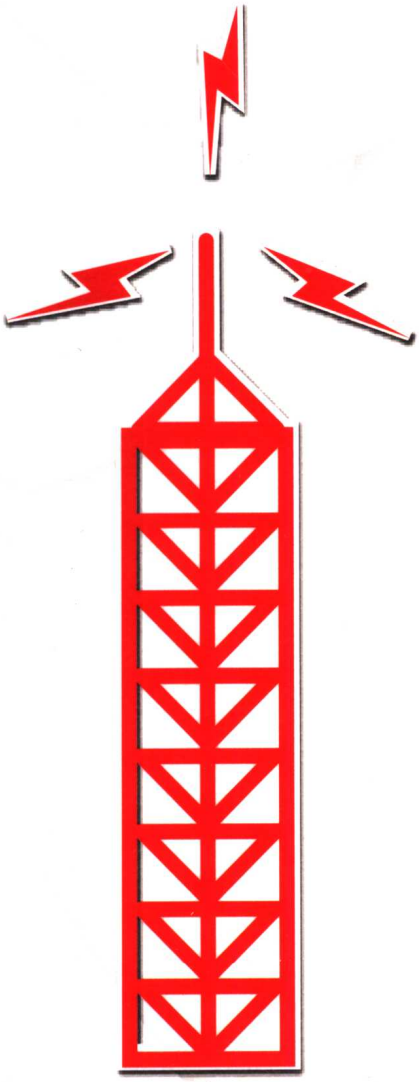
Broadview®
www.broadview.com.cn

安全技术大系

Maximum Wireless Security

无线网络安全



[美] Dr. Cyrus Peikari　Seth Fogie 著
周　靖　等译

SAMS

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

附光盘1张

安全技术大系

无线网络安全

Maximum Wireless Security

[美] Dr. Cyrus Peikari Seth Fogie 著

周 靖 等译

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

随着 WLAN 在中国乃至全世界的逐渐流行，再加上 WLAN 天生便是一种不安全的网络，所以安全意识必须加强，本书便是基于这个前提而编著的。本书通过最直接、有效的方式，利用大量真实的例子，全面揭示无线网络的安全机制和安全漏洞，并通过让你认识黑客的攻击方式，从而针对性地保护自己的无线网络。本书的核心在于“战争驾驶”（War Drive）。由于 WLAN 是一种发散型的网络，所以你建立的无线网络可能在不知不觉之间被偶然路过的黑客盯上。因此，无论安全审计人员还是黑客，都必须借助“战争驾驶”这一方式，携带一套专用的软硬件工具，对身边的无线网络进行检测，并尽量找出它的漏洞。作者凭借他们在无线安全行业的丰富经验，在本书中透彻讲述了 WLAN 的基本安全机制、存在的安全风险、黑客的攻击方式以及安全审计人员和网管应该如何最有效地保护自己的 WLAN。

全书信息丰富、行文朴实、简单易懂，是网管和安全行业的专业人士不可多得的参考书。

版权贸易合同登记号　图字：01-2003-7871

图书在版编目（CIP）数据

无线网络安全 /（美）皮科尔（Peikari, C.），（美）福杰（Fogie, S.）著；周靖等译. —北京：电子工业出版社，2004. 7
（安全技术大系）

书名原文：Maximum Wireless Security

ISBN 7-120-00092-6

I. 无… II. ①皮… ②福… ③周… 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（2004）第 052134 号

责任编辑：毕　宁　bn@phei.com.cn

印　　刷：中国电影出版社印刷厂

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

经　　销：各地新华书店

开　　本：787×980　1/16　印张：21.25　字数：402 千字

印　　次：2004 年 7 月第 1 次印刷

印　　数：4000 册　　定价：48.00 元（含光盘 1 张）

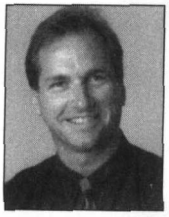
凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

作者简介

Cyrus Peikari 博士，1991 年毕业于 Southern Methodist University 电子工程专业。在长达 8 年的时间里，Peikari 博士在得克萨斯州达拉斯的 SMU Learning Enhancement Center 讲授高等数学。他同时担任 Alcatel 的电信软件研发工程师。Peikari 博士开发了几款获奖的安全软件。他还是 DallasCon 研讨会（美国西南地区最大的年度无线安全会议）的发起人之一。你可通过电子邮件联系他，地址是 cyrus@virusmd.com。

