科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

计算机安全精要

电子邮件、因特网及无线安全指南

【美】Tony Bradley 著

罗守山 陈萍 刘琳 周虚 译

Essential Computer Security

Everyone's Guide to E-mail, Internet and Wireless Security

科学出版社

Essential Computer Security

Everyone's Guide to E-mail, Internet and Wireless Security

计算机安全精要

电子邮件、因特网及无线安全指南

〔美〕Tony Bradley 著

罗守山 陈 萍 刘 琳 周 虚 译

科学出版社

北 京

图字：01-2008-2328 号

ISBN：1-59749-114-4

图书在版编目(CIP)数据

计算机安全精要：电子邮件、因特网及无线安全指南/（美）布拉德利（Bradley, T.）等著；罗守山译. —北京：科学出版社，2008
（21 世纪信息安全大系）
ISBN 978-7-03-023098-0

Ⅰ. 计… Ⅱ. ①布…②罗… Ⅲ. 电子计算机-安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2008）第 151972 号

责任编辑：田慎鹏 霍志国/责任校对：钟 洋
责任印制：钱玉芬/封面设计：耕者设计工作室

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 1 月第 一 版 开本：787×1092 1/16
2009 年 1 月第一次印刷 印张：13 3/4
印数：1—4 000 字数：326 000

定价：38.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

作者简介

Tony Bradley（CISSP-ISSAP） 是著名的网络安全公司 About. com 的领导者。他曾在许多媒体发表相关文章，包括 *PC World*、SearchSecurity. com、WindowsNetworking. com，以及 *Smart Computing* 和 *Information Security* 等杂志。目前，Tony 是世界财富 100 强公司的安全设计师和顾问，同时他也推动了财富 500 强公司反病毒的安全策略和技术，以及应急响应方案的实施。

Tony 获得多种认证，包括 CISSP（Certified Information Systems Security Professional）和 ISSAP（Information Systems Security Architecture Professional）、MCSE（Microsoft Certified Systems Engineer，微软认证系统工程师）、MCSA（Microsoft Certified Systems Administrator，微软认证系统管理员）、MCP（Microsoft Certified Professional，微软认证专家），以及 Windows 安全 MVP（Most Valuable Professional，最有价值专家）等。

About. com 网站平均每月有 600 000 的浏览量，并且有 25 000 个固定用户。Tony 创办了 10-part Computer Security 101 课程，至今已培训数千人。除此之外，Tony 还曾参编多部安全图书，包括“*Hacker's Challenge* 3”（ISBN：0072263040）、“*Winternals*：*Defragmentation*，*Recovery*，*and Administration Field Guide*”（ISBN：1597490792），以及“*Combating Spyware in the Enterprise*”（ISBN：1597490644）。

合 著 者

Larry Chaffin 他是 Pluto 网络公司的 CEO/主席，这是一家专注于 VoIP、WLAN 和安全的全球网络咨询公司。他是一位有成就的作者。他是“*Managing Cisco Secure Networks*”（ISBN：1931836566）的合著者，也是“*Skype Me*”（ISBN：1597490326）、“*Practical VoIP Security*”（ISBN：1597490601）和“*Configuring Check Point NGX VPN-1/Firewall-1*”（ISBN：1597490318）的合著者。他也编著了“*Building a VoIP Network with Nortel's MS*5100 ”（ISBN：1597490784）一书及合著/代写了其他 11 种关于 VoIP、WLAN、安全和光盘技术的科技图书。Larry 拥有超过 29 种来自如 Avaya、Cisco、HP、IBM、isc2、Juniper、Microsoft、Nortel、PMI 和 VMware 等公司的证书。他拥有在 22 个国家为很多财富 100 强的公司设计 VoIP、安全、WLAN 和光盘网络的丰富架构经验；他的同行认为他是一位在世界范围内 VoIP 和安全领域的备受尊敬的专家。Larry 花费了大量的时间教授和指导全球的 Voice/VoIP、安全和无线网络领域的技术人员。目前，Larry 正在从事利用 Nortel 的多媒体通信服务器 5100 创建 VoIP 网络方面的工作，而且编著一些关于 Cisco VoIP 网络、实践 VoIP 案例研究和国家网络浪费纳税人的钱的新书。

Larry 合著了第 5 章。

Jennifer Davis 是 Decru 网络应用公司的高级系统管理员。Decru 公司提供存储安全方案以帮助系统管理员保护数据。Jennifer 的专长在脚本、系统自动化、整合与故障排除，以及安全管理等方面。

