Broadview
www.broadview.com.cn

零壹 SECURITY
ZerOne
Anywlan

安全技术大系

无线网络安全攻防实战

杨哲 编著

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

零壹 SECURITY
ZerOne
Anywlan

安全技术大系

无线网络安全攻防实战

杨 哲 编著

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

内 容 简 介

面对当前国内外无线网络飞速发展、无线化城市纷纷涌立的发展现状，本书以日趋严峻的无线网络安全为切入，从基本的无线网络攻击测试环境搭建讲起，由浅至深地剖析了无线网络安全及黑客技术涉及的各个方面。本书分为 13 章，包括无线 WEP 加密破解、无线 WPA/WPA2 破解、内网渗透、无线 DoS 攻击与防护、无线 VPN 搭建与攻击防护、War-Driving 战争驾驶、无线钓鱼攻击及无线 VoIP 攻击、无线打印机攻击等特殊角度无线攻击和解决方案。

本书可以作为军警政机构无线安全人员、无线评估及规划人员、企业及电子商务无线网络管理员的有力参考，也可以作为高级黑客培训及网络安全认证机构的深入网络安全辅助教材，是安全技术爱好者、无线安全研究者、无线开发人员必备的参考宝典。

图书在版编目（CIP）数据

无线网络安全攻防实战 / 杨哲编著.—北京：电子工业出版社，2008.11
（安全技术大系）
ISBN 978-7-121-07508-7

I. 无… II.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（2008）第 154115 号

策划编辑：毕　宁
责任编辑：葛　娜
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
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　　印张：26.5　　字数：636 千字
印　　次：2008 年 11 月第 1 次印刷
印　　数：4000 册　　定价：59.00 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。

" SomeBody tell me
Why it feels more real when I dream than when I am awake?
How can I know if my senses are lying? "

There is some fiction in your truth,
and some truth in your fiction.
To know the truth, you must risk everything。"

谁能告诉我
为何做梦时比醒着清醒?
我怎么知道我的感觉是否在撒谎?

在你的真实中存在虚幻,
在你的虚幻中存在真实。
想知道真实,就要冒险。

——源自电影"黑客帝国"外传—*Kid's Story*

前　言

当你坐在3楼熟悉的星巴克咖啡屋，在靠窗的角落里习惯性地打开笔记本，连上星巴克提供的无线接入点，翻看着当天网络上最新的资讯信息时，可曾想过就在街对面，一栋新建不久的饭店4楼，有人正试图通过无线网络，攻入你的电脑并窃取你保存在硬盘深处的新闻调查笔记？

当你坐在办公室里，在空调送来的凉爽微风下，整理刚参加完的公司会议记录时，可曾想过就在和你间隔3米的楼上，有人正试图通过公司的无线网络，窃取你计算机上备份的公司内部发展计划？

当你坐在机场环境优雅的VIP候机厅里，一边漫不经心地在笔记本上翻看着自己的个人Blog，一边听着MP3时，可曾想过离你500米远的一辆黑色SUV里，会有一台笔记本正一样通过机场提供的无线接入服务，在快速下载并记录着你笔记本里所有关于后天安全技术峰会的秘密资料？

当你和朋友们外出旅游，在休息的酒店里拿出新买的IPhone，迫不及待地连上酒店的无线网络收取当天的电子邮件时，可曾想过就在走廊尽头的一个单间里，有人已经通过无线网络进入你的IPhone，正翻看着你那些不能见光的个人写真图集？

……

这不是什么好莱坞的科幻电影，更不是什么危言耸听的传言，而是就在我们的身边，就在我们的桌旁，每一个标识着WiFi的便携设备上，一个繁华技术背后的安全阴影——无线网络，是不是真的方便了自己也方便了别人？

无线网络带来的巨大便利和庞大的商业价值，已经无须证明。作为政府及通信部门对无线网络技术的扶持，也使得无线技术开始成为发展最快的高新技术之一。但是人们在沉浸于享受无线网络带来便利的同时，很多人却并没有意识到，技术的两面性已经开始在一些不为大多数人所知的领域有所体现。