Seth Fogie 是前美国海军核能工程师。退役后担任一家大型 ISP 的技术支持专家，并在此期间拿到了 MCSE 证书。他目前是 VirusMD Wireless Security 公司的项目总监，负责下一代移动安全软件的研制。

Brett L. Neilson 在无线行业是具有很高资历的网络和系统工程师。Neilson 先生以前担任 Verizon Wireless 公司的高级系统管理员和无线电现场技师。在 Verizon 工作时，他主要负责开发、部署和维护公司的全美性基础结构。目前，Neilson 先生就职于一家行业领先的信息安全公司。作为一名拥有 FCC 执照的业余无线电操作员，他还为负责提供通信辅助和协作的几家政府机构工作过。其丰富的计算机和 RF 技术及经验，使他能在实务无线安全领域进行一些创造性的研究。Neilson 先生还在讲授“无线安全专家证书”（WSEC）的一系列复习课程。



Sten Lannerstrom 是 SmartTrust 公司的产品组合经理（Product Portfolio Manager），该公司致力于提供保护和管理移动服务及设备的基础结构软件。Lannerstrom 先生于 1997 年加入 SmartTrust（当时叫做 iD2 Technologies）公司，在信息技术领域已经有 22 年的从业历史。Lannerstrom 先生负责监管 SmartTrust 的无线安全产品组合方案，这些产品包括智能卡、无线设备、数字签名及生理特征加密，等等。他拥有 CISA（Certified Information Systems

Auditor，认证信息系统审计师）证书。

技术编辑

Marc Charney 是一名系统和网络结构师，在有线和无线（WLAN/WWAN）网络行业具有很高的资历，目前是在移动和无线终端行业占据领先地位的 Symbol Technologies 公司的一名高级系统顾问。Charney 先生目前致力于无线网络技术研究，重点关注的是 IEEE 802.11 标准。他自 1995 年起涉足无线 LAN，并担任过多种职位，其中包括无线电现场勘测员、无线系统工程师和无线系统结构师。凭借在网络和 WLAN 技术上的丰富经验，他能游刃有余地与大量客户展开合作，负责设计、开发和支持他们的 WLAN 和 WWAN 计划。除了就职于 Symbol，Marc 还是 Sams Publishing 的一名技术编辑，迄今为止已经有 7 年的历史。他的组稿范围涉及 Windows（NT/2000）、联网（有线和无线）及安全性等主题。Marc 目前关注的主题是 WLAN 和 WLAN 安全性。

William Rybczynski（GSEC，GCFW，CCNA，Network+）作为一家之主，膝下有 4 个小孩。他目前是美国太平洋舰队的现役军士长。他在信息技术和信息系统安全领域已经有 8 年的从业历史，同时还担任美国海军陆战队计算机科学学校及几家民间 IT 学校的高级教官/主题专家。

Anton Rager 是 Avaya Security Consulting Services 公司的高级安全顾问和创始人之一。Rager 先生的专长是漏洞研究、VPN 安全，以及无线安全。Rager 先生创作了几款用于无线网络和 VPN 安全分析的工具，其中包括 WEPCrack，它是第一款公开的 Wep 密钥破解软件，允许攻击者破解 802.11 协议使用的加密密钥。Anton 最近的工作涉及 IPsec VPN 协议、客户端和网关的漏洞测试，而且在几家主要的 VPN 厂商那里领导漏洞发现工作。

译 者 序

感谢 IT 技术的飞速发展，从前让人可望不可及的无线局域网技术如今已经唾手可得。围绕 WLAN，已经发展起来一个非常成熟的产业。从基础设施的建设，一直到软件和硬件的准备，无线生活已经不再是梦想。

但是，随着 WLAN 的逐渐普及，安全问题也正在变得日益严峻。由无线通信的本性使然，空中传播的数据天生就是不安全的，更何况 WLAN 标准本身还存在着严重的安全隐患。本书正在这一背景下问世的。纵览市面上的无线技术参考书，专门讲解无线安全的基本上等于零。但事实上，相较于有线网络，无线网络更应该关注安全问题。

