计算机安全技术丛书

潜在威胁分析
——从恶作剧到恶意犯罪

[美] David Maynor 等编著
谢 俊 潘洪涛 等 译

一站式参考资料

- 涵盖Syngress安全知识库中最吸引人的主题
- 涵盖David Maynor在黑帽子黑客大会上令人震撼的设备驱动程序研究成果

中国水利水电出版社
www.waterpub.com.cn

计算机安全技术丛书

潜在威胁分析
——从恶作剧到恶意犯罪

[美] David Maynor 等编著

谢 俊 潘洪涛 等 译

中国水利水电出版社

内 容 提 要

本书共分为五部分，系统地介绍了 VoIP、恶意软件、钓鱼与垃圾邮件、RFID 和非传统威胁。其中 VoIP 部分介绍了 VoIP 通信系统的基础架构和所面临的威胁，以及 Skype 软件的安全问题；恶意软件部分介绍了间谍软件的危害以及检测和删除间谍软件的各种方法；钓鱼与垃圾邮件部分介绍了识别和应对钓鱼与垃圾邮件的方式；RFID 部分探讨了越来越常见的 RFID 攻击以及 RFID 的安全管理方法；非传统威胁部分介绍了人员攻击和设备驱动程序攻击。

本书囊括了计算机网络安全领域的大多数主题，是一本很好的网络安全参考资料。本书适合企业构建安全网络的系统管理员阅读，也适合注重信息安全和网络安全的任何读者。

北京市版权局著作权合同登记号：图字 01-2006-7281

图书在版编目（CIP）数据

潜在威胁分析：从恶作剧到恶意犯罪 /（美）梅诺（Maynor, D.）等编著；谢俊等译．—北京：中国水利水电出版社，2008

（计算机安全技术丛书）

书名原文：Syngress Force Emerging Thread Analysis: From Mischief to Malicious

ISBN 978-7-5084-5026-1

Ⅰ．潜…　Ⅱ．①梅…②谢…　Ⅲ．电子计算机－安全技术　Ⅳ．TP309

中国版本图书馆 CIP 数据核字（2007）第 155136 号

书　　名	潜在威胁分析——从恶作剧到恶意犯罪
作　　者	[美] David Maynor　等编著
译　　者	谢　俊　潘洪涛　等译
出版发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京蓝空印刷厂
规　　格	787mm×1092mm　16 开本　27 印张　608 千字
版　　次	2008 年 1 月第 1 版　2008 年 1 月第 1 次印刷
印　　数	0001—4000 册
定　　价	58.00 元

