信息安全丛书

计算机与网络安全

——如何应对身边的安全问题

[美] MARK CIAMPA 著　　陶 洋 主译

重庆大学出版社

计算机与网络安全

——如何应对身边的安全问题

原著:[美]MARK CIAMPA
主译:陶洋
译者:周霞　赵艳梅　孙清然　李玲香

重庆大学出版社

Mark Ciampa
SECURITY AWARENESS: APPLYING PRACTICAL SECURITY IN YOUR WORLD
ISBN: 0-619-21312-4

981-265-144-6

版贸核渝字(2004)第39号

图书在版编目(CIP)数据

计算机与网络安全——如何应对身边的安全问题/(美)查姆帕(Ciampa,M.)著;陶洋主译.
—重庆:重庆大学出版社,2005.1
(信息安全丛书)
书名原文:Security Awareness:Applying Practical Security in Your World
ISBN 7-5624-3174-4

Ⅰ.计... Ⅱ.①查...②陶... Ⅲ.①电子计算机—安全技术②计算机网络—安全技术
Ⅳ.①TP309②TP393.08

中国版本图书馆CIP数据核字(2004)第112324号

计算机与网络安全——如何应对身边的安全问题
Jisuanji yu Wangluo Anquan——Ruhe Yingdui Shenbian de Anquan Wenti
[美]MARK CIAMPA(查姆帕)著 陶洋 主译

出 版 者:重庆大学出版社 **社 址**:重庆市沙坪坝正街174号重庆大学(A区)内
网 址:http://www.cqup.com.cn **邮 编**:400030
电 话:(023)65102378 65105781 **传 真**:(023)65103686 65105565
出 版 人:张鸽盛
责任编辑:方天瞳 陈晓阳 **版式设计**:陈晓阳
责任校对:廖应碧 **责任印制**:秦 梅
印 刷 者:重庆科情印务有限公司印刷
发 行 者:全国新华书店经销
开 本:787×1092 1/16 **印张**:11.5 **字数**:232千
版 次:2005年1月第1版 2005年1月第1次印刷
书 号:ISBN 7-5624-3174-4
印 数:1—4 000
定 价:18.00元

序

随着世界科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息网络已成为国家和社会发展新的重要战略资源。与此同时，社会对信息的依赖程度越来越高，网络和信息系统的安全问题愈加重要。保障网络与信息系统安全，更好地维护国家安全、经济和社会稳定，是信息化发展中必须要解决的重大问题。

面对复杂多变的国际环境和互联网的广泛应用，我国信息安全问题日益突出。加入世界贸易组织、发展电子政务等，对信息安全保障提出了新的、更高的要求。我国政府始终高度重视信息安全问题，将信息安全作为全面推进我国国民经济和社会信息化进程的重要环节，做出了一系列重要决策和部署。2003 年 9 月国家信息化领导小组研究提出了《关于加强信息安全保障工作的意见》，进一步明确了我国信息安全保障工作的总体要求、主要原则和重点任务；2004 年初又专门召开了全国信息安全保障工作会议，对信息安全保障工作做出了全面部署，为国家信息安全保障体系的建设注入了强劲的动力，将我国的信息安全工作推进到一个崭新的阶段。

有幸经历近 10 年来中国信息化进程的人都不会忘记，我国信息安全事业的发展、技术的进步和产业水平的提升从世界各国，特别是西方发达国家得益颇多。现代信息安全概念和技术的引入，给长期以通信保密为核心的中国信息安全界带来一股清新的风，它们的许多理论、观点、概念和方法对更新我们的安全观念、发展自主的安全技术、加强信息安全的管理等都发挥过相当积极的影响，进入新世纪后，在中国加入 WTO 和经济全球化的推动下，国内外在信息安全领域的学术交流和技术互动日益加深，信息安全国际化已成不可阻挡之势。在统筹考虑国际国内两个大局的背景下，中国信息安全界对于世界各国，尤其是西方发达国家的信息安全理念、法则、规范和实践经验的学习与研究正掀起新一轮热潮。