Jennifer 是 USENIX、SAGE、LoPSA 和 BayLISA 的成员。她住在加利福尼亚州的硅谷。

Jennifer 编写了附录 B。

Paul Summitt（MCSE、CCNA、MCP+I、MCP） 拥有大众传播专业硕士学位。Paul 是一位网络、交换机和数据管理员，也是 Web 和应用开发人员。Paul 编写了一些关于虚拟现实和 Web 开发的书，也是几本关于 Microsoft 技术的书的技术编辑。Paul 和他的妻子 Mary 生活在哥伦比亚的 MO——Mary 也是他的写作同伴。

Paul 合著了第 7 章。

技术编辑

Harlan Carvey（CISSP） 是ISS/IBM计算机取证工程师，主要为ISS客户提供应急响应服务。他主要专注于漏洞评估、渗透测试，以及为联邦政府和商业客户提供应急响应和计算机取证服务。同时，他在应急响应培训方面也有丰富的经验。

Harlan获得弗吉利亚军事学院（Virginia Military Institute）电子工程学士学位和拉瓦尔研究生学院（Naval Postgraduate School）电子工程硕士学位，并且在Usenix、BlackHat、DefCon和HTCIA等会议发表演讲。同时，Harlan还是一位多产的作家，许多期刊和网站都刊载其发表的文章。另外，他还编著了《Windows取证和事件恢复》（*Windows Forensics and Incident Recovery*）一书。

前　言

不可否认，个人电脑的革命已经改变了社会的通信方式。现在，收到一封电子邮件已经变得比收到一封邮政邮件要普遍得多。事实上，计算机网络已经成为生活中不可或缺的组成部分。伴随着因特网的增值和扩展，个体和商业机构从来没有如此清楚地认识到访问网络和网络所能提供的是那么重要。生活中的方方面面都可以在因特网上接触到。我们可以在网上购买各种商品；管理银行账户，计划旅游及预订旅店；获取建议和评论；在任何选定的时间、任何的地点同任何用户交流。然而如此的便利性并非没有相应的危险，这种危险包括大家所熟悉的黑客和病毒。本书提供了大量的计算机安全方面的知识。

对于初学者，因特网如同18世纪中期拓荒前的美国西部，对于许多美国人来说它是如此的迷人和让人激动。西部那些广博的资源给予人们新的发现和机会。然而，如同狂野西部一样，因特网严重缺乏规范。缺少恰当、有效的法律来维护它的安全，而且时常充满了让人不愉快的意外事件。所有连接在网上的个人和组织每天都冒着被攻击的危险，同时，他们需要建立和维护自己的安全。

虽然因特网已经成为普遍存在的通信和搜寻工具，但是重要的是要记住因特网是一条双行线——你的电脑连接着它，反之亦然。理解确保安全所需要的工具和技术，意识到自己所处的位置是容易受到攻击的，并确保其电脑安全，这些对用户是有益的。幸运的是，基本的计算机网络安全知识是一个不懂技术的人也能理解的。不论使用的是一个单独的计算机或是整个的计算机网络，Tony Bradley都将会手把手的教给你建立和确保安全所需要的知识。

安全是一个过程，而不是一个产品，并且计算机安全是所有人的责任。你不会把家或者企业的后门敞开留给入侵者，对于计算机里的价值需要同样的审慎。即便Dodge City（道奇城）也需要有Wyatt Earp，在事情失去控制的情况下来维持秩序。在因特网的世界中，没有治安州长。伴随《计算机安全精要》一书，你将会使用计算机安全各方面的基本知识来武装自己。

Douglas Schweitzer，Sc. D.

安全专家，《防御恶意代码》的作者

引　言

购买大多数家用电器的时候，随机都会附有用户手册。用户手册包含家用电器的全部信息。它介绍这个按钮是干什么的，如何安装和设置家电以使其能够工作。用户手册还包括操作家电的实际步骤。通常，还包括如何获得服务、在何处获得服务、零件册、基本故障处理，以及在使用前应该注意的事项。

对于录像机、微波炉、面包机和吸尘器而言，它们都是居家常用的电器，都是家居必需，都有其职能。购买这些东西的时候，是因为它们能够完成具体的任务，而用户手册提供了所有完成这些任务需要的信息。

大多数人把个人计算机也看作是一种家电。对一些用户来说，计算机是一种很棒的计算器，它能跟踪和管理他们的经济状况。对另一些用户来说，计算机是给朋友和家人发送电子邮件的一种通信方式。还有人认为计算机是一种高档的游戏终端，可以运行最新的动作游戏。有关计算机的这个列表可以不断地继续下去。总之计算机是一种多功能的电器，它对不同的人来说意味着不同的功能——有时甚至对相同的人也意味着不同的功能——这取决于用户那时想让计算机做什么。