万水软件项目应用与实例开发丛书

NIIT资深开发人员编写

创新性的内容安排

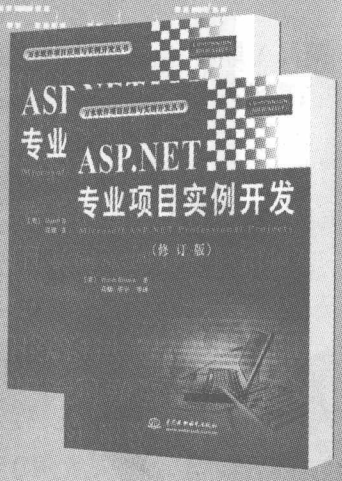
实用的案例开发

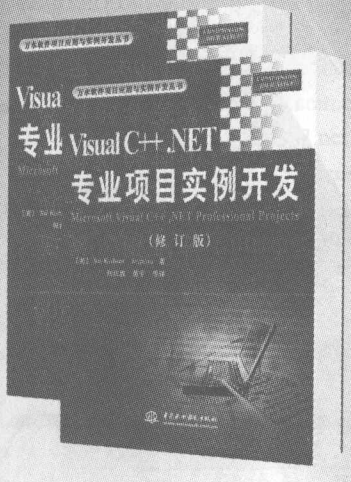
丰富的实例代码

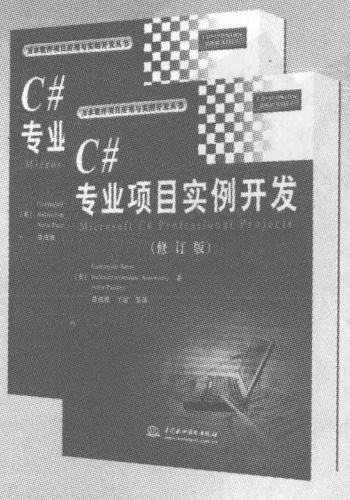
全面的知识讲解

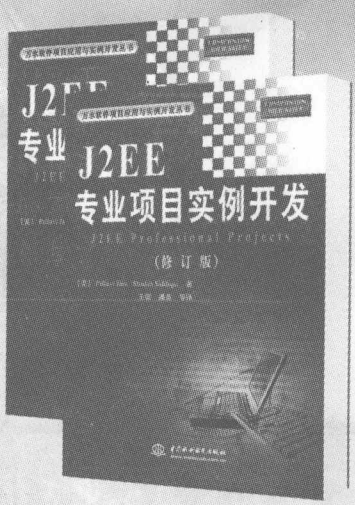
内容由浅入深 循序渐进

理论与实践密切结合









译者序

随着网络和信息技术的高速发展和普及，信息化已经成为现代企业生存和发展的必备条件。在此背景下，网络安全成为人们越来越关注的主题。

本书由众多业内资深权威人士联手打造而成，从而使内容的广度和深度有所保障。本书全面呈现了当前存在的网络威胁的各种形式以及隐藏在它们背后林林总总的技术，并融入了作者们多年工作的经验和心得，以及他们提出的各种行之有效的解决方案。本书共分为五部分：VoIP、恶意软件、钓鱼与垃圾邮件、RFID 和非传统威胁。第一部分包括第 1 章到第 4 章，探讨了 VoIP 通信系统面临的威胁、VoIP 现有的安全基础架构，并针对 VoIP 安全提出了一些建议，同时还专门讨论了 Skype 的安全性。第二部分包括第 5 章到第 8 章，主要讨论了间谍软件的由来、技术和所带来的危害，给出了检测和删除间谍软件的各种方法。第三部分包括第 9 章到第 14 章，探讨大家常见的垃圾邮件、垃圾消息和钓鱼，从深层次对这些技术进行了分析。第四部分包括第 15 章到第 19 章，详细阐述了 RFID 攻击方式和 RFID 的安全性。第五部分包括第 20 章和第 21 章，其中第 20 章讨论了对“人”的攻击，也就是通过人员获得信息；第 21 章由高级安全专家 David Maynor 讲述设备驱动程序攻击方面的知识。综上，本书不仅全面介绍了大家容易想到的病毒防护、木马防护、漏洞检测技术和黑客攻击防护知识及方法，还从深层次分析了 VoIP 安全、恶意软件（包括病毒、木马防护和黑客程序等）、网络钓鱼和 RFID 攻击的防御方法等，可以说，本书基本上囊括了目前存在的各种威胁形式。

通过阅读本书，业内人士和企业网络管理员能够扩大知识面，为企业和政府机构部署更为完善的威胁防御系统，而业余的个人用户也能够了解到目前存在的安全隐患，并找到有效的实际解决办法。我们真诚地希望，本书能够帮助读者从深层次分析网络安全威胁的来源，并给出适当的安全解决方案。

本书由谢俊、潘洪涛主译。参与本书翻译的人还有田玉敏、漆振、侯晓敏、胡娟、于阳、杜玲等。本书内容全面，技术较深，翻译过程中有些仓促，如有差错，敬请读者谅解。

谢　俊

2007 年 10 月

关于作者

David Maynor 是 SecureWorks 的高级研究员，他的职责包括漏洞研发、新逃避技术的开发和评估，以及客户保护的开发。他以前在 ISS Xforce R&D 团队中从事过逆向工程和研究新逃避技术的工作，在佐治亚州技术学院进行过应用程序开发，并与很多企业签订合同，帮助他们进行安全咨询和渗透测试。