应对当前国内外无线网络发展的种种势头，本书从身边基础的无线网络环境讲起，由浅至深地探讨了无线网络涉及的各个方面，包括无线WEP加密破解、无线WPA/WPA2破解、内网渗透、无线DoS攻击与防护、无线VPN搭建与攻击防护、War-Driving战争驾驶及其他各种无线攻击可能的角度和解决方案。

和以往注重理论化的无线安全书籍不同的是，在本书中，笔者将带给大家关于无线网络的实际攻击技术及对应的防御技术。需要说明的是，在所有涉及攻击技术的章节，对那些试图通过无线网络进行非法攻击、渗透及破坏等非法行为的家伙们，本书中都会称之为“恶意的攻击者”。真正能被称之为无线“黑客”的，正是那些通过不断研究无线攻防技术，来促使无线安全技术整体提升，以达到完善无线网络，推动更高级无线网络规范实施的可敬的人们。谨以此书向这些投入大量心血的幕后黑客们致以发自心底的敬意。

如果说公布或者研究无线黑客技术会引起别有用心的人注意，甚至让一些人觉得有些不可理解的话，那么，摆在我们面前的事实是：很多无线网络只是由一些“自负”的管理员们凭着传统有线网络的经验管理，有很大部分的人无视或根本不知自身的无线将面临何种风险。为此，与其不知所措，不如正视这些可能的攻击行为和方式，这样，才能够真正强化巩固好现有的无线网络。何况，古人亦云：师夷长技以制夷。

希望这样一本实际操作的教程可以帮助同样喜欢无线网络安全的朋友们少走弯路，也希望能吸引更多的人投入到无线网络安全领域来。

本书适合的读者

——通信部门无线安全人员、无线评估人员及规划人员、无线网络管理员；
——军警政机构无线安全人员、无线评估人员、无线网络管理员；
——企事业单位无线安全人员、无线网络管理员；
——致力于无线网络安全技术的理论研究者；
——无线产品开发人员；
——高级黑客培训及国际网络安全认证课程讲师；
——致力于学习高级网络安全技术的大中专院校学生；
——所有无线黑客技术爱好者。

反馈与提问

读者在阅读本书时如遇到任何问题，可以到本书合作网站——中国无线门户网站 www.anywlan.com 论坛安全板块提出，同时读者可以从网站上找到本书中涉及的全部工具及其他一些有用的资料，如有其他事宜可以直接 E-mail 给我（longaslast@gmail.com）。

关于本书的修订内容及更多深入情况，请关注我的个人博客 http://bigpack.blogbus.com。

致　　谢

——谨以此书献给我的妻子和刚出生的女儿丫丫

回顾这本书的写作历程，里面凝聚了我大量的精力和心血，开始确实没想到写书会如此艰辛，前后花费了近 10 个月的时间，中间几度搁置，甚至一度由于工作生活的繁忙和心情的烦闷而放置一边。这本书的完稿除了自身的努力之外，离不开家人的包容和朋友们的鼓励，还有其他很多人的支持。

首先感谢我的家人，在我写书的日子里，给予我最大程度的支持与鼓励。尤其是我的母亲，从很久以前开始，即使是在我最低落的时候也从未对我放弃过希望，使用语言来表述我的感情只会显得苍白，但是在这里还是要说：谢谢您，妈妈，我会一直让您引以为豪。

感谢西安市特警支队指挥中心的樊安，和你一起在城市里 War-Driving 的日子值得纪念，ZerOne 安全团队在各位同仁的支持下将会做得更好。

感谢 ZerOne 安全团队的任明哲，天线的改装离不开你的支持，感谢一直以来的信任和努力，团队的发展需要你的潜力。感谢团队的小苏，虽然从地图上看我们相距遥远，但距离从来不是问题。感谢团队的其他队员，谢谢大家的支持和鼓励。