所以，也许希望计算机有一个非常庞大的、包含所有可能用到的任务的用户手册，不是吗？不幸的是，事实并不是这样。现实是有关计算机的用户手册一般是相当简单的。通常，一台新计算机所带的用户手册中只有一些简单的指令说明，如将哪根电线插入哪个孔就可以启动计算机。还会提供一些关于主板的技术细节，如处理器、内存，以及其他部件在主板的什么位置，或者是如何设置 BIOS（基本输入输出系统——控制和操作主板的“大脑”）。不过大多数计算机用户手册言尽于此。

但是，不能责备计算机制造商。录像机只是预先录制，播放录像带，面包机只设计来烤面包；与这些电器不同，计算机有太多可能的用途，以至于不能在用户手册中全面叙述。

本书就是一本这样的手册，它把系统看成一个整体，并介绍一些保护这个系统的必备知识。当把录像机接入电源没什么特别的事情会发生。当有人接触面包机的时候，也不会有泄露私人财务数据的危险。恶意的攻击者也不会用吸尘器攻击世界上另一些吸尘器。

但是，当把计算机接入互联网，你就变成了一个包含数百万计算机和设备的系统中的一份子。在这个系统中，所有计算机都互相联系并可能影响其他计算机。这里每个计算机是独一无二的，因为它是家用“设备”的一部分，每一个都具有安全的考虑与实现，并且正常运行。

你对计算机的了解程度，可能与你对录像机或者微波炉的了解差不多。你知道如何使用，怎么启动、登录、浏览网页、发送电子邮件等。但是你很可能不知道处理器的速度、内存的容量，或者 TCP 的端口 80 是否开放给外部的连接。你甚至不知道一些攻击者在利用你的计算机。

你可能不想成为计算机或者安全专家。你可能不在乎硬盘有多大、处理器有多快。你只想让计算机以最小的代价完成工作。但是当你在互联网与他人分享信息的时候，如果想安全地使用计算机，那么理解其中的危险、如何避免这些危险、如何保护计算机远离诸如病毒和木马、间谍软件之类的恶意威胁，就很重要了。

已经有了不少关于计算机和网络安全的书，大多数书的问题是，它们都是写给已经了解计算机和网络安全的人的；而普通的计算机用户并不了解网络安全，甚至不知道从哪里开始。本书就是写给普通的计算机用户，或者刚开始接触网络安全的用户，它提供了对不同的威胁及相应防护措施的入门性指导。

我不打算教读者所有的东西，也不指望你们能够成为专家。我只是希望通过阅读本书，讲述这些预防措施——或者甚至只是部分预防措施——能够使你们有一个更安全、更有趣的网上冲浪体验，并且保证缺乏计算机安全知识的你不会在与我们一起分享互联网的时候影响其他人。我希望本书成为互联网用户手册，帮助你理解遇到的危险、告诉应该采取的预防措施，这样就可以让你的“家电”以最小的代价和最少的失败安全地工作。

为什么要写这本书?

本书并不想做到面面俱到。书架上有数以百计的书，覆盖了计算机和网络安全的各个方面。从这些书中，你可以找到很多比本书更深入、技术性更强的信息安全方面的书。也有很多书阐述网络安全的具体方面，如加密、防火墙、备份、恢复等，要比本书更深入、更细节化。

本书写给安全方面的入门者，告诉他们有关“电器”安全操作的信息和建议，不仅仅是为了保护他们自己，同样为了保护与他们联网的人们。我已经尽可能用简单的方式表达，并没有太多的术语，但是如果确实碰到任何缩写或是不熟悉的名词，可以在附录C的术语表中查找。

本书的目的在于介绍足够的计算机和网络安全知识，帮助读者理解潜在的威胁并保护计算机。在每章的最后有该章要点的摘要。

本书着眼于安全，大部分内容可以应用于所有的计算机系统，其中的例子和插图主要来自 Microsoft Windows XP。诸如防火墙、口令、无线网络安全这样主题的细节与具体的操作系统无关，它们可以应用在所有系统上。不必在意是否使用 Windows XP。计算机安全的基本概念不局限于操作系统，而适用于所有的平台。