Lance James 已经在信息安全社区中工作了 10 多年。他在编程、网络安全、逆向工程、密码设计与密码分析、攻击协议方面有着 10 年以上的经验，并在信息安全领域有独到之处，所以能够为很多企业提供咨询服务，包括刚开始创业的小型公司到很多国内外政府部门，以及财富 500 强和美国的顶级金融机构。过去 3 年间，他一直致力于设计用于预防、跟踪和检测钓鱼与在线欺诈的技术。他是 Dachb0den 实验室（一家著名的南加州“黑客”智囊团组织）的首席科学家，InvisibleNet 的创始人，当地 2600 宪章的重要起草成员，以及 Secure Science Corporation（一家忙于跟踪超过 53 类钓鱼行为的安全软件公司）的首席科学家。作为众多安全会议的发言人常客和各家新闻机构的可靠消息来源，Lance James 被认为是信息安全社区中的宝贵财富。

Brad “RenderMan” Haines 是 wardriving 社区中的活跃成员，他经常现身各种媒体中，而且每年要在好几次会议上发表演讲。由于经常参与 wardriving 社区和无线安全问题，所以他的名字常出现在此类新闻中。他的卓越技能来自于为多家 IT 公司工作和数年潜心研究黑客社区的经历，有时甚至会引起加拿大和美国情报局的注意。他坚守黑客道义，倡导有责任的黑客行为和思想共享，他为无线窃听者（wardriver）新手编写了“行为道德规范”，并且非常喜欢在公司会议上发言，对黑客和无线窃听者的负面形象提出忠告。由于他的方法太有个性，忽视了传统逻辑体系，他的工作经常被认为是荒谬的。您可以在加拿大艾伯塔省的埃德蒙顿找到他，他很可能正在分析什么事情。

Thomas Porter 博士（CISSP、IAM、CCNP、CCDA、CCNA、ACE、CCSA、CCSE 和 MCSE）是 Avaya 的咨询与系统集成实践部门的首席安全架构师。他也是 FIFA World Cup 2006 的网络安全负责人。

作为一名顾问、演讲家和安全工具开发者，Porter 在网络与安全领域中已经打拼了 10 多年。Porter 当前的技术兴趣包括 VoIP 安全、嵌入式微控制器开发、FPGA 以太网工具和 H.323/SIP 漏洞测试环境。他是 IEEE 和 OASIS（Organization for the Advancement of Structured Information Standards，结构化信息标准推动组织）的成员。Porter 最近为 SecurityFocus 发表了几篇基础性研究文章，标题为“H.323 Mediated Voice over IP: Protocols, Vulnerabilities, and Remediation”和“Perils of Deep Packet Inspection”。

Tom 和妻子 Kinga 以及两条乞沙比克猎犬一起居住在北卡罗来纳州的 Chapel Hill，他的妻子是北卡罗来纳大学的内科医学教授。

Brian Baskin [MCP、CTT+]是 Computer Sciences 公司的研发人员，在防御计算机犯罪中心（Defense Cyber Crime Center，DC3）主攻计算机调查培训程序（Computer Investigations Training Program，DCITP）。在这里，他负责研究、开发和教导针对军事和法律实施机构成员的计算机法证课程。Brain 目前专攻 Linux/Solaris 指令调查，以及对各种网络应用程序的调查。他设计并实现了可应用于各种场景中的网络，还完成了一些渗透测试过程。

Brian 授课已有 6 年时间，他每年都要在 DoD 计算机犯罪会议上发表演讲。他是一位狂热的业余程序员，精通多种编程语言。他 11 岁时，父亲给他买了一本 QuickC，从此他把生命中的大部分时间都花在了实现这门技术上。从 1994 年以来，他就是一位热心的 Linux 用户，一有机会就盯着终端显示屏，并以此为乐。他已经在网络环境中工作了 10 多年，从小型的 Novell 网络到基于 Windows 的大型任务关键型网络，他都熟稔于心。

Brian 与他可爱的妻子和儿子居住在巴尔的摩的 MD 区。他还是 Lightning Owners of Maryland 汽车俱乐部的发起人和主席。Brian 是一名摩托车运动爱好者，他花了很多时间来组装和驾驶他的爱车。他把成功的很大一部分归功于他的父母，在他很小的时候，父母就把家用的 80286 电脑给了他，让他自由探索技术。