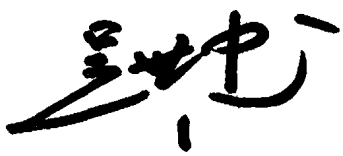
与过去相比，新一轮的学习与研究热潮在内容上已有本质的提高。几年前，西方的信息安全理论和技术让急于寻求解决方案和发展思路的中国信息安全界眼界洞开，我们曾以一种饥不择食的急迫心情将西方的信息安

全理论、概念和做法搬到国内来。但近年来，我们欣喜地看到，中国信息安全产业界和学术界已逐渐走向成熟，开始理性地审视国外的技术与方法，紧密结合中国的实际需要精心选择国外信息安全理论和实践的成果，并在研究、思考的基础上，努力探索适合中国国情的信息安全之路。生活在重庆的几位归国学人从众多的海外著述中精选了《计算机与网络安全——如何应对身边的安全问题》、《信息安全管理》和《灾害恢复指南》3 本，细心译介给国内，就是众多的努力之一。信息安全意识、信息安全管理和安全容灾与恢复正是当下国内急需的知识与方法。从这 3 本书内容的深入浅出和方法的清晰实用，可以看出编译者的良苦用心，相信他们的愿望和努力会得到业界和学界的认可和尊重。

中国信息安全事业的发展需要更系统、更全面、更深入地翻译、介绍国外的经典著述，需要更迅速、更经济、更便捷地学习、掌握他人的实践经验。因此，我们十分乐见《计算机与网络安全——如何应对身边的安全问题》、《信息安全管理》、《灾害恢复指南》3 本译著的出版，并乐于在其付印之前，将个人的观感和陋见附上，以示敬意。

兹为序。

中国信息安全产品测评认证中心　主任
中国信息产业商会信息安全产业分会　理事长
全国信息安全标准化技术委员会　副主任



2004 年秋
于北京昆明湖畔

译　序

这是一本难得的好书，它将深奥的计算机和网络的安全概念、理论、技术以及操作等以非常易懂而生动的语言进行了描述、分析，真正做到了由浅入深、通俗易懂。

该书从病毒到黑客、从小偷到间谍、从门锁到防火墙等等，以独特的视角对计算机及网络安全的各个方面进行了完整而系统地描述，并且对现实生活中的安全实例和Internet的安全防范技巧亦做了全面的描述，清晰地勾画出了信息安全的全貌，为我们的工作、学习和生活提供了非常有价值的安全知识和操作技巧。

该书充分结合管理、技术和生活工作方式，对安全知识进行了系统而详细地阐述，大大超越了以往仅就安全技术进行介绍和分析的著作方式，因而使得该书不论对专业技术人员还是普通读者都大有益处。书中有大量的基于安全应用的基本概念介绍和分析，这会帮助读者更加深刻地理解信息安全。该书的另一个特点在于给出了大量常用的安全技巧操作项目，让读者有实践的项目，通过这些项目实践可以大大提高读者的信息安全防范技能。

全书分为六章，第一章介绍了计算机及网络安全的概貌，让读者对安全及危害有一个全面的了解；第二章着重介绍了个人计算机安全及防范的措施等；第三章从管理的角度对团体及组织安全的技巧和措施进行了介绍；第四章介绍了Internet安全；第五章介绍了网络安全；第六章对涉及信息安全的各个方面进行了系统而全面地介绍和描述。