这是一本实务性的参考书，全书没有只言片语的废话，一切都围绕真正的无线黑客攻防战来展开。首先介绍的是一些必要的无线基础知识，帮助你认识相关的无线硬件、无线协议、无线编程，以及 WEP 安全机制。然后，作者在基本算法的级别上，详细分析了 WEP 存在的安全漏洞，并从安全审计员和黑客的角度，介绍了具体的加密和破解过程。随后，作者还介绍了一些常规的黑客攻击方式。它们不仅适用于无线网络，也适用于有线网络攻击。有了这些知识准备之后，从第 7 章开始，就要进入真正的无线攻防实战。作者将教你如何利用各式各样的软件和硬件工具，对目标网络进行攻击和防守。

这本书的成功之处在于，作者毫不保留他们的亲身经验和体会，手把手地教会网管如何像黑客那样思索，了解各种各样黑客手段，从而有的放矢地防卫自己的网络。全书内容清晰、翔实，有很高的参考价值。

本书的作者是病毒和安全行业知名的专家，他们经常在达拉斯（世界信息安全之都）举办的各种安全会议上发言，拥有多项病毒和安全专利，还专门成立了一家 Airscanner 无线安全公司，拥有丰富的行业经验。

在本书翻译过程中，译者与作者进行了积极而有效的沟通，就一些难点问题进行了频繁的商议，最终在作者的授权下要么更改了一些错误，要么补充了一些内容，使本书中译本的质量上升到一个新的台阶。

周 靖

前　言

周五晚上是我们的“狂欢之夜”。我们像幽灵一样出没于黑沉沉的街道，冰冷的空气丝毫没有降低我们的热情。今晚，我们要将达拉斯黑掉！

蜷缩在一辆多功能运动车里——黑色的车身，浅色的车窗——伸出窗外的奇形怪状的天线，里面的人不知在干什么勾当。车子沿着理查森电信公司外面的一条路缓缓滑行，在一台笔记本电脑发出的微光中，我们脸上都闪烁着期待的神情。几乎马上就开始了，网络安全的壁垒在我们周围像冰一样地融化。只过了一小会儿，这个城市最大的网络便完整地展现在我们面前。Nortel（北方电信）的 28 个访问点全部向我们敞开。再开远一点，我们的天线发出了快乐的嗡嗡声。富士通、爱立信、阿尔卡特……几百个没有安全措施的门户就这样一个接一个地暴露在我们面前。有的加了密，但未免太软弱，大多数连最起码的密码都没有。我们知道，它们是我们的了。我们感觉自己在上升，高高盘旋在这些钢筋混凝土建筑的上方，我们凝视着它们，带着嘲弄和怜悯的眼光。然后，我们进入了……

——摘自 www.dallascon.com，使用已获许可

我们第一次提出这个主题是在 DallasCon 无线安全研讨会上（www.dallascon.com）。与会者的积极反应出乎我们的意料。其中有 IT 经理、网管、执法人员、军官和黑客，年龄从 18 岁到 63 岁。听众们都醉心于无线安全演讲，而且大部分人一直听完了长达 16 个小时的讲座。根据我们的调查，有 98%的人希望能再次听一遍这些讲座。

研讨会一直持续到半夜，直到场地提供方要求我们离开，很多人仍然跟着我们到了当地一家咖啡店，在那里我们又进行了一番演讲，直到第二天黎明。从那天晚上开始，与会者（许多人从那以后，成为我们的密友）强烈要求我们提供一些书面的材料。这使我们产生了尽快写一本书的想法。

最终的结果就是这一本书。这是迄今为止最实用的无线安全指南，不过，我们这样说并没有贬低其他同类书的意思。事实上，那些优秀的无线安全书的作者非常乐意成为我们的技术审稿人。因此，我们鼓励大家将其他无线安全书籍作为辅助读物。不过，如果你真的想学习如何进行“战争驾驶”（War Drive），就请从本书开始。注意，假如你不尽快审计自己的无线网络，其他人就可能“帮”你做这件事情——只是出于不良的动机。

注意，本书是一本“实务”指南。尽管书中为业余爱好者提供了大量的理论，但重点仍然在于满足专业人士的需求。我们将从理论开始，然后很快就会通过实例和实际的应用

程序来实践这些理论。读完本书之后，你将完全掌握如何按部就班地保护自己的无线网络。尽管本书的技术等级为高级，但书中的例子和案例都能帮助你轻松理解这些内容。

本书的目标读者是安全顾问、网管、IT 经理和“有道德”的黑客。本书要求读者具备一些基本的 Windows 或 Linux 联网知识。不需要事先了解无线安全方面的知识。本书适合中高级专业人士阅读。