Tony Bradley（CISSP-ISSAP）是 About.com 的领路人，这个 Internet 网络安全站点是纽约时代公司的一部分。他也为很多其他 Web 站点和刊物撰稿，包括 PC World、SearchSecurity.com、WindowsNetworking.com、Smart Computing magazine 和 Information Security magazine。目前，作为一家财富 100 强公司的安全架构师和咨询师，Tony 不断为财富 500 强公司开发着更好的防病毒安全策略和技术，并提高其事故响应速度，同时他也在较小的公司中担任网络管理员并提供技术支持。

Tony 是 CISSP（Certified Information Systems Security Professional，认证的信息系统安全专家）和 ISSAP（Information Systems Security Architecture Professional，信息系统安全架构专家）。他还取得了一些 Microsoft 认证，包括 Windows 2000 的 MCSE（Microsoft Certified Systems Engineer，微软认证系统工程师）和 MCSA（Microsoft Certified Systems Administrator，微软认证系统管理员），以及 Windows NT 的 MCP（Microsoft Certified Professional，微软认证专家）。Tony 被 Microsoft 授予 Windows 安全领域中的 MVP（Most Valuable Professional，最有价值专家）。

在他的 About.com 站点上，Tony 每月平均要查看超过 600000 个页面，向 25000 位订阅者发送他的每周通讯。他开发了一门共分为 10 个部分的计算机安全 101 课程，自问世以来这个课程已经有数千人参加，而且还在不断推广和赢得好评。除了他在 Web 站点和杂志方面的贡献以外，Tony 还是 Hacker’s Challenge 3（ISBN: 0072263040）一书的合著者，以及 Winternals: Defragmentation, Recovery, and Administration Field Guide（ISBN: 1597490792）和 Combating Spyware in the Enterprise（ISBN: 1597490644）两本书的撰稿人。

Jeremy Faircloth（Security+、CCNA、MCSE、MCP+I、A+等）是 EchoStar Satellite L.L.C. 的一位 IT 经理，他和他的团队设计并维护了企业范围内的客户端/服务器和基于 Web 的技术。他还可以为其他 IT 专业人士提供技术资源，他的专业技能可以帮助他人拓展知识面。作为一名有着 13 年以上实际 IT 从业经验的系统工程师，他已经成为了很多领域中的专家，

包括 Web 开发、数据库管理、企业安全、网络设计和项目管理。Jeremy 为几本 Syngress 书籍供过稿，包括 Microsoft Log Parser Toolkit（Syngress, ISBN: 1932266526）、Managing and Securing a Cisco SWAN（ISBN: 1-932266-91-7）、C# for Java Programmers（ISBN: 1-931836-54-X）、Snort 2.0 Intrusion Detection（ISBN: 1-931836-74-4）和 Security+ Study Guide & DVD Training System（ISBN: 1-931836-72-8）。

Paul Piccard 担任 Webroot 的威胁研究负责人，他把重点放在研发工作上，并为 Webroot 客户提供了早期识别、警告和响应服务。在加入 Webroot 之前，Piccard 是 Internet Security Systems 全球威胁操作中心的管理人。这家顶尖的检测和分析机构维护着 Internet 威胁的全球视图，负责跟踪和分析黑客、恶意 Internet 行为和四大洲的全球 Internet 安全威胁。

在职业生涯中，他担任过 VistaScape Security Systems、Lehman Brothers 和 Coopers & Lybrand 的管理岗位。Piccard 曾是每个季度的 Internet Risk Impact Summary（IRIS）报告的研究人员和作者。他拥有纽约福特汉姆大学的艺术学士学位。

Frank Thornton 经营着他自己的技术咨询公司 Blackthorn Systems，专门解决无线网络方面的问题。他主要研究方向包括无线网络架构、设计和实现，以及网络问题解决和优化。对业余无线电的爱好帮助他把计算机和无线网络联系起来。在小时候了解到烙铁温度很高之后，他甚至就知道如何维修硬件了。除了计算机和无线方面的兴趣之外，Frank 也是一名有多年经验的警官。作为侦察和法证专家，他曾调查过大约 100 名杀人犯和数以千计的其他犯罪事件。

结合以上两种专业爱好，他成为了建立 ANSI 标准“ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information”的小组成员。他与人合著了 WarDriving: Drive, Detect, and Defend: A Guide to Wireless Security（Syngress Publishing, ISBN: 1-93183-60-3）一书，并为 IT Ethics Handbook: Right and Wrong for IT Professionals（Syngress, ISBN: 1-931836-14-0）和 Game Console Hacking: Xbox, PlayStation, Nintendo, Atari, & Gamepark 32（ISBN: 1-931836-31-0）等书供过稿。他与妻子居住在佛蒙特州。

