1 月，他加入了 Lucent Worldwide Service 担任网络系统工程师。他不仅在桌面平台上拥有丰富经验，也对大量技术领域（包括远程访问、ATM、帧中继和无线网络等）有深入的理解。他的行业背景还包括为大学和公司客户提供售前及售后咨询、业务和技术规划以及客户服务工作。他在堪萨斯州立大学的专业是电子工程，重点研究了通信系统。在 2000 年，Darren 被提名为堪萨斯州的年度青年企业家。他最近还获得了《洛杉矶时报》的报道，以表彰他对在线客服领域的贡献。

Anthony Bruno（拥有 CCIE #2738、CCDP、CCNA-WAN、MCSE、NNCSS、CNX-Ethernet 等认证） 是 Lucent Worldwide Services 部门的一位资深顾问。作为一名顾问，他协助许多客户完成了大规模、多协议网络的设计、实现和优化。Anthony 在无线网络的设计、IP 语音和互联网接入领域也拥有丰富的工作经验。

此前他是一名空军上尉，从事网络的运营和管理工作。在担任此职位期间，他负责在基线网上实现了无线网络。Anthony 在 1994 年从 Missouri 大学 Rolla 分校获得了电子工程硕士学位，在 1990 从 Puerto Rico 大学 Mayaguez 分校获得了电子工程学士学位。他是《*CCDA Exam Certification Guide*》一书的共同作者，并担任若干 Cisco 专业书籍的技术评阅职务。

Dan Connelly（拥有 MSIA、GSNA 等认证） 是在华盛顿特区为联邦政府机构工作的一位高级渗透测试人员。他对许多 IT 技术都拥有丰富的经验，包括 Web 应用、数据库开发、系统管理和网络工程等。在过去 5 年里，他一直在从事信息安全方面的工作，为许多联邦机构提供了渗透测试、无线网络审计、漏洞评估和网络安全工程等服务。Dan 从 Radford 大学获得了信息系统专业的理学学士学位，并从 Norwich 大学获得了信息保障专业的理学硕士学位。

我要感谢 Chris Hurley、Mike Petruzzi、Brian Baker 以及 GTN 和 GMH 实验室的每个人，谢谢你们创造了一个舒适的工作环境。我还要感谢 ERG 的每个人，谢谢你们让我做自己喜欢的事情，同时还付给我工资。

我还要感谢父母提供的无私支持、智慧和指导，兄弟带来的积极影响，以及姐姐的一贯支持。我尤其要感谢美丽的妻子 Alecia，谢谢你多年来的爱和支持以及对儿子 Matthew Joseph 的关爱。儿子是来自上帝的礼物，我不能想象没有他的生活。

Chuck Fite 目前是 Iconixx 系统工程公司的一名顾问，负责参与 Sprint 公司的 ION 项目。在过去 8 年里，他在计算机和通信行业担任过技术作者、测试工程师和行业分析师等职务。Chuck 从 Iowa 州立大学获得了物理专业的理学学士以及修饰和专业交流专业的硕士学位。

Randy Hiser 是 Sprint 研发部门架构与设计小组的一位高级网络工程师，负责为 Sprint 公司的集成按需网络（Integrated On Demand Network，ION）设计家庭总线和 DSL 自安装服务。他对多媒体服务和各种新兴技术拥有丰富的知识，曾负责在中东地区安装并运营了 6 个固定式无线 MMDS 设施，并为 Sprint 公司获得了一项通信网络设备识别技术的专利。Randy 与妻子 Deborah 和孩子 Erin、Ryan、Megan、Jesse、Emily 一起居住在堪萨斯州的 Overland Park 地区。

Jan Kanclirz Jr.（拥有 CCIE #12136-Security、CCSP、CCNP、CCIP、CCNA、CCDA、INFOSEC Professional 认证） 是 IBM Global Services 部门的一位高级网络信息安全工程师。他目前负责一个多用户多数据的大型中心网络及其安全环境的战略和技术发展项目。Jan 专注于对各种跨厂商网络技术的亲手实施和架构设计，包括路由器、交换机、防火墙、入侵探测工具、内容网络和无线网络等。Jan 还对 Linux 和 BSD 系统的管理和安全实现拥有丰富的经验。

Andy McCullough（拥有 BSEE、CCNA 和 CCDA 认证） 已经在网络咨询行业工作了 7 年。他目前在 Lucent 公司的高级服务及销售部门工作，是顾问团队里的一位资深成员。Andy 已经为 Lucent Technologies 的许多全球客户完成了网络的架构和设计工作，包括 Level 3 Communications、Sprint、MCI/WorldCom、伦敦证券交易所和 British Telecom。他擅长的领域包括网络架构和设计、IP 路由和交换以及 IP 多播。在为 Lucent 工作之前，Andy 创办了一家咨询公司和一个地区性的 ISP 公司。