本书分为以下 4 个部分。

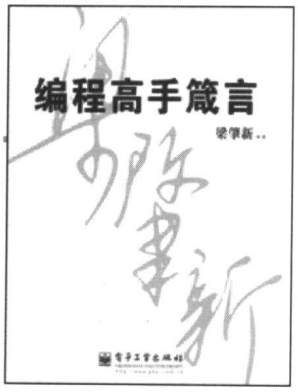
- 第 1 部分“无线基础知识”：介绍无线编程和 WEP 理论。
- 第 2 部分“无线安全威胁”：介绍如何出于自我防护的目的而攻击和破解自己的无线网络，还介绍了空中传播的病毒（无线病毒）。
- 第 3 部分“专业工具”：详细而全面地讨论最佳的无线安全工具，包括这些工具的具体使用步骤。
- 第 4 部分“无线安全”：指导你锁定自己的无线网络，其中包括 WLAN、3G 无线 PKI 和 WAP。

对于那些对无线安全岌岌可危仍然持怀疑态度的人，可考虑这个例子：一名研究人员在美国弗吉尼亚州亚历山大进行“战争驾驶”的过程中，发现美国国防信息系统局（Defense Information Systems Agency，DISA）总部有一个漏洞。当时，DISA 下属的国防部全球网络操作中心和计算机安全事件响应小组（Defense Department's Global Network Operations Center and Computer Emergency Response Team）正在使用一个无线 LAN 来控制前院的保安摄像机——但是这个网络甚至没有最基本的 WEP 加密。

畅 销 经 典

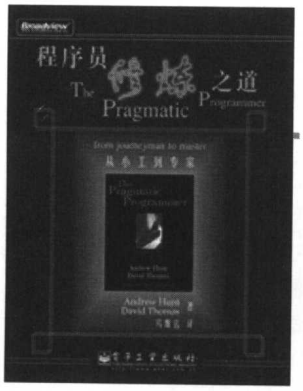
我就是程序，程序就是我！

编程高手箴言



梁肇新 著　　2003 年 11 月出版　　50.00 元

本书是梁肇新自己十余年厚积薄发的编程经验的集结，相信对广大程序员大有裨益。通篇没有时髦的 IT 新名词或新思想，而是踏踏实实地对很多知识进行了深刻的剖析，这有助于为编程打下坚实的根基。只有这样，才能在飞速变化的软件领域里免于雾里看花，才能更快更深地认识许多新问题、新知识，也才能更从容地应对未来的挑战。



领悟程序员修炼之道！做注重实效的程序员！

程序员修炼之道——从小工到专家

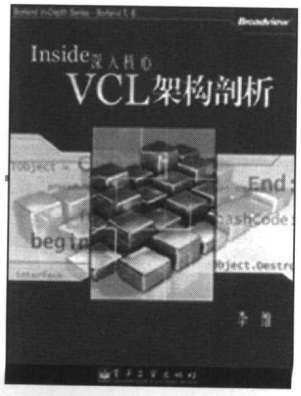
[美]Andrew Hunt,David Thomas 著　　马维达 译

2004 年 4 月出版　　48.00 元

本书直指编程前沿，透过日益增长的现代软件开发规范和技术，对软件开发的核心过程进行了审视——以满足用户为本，针对用户需求来产出高效、可维护的优秀代码。本书所涉及到的开发技巧、开发习惯以及职业态度，将帮助读者修炼成为一名真正的 Pragmatic Programmer！

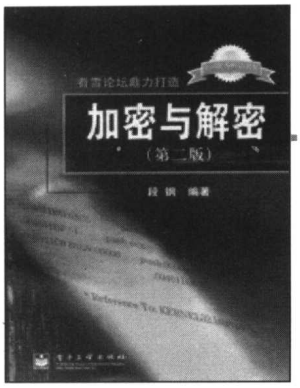
追寻大师级的 VCL Framework 设计思路！

深入核心——VCL 架构剖析



李维 著　　2004 年 1 月出版　　80.00 元

本书不但涉及 VCL Framework 本身，还旁及 Windows Framework、COM、设计模式等相关技术。读者从中获得的，不仅只是 VCL 架构知识，更会在整个阅读和实作过程中极大地拓宽自己的开发眼界，形成在系统设计方面的大局观，追寻大师级的 Framework 设计思路，提升整体开发素质。