全书由陶洋教授主译且审校全书，周霞翻译第二章、第六章部分等、赵艳梅翻译第一章和第三章部分等、孙清然翻译第四章和第六章部分、李玲香翻译第五章和第三章部分。

前　言

安全问题是计算机及网络领域非常重要的主题。其原因是显而易见的，因为当前有超过 85 000 种计算机病毒在毫无阻碍地传播，并且平均每个小时就会产生一种新的病毒。2003 年出现的一种叫做 Slammer 的蠕虫病毒（针对 Microsoft SQL Server 2000 和 Microsoft Desktop Engine（MSDE）2000 的一种蠕虫），在它出现的最初 11 分钟内就感染了 75 000 台计算机，其后，受感染数每过 8.5 秒就翻一番。在 2003 年出现了病毒感染的最高峰，病毒每秒钟扫描 5 500 万台计算机。一种叫 Blaster（冲击波）的蠕虫病毒在它出现的最初 4 小时内感染了 138 000 台计算机，最终感染数超过 140 万台。这样的例子不胜枚举！无论何地你都能发现计算机遭受攻击的新迹象，让你时刻不能忘记安全防范。

目前，很多人对如何保证一台计算机以及家庭、小型工作室中网络的安全仍然充满了神秘感。反病毒软件将阻止何种攻击？如何安装防火墙？如何阻止攻击者通过互联网攻击我的计算机？是否需要安装反病毒软件以及在什么地方可以找到它？何时需要安装 Windows 补丁？对大多数人来说，掌握如何在遭受攻击时确保计算机安全的方法似乎是一件令人生畏的事。

本书为你提供了确保计算机及网络安全所需要的知识和技巧。给出了计算机及网络安全领域的基础知识，它适用于包括专业人员、学生和家庭计算机使用者在内的所有用户。对于安全这一主题，本书将通过用户在实际生活中的诸多安全实践经验来进行介绍和描述，阐明计算机及网络安全的必要性以及确保计算机及网络安全的必备要素。本书除了介绍计算机及网络安全的概念之外，还包括如何确保计算机安全的实用技巧，从而在日趋复杂的攻击面前确保计算机和网络的安全。

本书每章都提供了许多让读者实践的技巧，介绍了如何确保计算机及网络的安全。另外，每章节还向读者展示了如何安全地使用和配置软件和硬件的内容。通过自己动手实践以上这些内容和技巧，有助于让你的学习体验更加生动、真实。除实践操作项目之外，每章通过实际的安全项目让你充当安全顾问的角色，给予你一种经验，并在不同工作场景中解决问题。此外，每章中还包括了习题，以此来巩固本章所学知识，同时也帮助你将安全实战技巧应用于你自己的领域中。

章节内容

本书各章将讨论以下内容：

第 1 章:“计算机安全入门”。阐述计算机安全的重要性及其原因、解释攻击者的概念以及他们如何进行攻击,此外,还概述了保护计算机系统的基本任务。

第 2 章:“个人计算机安全”。讲述如何通过保护设备及存储于其中的数据的安全,以及阻止病毒和间谍件控制你的计算机来保证桌面计算机(PC)及便携式电脑的安全。

第 3 章:“团体及组织安全”。描述了团体或组织如何通过安全策略、人力资源程序和商业持续性计划来营造一个安全的环境。

第 4 章:“Internet 安全”。解释攻击是如何通过因特网进行的以及该采取怎样的措施来减少因特网和电子邮件的攻击所带来的风险。

第 5 章:“网络安全”。描述各种类型的网络安全攻击,讲述如何建立有线和无线的网络安全防护。

第 6 章:“全局安全”。综述如何预防攻击,如何保持警惕以及攻击发生之后所采取的应对措施。

本书特点

为了确保学习的成效,本书在教学上具有以下特点:

■ 章目标:本书每章的开始部分都包含了本章中应该掌握内容的详细列表。这个列表好比一个学习助手,可以为你提供本章内容的快速浏览。

■ 插图和表格:众多的插图和表格帮助你更好地理解和运用计算机安全知识和技巧。

■ 章末尾材料:每章的结尾部分都包含了对本章内容的小结,具有以下特点:

■ 章小结:每章正文后都有一个关于该章内容的摘要。该摘要可以帮助你复习本章相关内容。

■ 关键术语列表:每章中所有用粗体字表示的关键术语都汇总在每章末尾的关键术语列表里面,可以帮助你检查是否掌握了这些术语。

■ 复习题:每章的复习题可以巩固你对本章节内容的理解。通过回答这些问题可以确保你已经掌握了本章中的重要概念。

■ 实践项目:虽然理解与安全相关的概念很重要,但是它并不能提高你在现实生活中的经验。为了提高读者的应用或实战能力,每章提供了大量的实践项目,使读者能在设立和配置安全项目方面获取经验。

■ 安全项目:位于每章结束部分的是多段式的案例。在这些涉及面极广的案例中,作为一个假设的 Woodlake 顾问,你将通过实际研究、操作、分析并解决问题来应用本章中所学知识。

正文与图例说明

本书在适当的地方加入了附加的资料和习题，帮助你更好地理解本章所讨论的内容。正文中的一些图标会提示你注意这些附加的资料。本书中所使用的图标如下：

警告：提醒你注意可能出现的错误和问题，并且说明如何避免。

注释：提示你注意和主题内容相关的附加的有用资料。

小技巧：基于作者自身的经验，为你提供关于攻击的一些附加的信息，并且指导你在实际情形中如何应付。

实践项目：本书中每个实践项目都由相应的图标提示，并且附着关于该项目的描述。

安全项目：是一些涉及面广、有一定情节的命题，要求读者独立地运用学过的知识来解决各种各样的问题。

教师阅读材料

下面这些补充的材料在使用本书进行教学活动时可以用到。教师只须填写书末的教辅材料申请表，寄给 THOMSON 公司北京办事处就可以索要如下资料。

电子版的教师手册 本书所附的教师手册中包含了对备课有帮助的资料：对教学活动的建议、教学中的讨论题以及其他附加资料。

习题答案 每章节后所有材料的答案，包括复习题、实践技巧和探索性的练习。

考试测评系统 本书有一套考试测评系统，这是一套可供教师创建和管理，进行书面的、局域网的以及因特网的测试的强大软件包。考试测评系统包含了上百个关于本书内容的考题，使学生能够列出详细的学习指南，包括供以后复习用的参考意见。基于局域网计算机和因特网的考试系统允许学生在他们自己的计算机上进行上机考试并由计算机自动评分，从而节约了教师的时间。

幻灯片 本书的每章都附带了相应的 Miscosoft Powerpoint(幻灯片)附件。它可以用于教室中的教学活动，也可用作学生进行网络学习的课件，或者作为参考资料打印后分发给学生。教师可以自由地添加自己需要在上课时讲到的补充话题。

图片文件 本书中所有的图片及插图都以位图格式的文件附在教师光盘中。与幻灯片相类似,它们可以用于教师课堂教学、学生复习,或者作为参考资料打印后分发给学生。

写在前面

学生必读

本书可以帮助你了解计算机及网络安全的相关知识。每章都以简练易懂的语言来描述与计算机及网络安全相关的信息，帮助你在不同的环境中设计和运用它们。每章后面附有复习题、实践项目，以及你在工作时可能会碰到的逼真的案例。教师可以为你提供复习题的答案和实践项目的相关提示信息。

课外因特网作业 一些项目需要通过因特网来搜索信息。这些项目将有助于你利用这个有价值的资源来与最新的计算机及网络安全出版物保持同步。

课外安全作业 为了完成本书中的项目，你将会使用到计算机和网络。这些项目将让你学到亲手安装与计算机及网络安全相关的软件、配置相关的设置、解决实际的安全问题等实践经验。为了动手实践安全项目，你将需要一台使用 Windows XP 操作系统并连接到因特网的计算机。微软的无线局域网也会用到。为了方便学习，我们推荐你使用有一个或多个可在教室内使用的接入点。此外，每个学生的计算机最好配有无线网络接口卡适配器。虽然不是必须的，但最好将每个接入点都连接到有线以太网，以便于学生体验无线网络的所有便利。