Andy 是《*Building Cisco Remote Access Networks*》（Syngress 出版社，ISBN: 1-928994-13-X）一书的共同作者。他也在堪萨斯州 Overland Park 地区的一所社区学院担任助理教授，开设有网络方面的课程。

Mike Petruzzi 是华盛顿特区的一位高级渗透测试人员。他在 IT 行业负责过许多项目并担任过多种职务。他曾经是项目主管、信息安全工程师、系统管理员和帮助桌面技术人员，并担任过 IKON 和 SAIC 等公司的技术负责人。Mike 对风险评估、漏洞评估以及行业认证和鉴定也拥有丰富的经验。Mike 还曾经是啤酒厂代表、酒类销售人员和一家餐馆的厨师。

Jackie Tucker 是居住在堪萨斯州的一位技术顾问，她在技术写作、界面设计和 Web 开发方面拥有超过 14 年的丰富经验。她在若干软件公司参与了软件设计的全过程，在 Informix Software Inc.曾拥有一个长期职位，深入参与了 Sprint ION 项目，目前则在 Sprint 公司的网络分部从事咨询工作。她以优异的成绩从 St. Mary College 获得了计算机科学专业的学士学位，随后从 Baker University 获得了管理学硕士学位。在工作之余，Jackie 尽可能多地与丈夫 Bob 和两个女儿 Sarah、Jessie 呆在一起；她的一家人都酷爱体育运动。

Jeffrey A. Wheat（拥有 Lucent WaveLAN Wireless 认证和 FORE ATM 认证） 是 Lucent Worldwide Services 部门咨询团队的一位资深成员。他目前为 Lucent 公司的服务提供商及大型企业客户提供战略指导和架构设计。他对融合网络（Convergence Network）和无线网络的架构十分擅长，也是 ATM 及其测试方法学的专家。Jeff 在 Lucent 工作期间，参与了 Metricom、Sprint ION、Sprint PCS、Raytheon 和 Marathon Oil 等项目的设计。在加入 Lucent 之前，他作为一名网络架构师和系统工程师为美国情报部门工作了 11 年。Jeff 在 1986 年从 University of Kansas 毕业并获得了计算机科学专业的学士学位。他目前与妻子 Gabrielle 和两个孩子 Madison、Brandon 一起居住在 Kansas 市。

Mark Wolfgang（拥有 RHCE 认证） 是俄亥俄州 Columbus 地区的一位高级信息安全工程师。他在渗透测试领域有超过 5 年的实战经验，在 IT 领域则有超过 10 年的经验。从 2002 年 6 月起，他开始为美国能源部（DOE）工作，负责带领并执行对 DOE 全国范围内的设施的渗透测试和漏洞评估。他发表了相关领域的多篇文

章和白皮书，并曾经两次在美国能源部主办的计算机安全会议上发表主题演讲。

在担任美国能源部的项目承包商之前，他为华盛顿特区的若干公司担任高级信息安全顾问，并为许多组织和公司执行了大量的渗透测试和漏洞评估。更早之前，他在美国海军担任了 8 年的作战专家（Operations Specialist），其中的四年两个月零九天是在 USS DeWert 导弹护卫舰上度过的。从海军退役之后，Mark 为 Red Hat 公司设计并开设 Red Hat 认证工程师（RHCE）课程；Red Hat 是 Linux 及开源技术领域的领袖级企业。