密界一流高手呕心之作

加密与解密（第二版）

段钢 著　　2003 年 6 月出版　　49.00 元

看雪将其 3 年的辛勤工作汇集于《加密与解密》一书之中，在写作期间博览群书，勤问多思，采众家之长，集各门之萃，几乎所有国内的密界好手都为本书奉献了自己平常不轻易示人的资料收藏和大量实践中积累下来的宝贵经验，因此毫不夸张地说，本书可算得上是中国加密解密技术发展的一个里程碑！

Web 标准组织创始人 Zeldman 力作

网站重构——应用 Web 标准进行设计

[美]Jeffrey Zeldman　著　　傅捷 王宗义 祝军　译

2004 年 5 月出版　　38.00 元

本书着重分析了目前网站建设中存在的一些问题，以及“Web 标准”思想的产生、发展和推广，并从技术细节上讲解了网站实际制作和开发的过程中如何向 Web 标准过渡，如何采用和符合 Web 标准。本书的出版目的就是帮助读者理解 Web 标准，创建出用最低的费用达到最多的用户，并维持最长时间的网站，并且提供一些相关的技术和技巧。

网友热评：和《肖申克的救赎》一样让人振奋！

DOOM 启世录

[美]David Kushner　著　　孙振南　译

2004 年 4 月出版　　29.00 元

本书是国内第一部游戏领域的传记。与所有传记一样，不同的读者能从中得到不同的体验：游戏制作的背景内幕、光环之中的趣闻轶事、年少创业的梦想豪情、奋斗途上的汗水艰辛，成名之后的势易情迁、独辟蹊径的商业模式、天下为公的黑客精神、众说纷纭的暴力问题……

新书介绍——安全技术大系

用图解的方式深入剖析黑客技术的矛与盾

黑客攻防实战入门

邓吉 著　　2004 年 6 月出版　　定价 38.00 元

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。内容涵盖信息的搜集、基于认证的入侵及防御、基于漏洞的入侵及防御、基于木马的入侵及防御、入侵中的隐藏技术、入侵后的留后门以及清脚印技术。

你的无线网络安全吗？

无线网络安全

Cyrus Peikari,Seth Fogie 著　　周靖 译

2004 年 7 月出版　　定价 48.00 元

本书通过最直接、有效的方式，利用大量真实的例子，全面揭示无线网络的安全机制和安全漏洞，并通过认清黑客的攻击方式，从而有针对性地保护自己的无线网络。

帮助你在这场重要的安全战役中致胜的宝典——

Microsoft，UNIX 及 Oracle 主机和网络安全

Erik Pace Birkholz, Foundstone 公司 著　　赵彦玲 潘吉兵 董春红 等译

2004 年 7 月出版　　79.00 元

本书凝聚了数十位权威的国际安全专家的实战经验和技术总结，不仅提供了 Windows 系统、UNIX 系统和 Oracle 系统的主机及网络安全解决方案，而且包括了企业的安全管理规范和原则；既高屋建瓴地描述了企业内部网整体面临的安全威胁和漏洞，又细致入微地介绍了 Windows，UNIX，Oracle 及无线 LANs 等各种系统具体的漏洞，同时还提供了各种漏洞评测方法和补救措施。

用网络优化与故障检修的利器，探测和补救网络安全漏洞。

Sniffer Pro 网络优化和疑难手册

Robert J. Shimonski 等 著　　陈逸 译

计划 2004 年 7 月出版　　估价 49.00 元

Sniffer Pro 是美国 Network Associates 公司出品的一种网络分析软件，可用于网络故障与性能管理，在网络应用业界应用非常广泛，现已占到网络分析软件市场的 76%。本书详细介绍了 Sniffer Pro LAN 的基本功能，Sniffer Pro 程序的安装、配置和 Sniffer 界面的各个方面，以及 SCP 认证考试的内容。

强有力的程序保护技术

黑客反汇编揭密

Kris Kaspersky 著　　谭明金 译

计划 2004 年 9 月出版　　估价 38.00 元

本书分为两大部分。第一部分结合精心挑选的实例，系统地讨论了黑客代码分析技术；第二部分介绍了程序保护所面临的各种挑战及其相关的反调试、反跟踪、防反汇编以及代码加密解密技术等内容。本书在内容上将针对性、实践性与综合性有机地结合在一起，很好地满足了学习代码分析技术的需要。