感谢好友徐枫，你漂亮的编程能力周围已经没有多少人可以赶得上了，很高兴看到你飞得更高。回顾十多年来一起努力、相互勉励、相持而笑的日子，技术上的交流反而是次要的。希望有一天我们可以背着登山包，再次走进太白山广阔的原始森林里去寻找内心的真实。

还要感谢来自我的母校——西安电子科技大学红外与通信研究所的好朋友何国经博士，谢谢你提供的宝贵意见和支持，近似领域的探讨总能让我的思维迸发出新的火花。期待下次滑雪时再看到你从南极归来般潇洒的身影。

感谢中国无线门户网站 AnyWlan 的站长 Tange 和 Zero，特别是 Tange，谢谢你们一直以来的信任和大力支持，在无线安全版块担任版主是件非常有意思的事情，在这里遇到了很多高手

和朋友，这里一并表示感谢，谢谢你们的支持、鼓励和抨击，和大家的探讨让我收益很多。愿AnyWlan早日成为国内无线网络技术的前沿领导和典范!!

感谢陕西省人民政府信息产业厅网络安全处的黄永宏处长及其同仁对本书的指导与大力支持，也诚挚地希望本书能为政府机构的无线安全实施做出贡献。

感谢陕西省人民政府信息产业厅电子政务处的高翔处长及丁尔兵处长，您们的支持和鼓励与这本书的出现有着重要的关系，相信这本书也能够成为完善电子政务安全可以参考的资料之一。感谢好朋友王伟，您的热情总是让人在冬季里感到温暖。

感谢陕西省人民政府信息产业厅法规处的王栋为本书的顺利出版提供了很多宝贵的建议，期待您的更多支持与鼓励。

特别感谢陕西人民广播电台的老同学姜志鹏，虽然职业不同，但这并不影响我们之间的探讨，谢谢你如此热心地帮助我查询资料和沟通，那一晚在STARBUCKS的“头脑风暴”令人印象深刻。

感谢好朋友刘铁山，在无线装备和其他设备上提供了许多便利，和幽默的你在一起总是让人感觉很轻松写意。

感谢西安Linksys代理商谢海源，提供的最新无线资讯和无线产品测试。

特别要感谢的是电子工业出版社编辑毕宁，您如此细致认真的办事作风令我印象尤为深刻，感谢您如此耐心地修正书中的所有细节，本书的顺利出版离不开您精益求精的态度和严谨求实的作风。还要感谢葛娜编辑在后期完善中一丝不苟及快速高效的做事风格，感谢您为这本书付出的努力。

最后，感谢那些曾经鼓励我、安慰我、打击我、和我一起走过又离我远去的朋友们，真诚地感谢你们的陪伴，谢谢。

杨　哲

于2008年5月29日晚

目　录

第 1 章　你所了解和不了解的无线世界

1.1　精彩的表面——无线网络现状

回想起并不遥远的以前，也就是 4、5 年前，在很多人为了给办公环境、酒店大厅及家庭 SOHO 的网络搭建、布线受到问题困扰时，无线网络作为一种新兴技术就已经开始崭露头角了。但由于当时无线设备过于昂贵，光是一张普通的 802.11b 无线网卡就能卖到 1000 元上下，更不用提其他的设备。其高额的价格不但制约了人们接受无线网络的速度，还严重影响到了其自身的发展。

幸好，很多对无线网络报以极大期望的厂商和研究人员都注意到这一点，在经过不断尝试和改进后，随着技术的愈加成熟和成本的下降，无线网络终于开始走进大众的视野。在 2007 年，全球 WiFi 设备数量已超过 7500 万个，并且据估计在 2008 年，无线设备将再增加一倍。现在，如图 1-1 所示的 WiFi 联盟认证，这个原本陌生的标识作为无线技术支持的象征，正开始频繁地出现在手机、PDA、笔记本和各种便携式设备上。