本书结构

本书分为 4 个主要部分：

- “基础知识”部分阐述了应该立刻掌握的安全知识。只有当这些准备工作完成后，你的计算机才能与其他计算机或互联网连接。如果遵循这些建议，那么就可以安全地连接到互联网。
- “安全进阶”部分对不同的安全技术和如何安全发送电子邮件及网上冲浪做了更深入的解释。
- “测试和维护”部分提供了一些测试计算机和网络安全的方法，以及必须注意安

全功能升级以保护安全。

- “安全资源”部分提供了一些参考资料和关于计算机网络及互联网基本概念的初级读物。这部分是为有志于更进一步提高水平的读者准备的。

章节概述

下面对本书中的章节进行简要的概述。

- 第 1 章：基本 Windows 安全。本章介绍 Windows 操作系统中的基本安全知识，例如，创建和管理用户账户，对文件和文件夹设置访问权限以保护数据。
- 第 2 章：口令。口令是进入计算机系统的钥匙。显然应该仔细选择一个不容易被猜中的或者不易被破解的口令，并且妥善保管。
- 第 3 章：病毒、蠕虫和其他恶意程序。本章探讨反病毒软件是如何工作的，可以防止何种威胁。本章同样包括为了保证始终处于被保护状态，应该更新维护反病毒软件方面的知识。
- 第 4 章：补丁。本章讨论保持计算机系统更新的重要性，这样可以使你免受已知的攻击方式侵犯。本章还包括在新安装的操作系统上打上必要补丁的步骤。
- 第 5 章：边界安全。本章概括了将计算机或网络围上一堵“墙”的安全技术，即所谓的“保护你的边界”。这些技术包括防火墙和入侵检测系统（IDS）。
- 第 6 章：电子邮件安全。电子邮件是一种非凡的通信工具，并且带来越来越高的生产力——前提是你能够摆脱垃圾邮件、欺骗者和带病毒的附件。本章旨在帮助读者尽可能地消除垃圾邮件，这样你就可以把注意力集中到想阅读的电子邮件上了。
- 第 7 章：网上冲浪的隐私和安全。本章简要介绍了上网的时候可能会遇到的潜在威胁，以及如何才能在网上冲浪获得最好的体验的同时，又有效保护计算机、网络和身份。
- 第 8 章：无线网络安全。无线网络使得连接互联网和其他设备更加容易方便。无线网络提供了连接的自由。但是自由的代价就是安全上的威胁，所以得更加谨慎以保护无线数据安全。
- 第 9 章：间谍软件和广告软件。在安装软件、上网冲浪的时候，一些被称为间谍软件或广告软件的小程序可能会安装到计算机上。它们中的一些是合法的，但是很多不是。这些程序都以某种方式监视你的计算机活动，并将相关信息反馈给发布的公司或用户。本章将帮助读者防御间谍软件和广告软件的入侵，以及在已经感染的情况下清除。
- 第 10 章：保持安全。你必须经历了安装安全产品（如反病毒软件、防火墙）的所有麻烦，并且把系统重新设置得尽可能安全。安全是一个过程，而不是一个产品。你必须做一些事情维持计算机安全。
- 第 11 章：当灾难袭来的时候。无论计算机多么安全，数据还是会遭到一些意外。定期备份重要数据是非常重要的。定期做一个备份，以防发生安全事故的时候丢失数据，这种规划也是很重要的。
- 第 12 章：Microsoft 的替代品：Linux。本书大部分着眼于 Microsoft Windows

平台及 Microsoft 自带的产品，如 Outlook Express 和 Internet Explorer。本章涉及其他厂商产品的应用，提高系统的安全性。

- 附录 A：网络通信基础。附录 A 提供了相当多的关于通用网络和互联网的细节。本书仅仅提供一些安全的基础知识，而并不打算讲解所有的事情。但是如果想获取更多的信息，这个附录将帮助读者简单掌握这些东西是如何工作的。
- 附录 B：案例学习：小型办公（5 台电脑、打印机、服务器等）。家庭安全并不像企业环境发展那样成熟。用户在远程办公的时候通常没有时间成为安全专家。这个附录讨论如何使用 netstat 打开系统端口，如何使用 lsof 检查打开的端口，并且包括了一个案例学习。这个案例展示了一个家庭用户是如何在没有很多系统和安全经验的情况下设计一个 SOHO 防火墙的。
- 附录 C：术语表。附录 C 提供了一个安全术语和首字母缩写词的词汇表。当遇到需要解释一些术语的时候，可以当作资料查阅。

目　录

第二部分　安全进阶

第三部分　测试和维护

第四部分　安全资源