Anand Das 在为国防部（Department of Defense，DOD）和商业部门创建和实现业务企业架构方面有着 17 年以上的经验。他是 Commerce Events（一家于 2001 年率先创建 RFID 中间件的企业软件公司）的创始人和 CTO。Anand 是推动全球的 RFID 和无线标准发展的 EPCglobal and INCITS T20 RTLS 委员会的创始成员。他勾划了早期 RFID 中间件产品 AdaptLink™ 的产品战略，并成功领导了企业范围内的部署，其中包括空军供应链的多站点展示。以前他曾是 SAIC 的副总裁，领导了跨多个行业的 RFID 实践，并完成了跨美洲、亚洲、欧洲和南非的 RFID 基础架构全球布局。他担任过 VeriSign 的公司联系人，并在为联邦和商业公司中 EPCglobal 网络的构建中扮演了重要角色。更早的时候，他是 BEA Systems 的首席架构师，负责 Weblogic Integration 产品套件的概念化和构建。他为 ebXML 和 RosettaNet 标准委员会做出了重要贡献，推动了面向服务架构的早期采用进程。Anand 在 Vitria、Tibco、Adept、Autodesk 和 Intergraph 等公司都担任过重要的管理职位。

Anand 拥有 IIT Kharagpur 的技术学士学位（荣誉称号），以及哥伦比亚大学的科学硕士学位，专业是计算机集成制造。他过去曾担任过 NVTC 的电子商务委员会的主席，是哥

伦比亚特区 TIE Washington 的发起人。Anand 和他的妻子 Annapurna 以及两个孩子一起生活在弗吉尼亚的 Mclean。

Michael Gregg 是 Superior Solutions, Inc.的总裁，在 IT 领域中有着 20 年以上的从业经验。他拥有两个大专毕业证书、一个学士学位和一个硕士学位，并通过了 CISSP、MCSE、MCT、CTT+、A+、N+、Security+、CNA、CCNA、CIW Security Analyst、CCE、CEH、CHFI、CEI、DCNP、ES Dragon IDS、ES Advanced Dragon IDS 和 TICSA 认证。

Michael 的主要职责是引导安全评估，帮助企业和政府机构保护他们的 IT 资源和资产。Michael 著有 4 本书，包括 Inside Network Security Assessment、CISSP Prep Questions、CISSP Exam Cram2 和 Certified Ethical Hacker Exam Prep2。他开发了 4 门高级安全课程，包括为 Global Knowledge 开发的高级安全训练营、为 Intense School 开发的专业黑客实验室指南，以及为 ASPE 开发的网络安全基础和评估网络安全漏洞。他在杂志和 Web 站点上发表的文章超过 50 篇，包括 Certification Magazine、GoCertify、The El Paso Times 和 SearchSecurity。

Michael 还是维拉诺瓦大学的教员，以及维拉诺瓦大学的学院级安全课程的创始人，这些课程包括 IS 安全基础、掌握 IS 安全和高级安全管理。他还是 4 个 TechTarget 站点的站点专家，包括 SearchNetworking、SearchSecurity、SearchMobileNetworking 和 SearchSmallBiz。他是 TechTarget 编辑委员会的成员之一。

Hersh Bhargava 是 RafCore Systems（一家提供 RFID 应用程序开发和分析平台的公司）的创始人和 CTO。他是 RafCore 理念的构思者：使企业能够使用 RFID 提供的自动数据收集技术实时地做出响应。在 RafCore Systems 之前，他还曾创立过 AlbumNet Technologies，主营业务是在线照片共享和打印。由于在构建企业级应用程序方面拥有 15 年经验，他曾在财富 500 强公司种担任过各种高级技术职位。他拥有印度理工学院（IIT－BHU）的计算机科学与工程的技术学士学位。