图 1-1 WiFi 联盟认证

WiFi 联盟（WiFi Alliance）是一家全球及非营利性的行业协会，拥有 300 多家成员企业，共同致力于推动无线局域网络（WLAN）产业的发展。以增强移动无线、便携、移动和家用设备的用户体验为目标，WiFi 联盟一直致力于通过其测试和认证方案确保基于 IEEE 802.11 标准的无线局域网产品的可互操作性。自 2000 年 3 月 WiFi 联盟开展此项认证以来，已经有超过 4000 种产品获得了 WiFi CERTIFIED™ 指定认证标志，有力地推动了 WiFi 产品和服务在消费者市场和企业市场两方面的全面开展。

而无线局域网（Wireless Local Area Network，WLAN）具有可移动性、安装简单、高灵活性和扩展能力，作为对传统有线网络的延伸，在许多特殊环境中得到了广泛的应用。随着无线数据网络解决方案的不断推出，“不论您在任何时间、任何地点都可以轻松上网”这一目标已经被轻松实现。

回顾国内无线网络的发展，可以直接从无线接入点数量的迅猛发展看出来，其完全可以用“与时俱进”来形容。无论是在繁华的商业大街上、高新技术产业开发区，还是在大学校园、科研单位，亦或是政府、警务及部队所属机构，甚至是在普通家庭，无线网络经历了从无到有，直到现在星罗遍布的局面。除此之外，在一些行业性的无线项目中也已得到广泛应用，如：石油、矿山、集装箱码头等。

不过，富有抱负的人们似乎并不满足于当前无线的发展现状，为了彻底实现覆盖面广的无线宽带网络，不仅仅局限在一个房间、一栋楼里，而是如手机信号那样覆盖整个地区，新

的目标已经提出并付诸行动，那就是——建立无线城市。

目前，全球包括已建和在建中的无线城市已经超过 450 个，如美国华盛顿、英国伦敦、法国巴黎、德国汉堡、新加坡以及中国台北、中国香港等都已建立无线城市。在内地地区，除上海嘉定正式开始建设以外，我国北京、天津、武汉、杭州、深圳、西安等地也已经在当地政府的支持下确立无线城市计划，如图 1-2 所示。

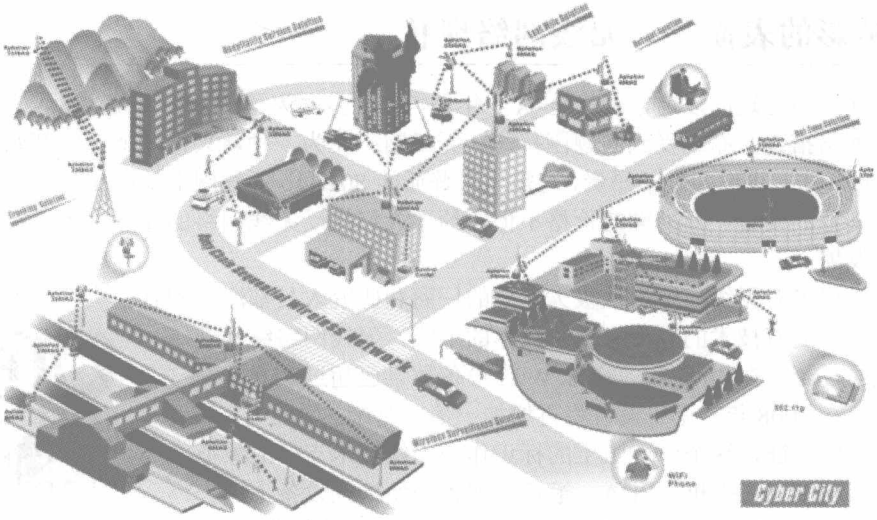

图 1-2 无线城市构想图

可以看到，在无线城市的架构下，无线网络真正深入到了生活的各个角落，无论是工作上网、在校学习还是商店购物、飞机订票，人们都可以随时随地打开笔记本，连上附近的无线基站，选择自己的生活。而在国外，甚至一些国营铁路公司也已开始试验在高速列车上提供无线上网业务，比如法国的高速列车时速超过 320 公里，在提供无线网络服务后，乘客将可以用有无线上网功能的笔记本电脑上网、查询列车位置等。