联系方式

读者反馈与咨询：（010）51922839，jsj@phei.com.cn

投　　稿：（010）51922839，editor@broadview.com.cn

网　　址：www.broadview.com.cn

传　　真：（010）51922823

网上书店：www.dearbook.com.cn

门　　市：（010）68279077

邮　　购：（010）68211478

博文视点资讯有限公司（BROADVIEW Information Co.,Ltd.）是信息产业部直属的中央一级科技与教育出版社——电子工业出版社（PHEI）与国内最大的 IT 技术网站 CSDN.NET 和最具专业水准的 IT 杂志社《程序员》合资成立的以 IT 图书出版为主业、开展相关信息和知识增值服务的资讯公司。

我们的理念是：创新专业出版体制；培养职业出版队伍；打造精品出版品牌；完善全面出版服务。

秉承博文视点的理念，博文视点的产品线为面向 IT 专业人员的出版物和相关服务。博文视点将重点做好以下工作：

（1）在技术领域开发专业作（译）者群体和高质量的原创图书

（2）在图书领域建立专业的选题策划和审读机制

（3）在市场领域开创有效的宣传手段和营销渠道

博文视点有效地综合了电子工业出版社、《程序员》杂志社和 CSDN.NET 的资源和人才，建立全新专业的立体出版机制，确立独特的出版特色和优势，将打造 IT 出版领域的著名品牌，并力争成为中国最具影响力的专业 IT 出版和服务提供商。

作为合资公司，博文视点的团队融合了各方面的精英力量：原电子工业出版社 IT 图书专业出版实力的代表部门——计算机图书事业部的团队；《程序员》杂志社和 CSDN 网站的主创人员；著名 IT 专业图书策划人周筠女士及其创作群。这是一个整合专业技术人员和专业出版人员的团队；这是一个充满创新意识和创作激情的团队；这是一个不断进取、追求卓越的团队。

电子工业出版社与《程序员》杂志和 CSDN 网站的合作以最有效率的方式形成了出版资源、媒体资源、网络资源的整合和互动，成为 2003 年 IT 出版界备受瞩目的事件。

“技术凝聚实力，专业创新出版”，BROADVIEW 与您携手共迎信息时代的机遇与挑战！

博文视点

地址：北京市复兴路 47 号天行建商务大厦 604 室

邮　编：100036

总　机：010-51922832　传　真：010-51922823

国内作者写作图书：010-51922839　国外作者写作、引进版图书：010-51922825

http://www.broadview.com.cn　投稿及读者反馈：editor@broadview.com.cn

武汉分部地址：武汉市洪山区吴家湾紫菘花园 16 栋西门 401　邮编：430074

电话：027-87691935　E-mail:yeka@csdn.net

《无线网络安全》读者调查表

尊敬的读者：

感谢您对我们的支持与爱护。为了今后为您提供更优秀的图书，请您抽出宝贵的时间将您的意见以下表的方式及时告知我们（可另附页）。我们将从中评选出热心读者若干名，免费赠阅我们以后出版的图书。

您的意见是我们创造精品的动力源泉！

姓名：_____ 性别：□ 男 □ 女 年龄：_____ 职业：_____

电话（寻呼）：_____ E-mail：_____

传真：_____ 通信地址：_____

邮编：_____

1. 影响您购买本书的因素（可多选）：

□封面封底 □价格 □内容提要、前言和目录 □书评广告 □出版物名声

□作者名声 □正文内容 □其他_____

2. 您对本书的满意度：

从技术角度 □很满意 □比较满意 □一般 □较不满意 □不满意

□改进意见_____

从文字角度 □很满意 □比较满意 □一般 □较不满意 □不满意

□改进意见_____

从版面、封面设计角度 □很满意 □比较满意 □一般 □较不满意

□不满意 □改进意见_____

3. 您最喜欢书中的哪篇（或章、节）？请说明理由。

_____

_____

4. 您最不喜欢书中的哪篇（或章、节）？请说明理由。

_____

_____

5. 您希望本书在哪些方面进行改进？

_____

_____

6. 您感兴趣或希望增加的图书选题有：

_____

_____

请寄：电子工业出版社博文视点资讯有限公司（计算机图书事业部）

地址：北京复兴路天行建商务大厦 604（100036）

电话：010-51922832 E-mail: jsj@phei.com.cn

目　录

第 1 部分　无线基础知识

第 2 部分 无线安全威胁