Craig Edwards 是 ChatSpike IRC 网络的管理员和 IRC 安全软件 IRC Defender（www.ircdefender.org）的设计者。IRC Defender 是一个安全服务，可以将恶意的用户和程序拒于 IRC 网络之外，只要主动维护便可处理最新的威胁。Craig 还是 WinBot IRC bot（www.winbot.co.uk）的设计者，这是一个用于保持对 IRC 通道控制的自动化 IRC 客户端。他花了 5 年多的时间亲自参与该产品的设计、维护以及支持和 Web 站点维护。在此期间，该产品已经在多个英国杂志随附 CD 中发行。

Ronald T. Bandes（CISSP、CCNA、MCSE、Security+）是一位独立的安全顾问。在成为独立顾问之前，他负责众多财富 100 强公司的安全，这些公司包括 JP Morgan、Dun & Bradstreet 和 EDS。Ron 拥有计算机科学的学士学位。

前　言

技术真是很奇怪的事情！就时间而言，不久之前人们还知道他们日常生活中所打交道的事情的一切。如果我们要烹煮什么，就要生火。如果我们要将某些东西捣烂，则需要使用锤子或者石头。如果想要某些东西生长，就要给它浇水。在技术开始渗透到普通人的日常生活中不久，人们就知道了如何使用它来达到自己的目的，但并不都能达到。汽车就是这方面的一个典型例子：大多数人能够驾驶汽车，但要求有人能够加油或调整汽车的正时皮带，他们就傻眼了。对于可能发生的非常危险的事情，正成为知道技术复杂性的人和不知道技术复杂性的人之间的界线。缺乏道德的人认识到了这一知识差距，开始攻击它。您也许曾经问过某个机修工多次并且想知道雨刷器是什么，为什么您要频繁地更换它？当然，如果您去拜访自己的一位汽车知识渊博的朋友，并且告诉他您刚刚又花了 400 美元更换了自己的雨刷器，您可能会看到同样快乐、震惊、恐怖、吃惊和困惑的表情。这种表情大体类似于有人告诉我他赢得了尼日利亚人头奖，或者他已经安装了从邮件中获得的安全更新，或者在 Internet 上玩猴子游戏时赢得了一个 iPod。通常，这仅仅是一种无奈的表情，因为我真的无话可说，也不知道该说什么。

IT 行业和计算机已经提出了见多识广的人和其他人之间的界线问题。大多数人与计算机之间的交互只是局限于浏览电子邮件、Web 冲浪、视频游戏和其他类似任务。目前大多数计算机用户都知道怎样完成他们的任务，但一旦出现什么故障，就会求助于精通技术的朋友、家人或者孩子，请他们帮助解决所陷入的技术沼泽。这一问题还不仅仅限于计算机，现在还包括移动电话、PDA、网络电话（VoIP）。这正与刚才所说的机修工例子完全一样，当然，并非所有的机修工都在等着利用您。一个人可能由于不熟悉这些新技术的实际工作原理而被利用，从而遭受过多的损失或碰到大量糟糕的事情。由于技术是如此普及，永远不要期望普通消费者能够完全理解它的工作原理，或者如何吓跑黑客。但是必须要教育他们，让他们知道所面临的风险，以及在没有深入技术经验的情况下如何保护自己。

本书由 Syngress 的杰出作者撰写，阐述了安全技术人员与非安全技术人员之间的界线。写作本书的目的是，的确有公开的坏人在了解您，并设法利用您没有全面深入的技术知识这一缺陷。这样的例子包括媒体广泛宣传的 VoIP 钓鱼、恶意软件和间谍软件，以及经常被忽视的接近型攻击 Wifi/Bluetooth 和 RFID。

我并非有意恐吓大家要完全远离技术。我只是说，目前最好的防御是逐渐形成怀疑一切的良好习惯。主动提供的电子邮件可能不是什么好事。机场内陌生的蓝牙请求可能并不合法。如果某人在电话中将自己描述成银行的客户服务人员，您也许应该挂断电话并使用已确定的银行电话号码打回去。注意这种小事可能会为您带来帮助。不过，真正安全的唯一方法是弥补见多识广的人与其他人员之间的间隙。

我希望您未来非常安全和幸福。

David Maynor

SecureWorks 公司的高级研究员

目　　录

第 3 部分 钓鱼与垃圾邮件

第 4 部分 RFID