他从 Saint Leo University 获得了计算机信息系统专业的理学学士学位，并且是 Delta Epsilon Sigma 全国学术荣誉协会的成员。

目　录

第 1 章　无线技术导论：历史与现状 ····· 1

引言 ····· 2

无线技术的历史发展 ····· 3

电磁学的探索 ····· 3

导电方法的探索 ····· 4

无线电的发明 ····· 4

为汽车配备无线电话 ····· 5

计算机和网络的发明 ····· 6

蜂窝电话的发明 ····· 7

无线技术的应用现状 ····· 8

无线技术在专门领域的应用 ····· 9

无线技术在通用领域的应用 ····· 11

本书对无线技术的涵盖内容 ····· 12

小结 ····· 13

快速解决方案 ····· 13

常见问题 ····· 14

第 2 章　无线网络安全 ····· 15

引言 ····· 16

为 Linksys WRT54G 802.11 g 接入点配置安全功能 ····· 16

设置独特的 SSID ····· 16

禁用 SSID 广播 ····· 16

启用有线等效加密（WEP） ····· 17

启用 Wi-Fi 保护访问（WPA） ····· 19

媒介访问控制（MAC）地址过滤 ····· 21

为 D-Link DI-624 AirPlus 2.4GHz Xtreme G 无线路由器（带有四端口交换机）配置安全功能 ····· 23

设置独特的 SSID ····· 23

禁用 SSID 广播 ····· 24

启用有线等效加密（WEP） ····· 25

启用 Wi-Fi 保护访问（WPA） ····· 27

媒介访问控制（MAC）地址过滤 ····· 28

为 Apple Airport Extreme 802.11 g 接入点配置安全功能 ····· 30

连接到 AirPort Extreme 并设置独特的 SSID ····· 30

设置独特的 SSID ····· 32
禁用 SSID 广播 ····· 33
在 Airport 上设置密码 ····· 33
启用有线等效加密（WEP） ····· 34
启用 Wi-Fi 保护访问（WPA） ····· 34
媒介访问控制（MAC）地址过滤 ····· 35
为 Cisco 1100 系列接入点配置安全功能 ····· 37
设置独特的 SSID ····· 37
禁用 SSID 广播 ····· 40
启用有线等效加密（WEP） ····· 41
启用 Wi-Fi 保护访问（WPA） ····· 43
媒介访问控制（MAC）地址过滤 ····· 45
为无线客户端配置安全功能 ····· 46
设置 Windows XP 客户端（WEP） ····· 46
设置 Windows XP 客户端（WPA） ····· 48
设置 Windows 2000 客户端（WEP） ····· 49
设置 Windows 2000 客户端（WPA） ····· 50
设置 MAC 客户端（WEP） ····· 50
设置 MAC 客户端（WPA） ····· 51
设置 Linux 客户端（WEP） ····· 52
设置 Linux 客户端（WPA） ····· 53
理解并配置 802.1X RADIUS 用户身份验证 ····· 61
Microsoft RADIUS 服务器 ····· 61
802.1X 标准 ····· 61
在 Microsoft 网络上使用 EAP-TLS 配置 802.1X ····· 64
小结 ····· 78
快速解决方案 ····· 79
常见问题 ····· 81

第 3 章　工作场所无线网络的安全风险 ····· 83
引言 ····· 84
入侵者访问合法接入点 ····· 84
投机者 ····· 84
犯罪黑客 ····· 85
阻止入侵者访问网络 ····· 86
案例研究：入侵者亲自讲述无线嗅探工具 ····· 87
入侵者访问非法接入点 ····· 89
案例研究：员工使用可访问的无线网络逃避控制 ····· 90
入侵者连接到 WLAN 网卡 ····· 91

小结 …… 93
快速解决方案 …… 94
常见问题 …… 94

第 4 章　无线局域网非法接入点的探测和处理 …… 97
引言 …… 98
非法接入点带来的问题 …… 98
非法接入点是安全链中最薄弱的一环 …… 100
入侵者安装的非法接入点 …… 100
非法接入点的预防和检测 …… 101
采用安全策略预防非法接入点 …… 101
提供安全可用的无线网络 …… 101
通过探测射频信号检测和定位非法接入点 …… 101
Cisco 的非法接入点检查工具 …… 104
使用 802.1x 基于端口的安全措施防止非法接入点 …… 107
使用 802.1x 防止用户连接到非法接入点 …… 107
通过 802.1x 阻止非法接入点连接有线网络 …… 108
从有线网络检测非法接入点 …… 111
使用 Catalyst 交换机过滤器在端口过滤 MAC 地址 …… 113
端口安全机制中的 MAC 地址种类 …… 113
安全违规 …… 114
设置 IOS Catalyst 交换机的端口安全 …… 115
小结 …… 117
快速解决方案 …… 118
常见问题 …… 120

第 5 章　无线局域网的 VLAN …… 121
引言 …… 122
理解 VLAN …… 122
有线网络的 VLAN 中继协议（VTP） …… 125
中继端口的处理 …… 126
无线网络环境中的 VLAN …… 127
单个 VLAN 的设置 …… 128
无线网络中的 VLAN 中继协议 …… 129
中继端口 …… 129
网桥之间的中继端口 …… 129
无线 VLAN 的部署 …… 130
本地 VLAN …… 130
VLAN 之间的路由 …… 130

单个 VLAN 的过滤器 ····· 131
单个 VLAN 的 QoS ····· 131
单个 VLAN 的身份验证和加密 ····· 132
使用 IOS 配置无线 VLAN：案例分析 ····· 132
广播域分割 ····· 137
通信模式 ····· 137
无线网络中的广播域 ····· 138
访客 SSID 和主副 SSID ····· 139
访客 SSID ····· 139
使用 RADIUS 进行 VLAN 访问控制 ····· 140
设置 RADIUS 控制 ····· 141
小结 ····· 142
快速解决方案 ····· 143
常见问题 ····· 144