试想一下，在办公室，人们可以通过无线网络轻松地收发邮件，也可以一边写着材料一边与外地的同事语音沟通；在咖啡屋，休息的人还可以通过无线网络更新自己的博客；在机场，等候出行的人还可以通过无线从自己喜欢的乐队网站下载新的 MP3。这些信息从我们的身体穿过，但我们看不见也听不见它们。

无线，不就是现实社会的一种魔法吗？

1.2 阴影下的世界——无线黑客技术的发展

无线技术在给我们带来极大方便的同时，也带来了极大的信息安全风险。人们对无线访问设备的需求是如此的强劲，以至于供应商和信息安全防护人员都未能跟上它们的快速发展。

首先，由于理论上无线电波范围内的任何一台电脑都可以监听并登录无线网络。若这些接入点的安全措施不够严密，则完全有可能被窃听、破解甚至深入到内部网络。虽然墙壁或玻璃可以降低传输速度，但通常的 WiFi 信号从理论上都可以从接入点或路由器处向外传输 30~200 米远。

其次，从各种实用的 802.11 无线访问设备面世的那一天起，它们无不存在着核心或协议级的基本设计缺陷。而无线技术是一种几乎适用于所有领域的技术，加上人们对这种技术的需求程度已经远远超过了它本身的成熟程度，所以，有很多企业、机构和个人都还沉浸于无线网络迅猛发展所带来的经济效益扩大化和工作效率便捷化的美梦中，根本没有发现无线网络繁华背后日渐巨大的阴影——无线黑客技术的发展。

作为对互联网一切根源有着无限探知心态的国内外黑客们，在无线领域也一样保持了很高的水准。关于无线网络攻击与防御从几年前起就开始受到重视，并且其攻击技术也呈现出一年比一年深入、复杂、高效的趋势。无线网络安全防御技术、无线黑客攻击技术已经在无线网络光彩照人的背后悄悄开始了较量。正如 2001 年在拉斯维加斯举行的，象征全球顶尖黑客集会的 BlackHat 黑帽子大会上描述的那样：无线网络将成为黑客攻击的另一块热土（大会图标见图 1-3）。

图 1-3 BlackHat 象征着全球黑客精英大会的黑帽子大会图标

也正是由于无数经验丰富的黑客个人、团体都开始将大量的时间和精力投入到无线领域，所以关于无线加密标准的攻击破解的工具和技术也开始快速出现、提升。以 Aircrack-ng 为核心的无线攻击工具基本上已经成为国内外黑客们的标准配置（见图 1-4）。而作为实力雄厚的黑客团体还推出了无线攻击操作系统平台，比如最出名的 BackTrack Linux 系列，这些 Linux 甚至无须安装，可以直接通过光盘启动引导进入，也就是我们所说的 Live CD。这些工具在本书中都会涉及并深入学习。

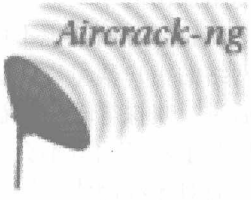

图 1-4 无线破解利器 Aircrack-ng

对于启用加密的无线接入点，黑客们可以通过破解 WEP 或 WPA 加密来进入内部网络，并在渗透成功后再对内部主机进行攻击。当然，无线黑客们还会根据情况进行复杂点的攻击，比如伪造基站、无线 DoS、钓鱼等。若是未加保护的无线局域网，那么连新手也可以轻易地接进宽带网络连接中。我们在生活中经常可以看到一些宽带用户喜欢开放自己的无线网络，然而，被分享的可能不仅仅是互联网接入，何况大多数的用户甚至根本不知道有