第 6 章 无线网络的设计 ····· 147
引言 ····· 148
探索设计过程 ····· 148
进行初步调查 ····· 148
分析现有网络环境 ····· 149
建立初步设计 ····· 149
确定详细设计方案 ····· 150
进行实施 ····· 150
搜集文档 ····· 151
确定设计方法学 ····· 152
建立网络规划 ····· 152
建立网络架构 ····· 157
详细设计阶段 ····· 160
从设计角度理解无线网络 ····· 165
应用支持 ····· 165
物理布局 ····· 167
网络拓扑 ····· 169
网络安全 ····· 170
小结 ····· 170
快速解决方案 ····· 171
常见问题 ····· 172

第 7 章 无线网络的架构和设计 ····· 175
固定无线技术 ····· 176

多通道多点分布式服务 176
本地多点分布式服务 177
无线本地回路 178
点对点微波 179
无线局域网 180
为什么需要无线局域网标准？ 180
通过 802.11 架构建立 WLAN 186
基本服务集 187
扩展服务集 188
CSMA-CA 机制 190
设置分片 191
使用电源管理选项 191
多区漫游 192
WLAN 安全性 192
通过 802.15 架构建立 WPAN 193
蓝牙 194
家用射频 196
高性能无线局域网 196
移动无线技术 196
第一代技术 198
第二代技术 198
第 2.5 代技术 198
第三代技术 198
无线应用协议 199
全球移动通信系统（GSM） 200
通用分组无线服务（GPRS） 201
短信服务 201
光学无线技术 201
小结 202
快速解决方案 204
常见问题 206

第 8 章 网络监控和入侵检测 207
引言 208
有利于入侵检测的网络设计 208
采用封闭网络 209
排除环境障碍物 209
排除无线电干扰 210
防御式监控的考虑因素 210

可用性和连通性……211
性能监控……213
入侵检测的策略……215
集成安全监控……216
常用的监控工具……218
攻击特征……220
进行漏洞评估……221
事件响应和处理……224
策略和过程……225
应对措施……225
入侵报告……226
清理……226
预防入侵……226
实地检查非法接入点……227
非法接入点的安装……227
小结……231
快速解决方案……232
常见问题……233

第 9 章 设计无线企业网络：医院案例……235
引言……236
企业网络中的无线技术应用……236
企业网络案例简介……236
机会评估……237
评估网络需求……238
附属建筑的物理布局评估……238
外部环境的物理布局评估……239
评估当前网络……240
医院会议室的网络布局评估……240
无线解决方案的设计……241
子项目 1：提供附属建筑的无线接入功能……241
子项目 2：为会议室提供无线技术……242
子项目 3：提供各个建筑之间的连接……243
建筑物之间无线连接的详细设计……244
无线解决方案的实现和测试……246
项目 1：附属建筑无线连接的实施……246
项目 2：医院会议室无线连接的实施……246
项目 3：建筑物之间无线连接的实施……246
医院目标的评审……248

经验总结 …… 248
小结 …… 249
快速解决方案 …… 249
常见问题 …… 250

第 10 章　设计无线商业网络：零售业案例研究 …… 253
引言 …… 254
商业网络中的无线技术应用 …… 254
商业研究案例的介绍 …… 255
机会评估 …… 255
定义案例研究的范围 …… 256
评估现状 …… 257
无线网络的设计和实施 …… 257
建立抽象设计 …… 257
建立详细设计 …… 258
获取物理布局图 …… 259
确定用户密度 …… 262
设备的安放规划 …… 264
确定接入点的安放位置 …… 265
无线网络的实施 …… 268
安装无线组件 …… 269
经验总结 …… 272
小结 …… 272
快速解决方案 …… 273
常见问题 …… 274

第 11 章　设计无线家庭网络：家庭办公室案例 …… 277
引言 …… 278
家庭网络的优势 …… 278
无线家庭网络的优点 …… 279
无线家庭网络的案例简介 …… 280
机会评估 …… 280
案例研究的范围定义 …… 280
无线家庭网络的设计 …… 281
功能需求的确定 …… 281
对家里进行实地考察 …… 282
建立初步设计方案 …… 287
建立详细设计方案 …… 288
无线家庭网络的实现 …… 289

安装网络设备 290
确定宽带网络的设置 290
安装硬件 291
安装和设置软件 291
测试网络 294
为数据、语音和高级服务设计无线家庭网络 295
家庭无线网络的市场现状 295
将来潜在的解决方案 297
经验总结 298
小结 298
快速解决方案 298
常见问题 299

第 12 章 无线渗透测试 301
引言 302
攻击途径 302
理解 WLAN 的安全漏洞 303
评估 WLAN 的安全漏洞 303
核心技术 304
WLAN 探测 304
WLAN 加密 306
攻击 308
开源工具 311
信号覆盖范围的检测工具 311
情报搜集工具 312
扫描工具 312
枚举工具 316
漏洞评估工具 317
攻击工具 318
案例研究 323
案例研究——破解 WEP 323
案例研究——破解 WPA-PSK 325
更多信息 327
其他 GPSMap 地图服务器 328