系统要求 推荐使用以下的软件和硬件配置：

桌面计算机

- Windows XP 操作系统
- Microsoft IE6.0 或更高版本的 Internet 浏览器
- 奔腾 733 MHz 以上的处理器
- 96 MB 以上的内存
- VGA 显示器
- 鼠标或其他定位设备
- 无线网络接口卡适配器(NIC)或者外置的 USB 接口无线适配器(需要 USB 1.1 或 2.0 协议支持)
- 硬盘驱动器
- 单面高密度 3.5 英寸软盘驱动器

接入点

■ 微软无线基站 MN-500 接入点

致谢

没有哪个作者可以脱离团队而完成一本书，本书也不例外。高级编辑 Will Pitki 负责将我们的想法整理并使之成型，融入实际的书本中。评论家 Fred Ahrens、Barbara Belon、Glenn Herlinger、Roger Zehner 和 Robert Zemelka 为我们提供了很多有用的批评及建议，而技术编辑 Randy Weaver 帮助确定技术方面的问题。产品经理 Amy Lyon 让一切步入正轨，策划编辑 Jill Batistick 进行协调工作并提供了非常有用的准备材料。制作编辑 Melissa Panagos 通过处理手稿及时地提出建议，为团队提供了帮助。我们同样感谢 Alyssa Winer，她在实习编辑期间将本书完善。另外，Course Technology 出版社的所有员工总是热心地帮助我们，并努力地完成了本书的出版。对以上提到的每个人，我在此表示由衷的谢意！

最后，我要感谢我的家人——我的妻子 Susan 和我的儿子 Brian 和 Greg，他们不间断的兴趣、支持和爱贯穿于我整个写作过程中。没有他们的支持，我不可能完成此书的写作。

献给

我的妻子 Susan 和我的儿子 Brian 和 Greg。

目 录

第一章

计算机安全入门

完成本章的学习之后，你将能够：

- 定义计算机安全并且列出安全的三个基本目标
- 列出可能入侵计算机的六类人
- 说明怎样保护一个系统
- 解释为什么信息安全很重要
- 描述可能对计算机发起的攻击类型
- 描述信息安全的全景

现实生活中的安全问题

学生 Susan 路经电器商店，把她室友的移动电话留下维修。Susan 不明白为什么她的室友 Rhonda 在公寓里还需要固定电话。Susan 用手机接听电话并和她的朋友互发短信。当 Susan 不使用手机时，她通过个人电脑或者学校实验室中的计算机，用 e-mail 和短信与朋友保持联系。

Susan 走进商店的时候，停下来看一台新型的笔记本电脑，好像就是她计划下周要买的那种电脑。Susan 一直在因特网上对比不同的笔记本电脑，并且已经决定在网上购买，这将为她节省好几百美元。

Susan 惊讶地看到一长队的顾客拿着他们的电脑排在维修柜台前。Susan 在排队的时候无意中听到了一些谈话。她于是想起了曾看到的关于“Blaster”蠕虫病毒在周末通过因特网扩散的消息。她想可能是这些顾客的电脑已经感染了这种蠕虫，并需要技术人员帮助他们修复电脑。

在柜台前一位年长的先生正告诉维修人员，他的电脑已经被 Blaster 蠕虫攻击。维修人员问这位先生：“你的操作系统修复盘（recovery disk）带来了吗？”“什么是修复盘？”那先生反问道。

在 Susan 后面，两个妇女开始谈论她们的经历。“那种蠕虫感染了我的电脑，现在电脑已经不能启动了！”一位妇女抱怨道。“我的电脑也一样，”另一个说，“蠕虫把我的打印机颜色弄淡了，我恨这些蠕虫。”

排在 Susan 后面的两个年轻男子也正谈论发生的事情。“有人告诉我反病毒软件不能抵御蠕虫，只有防火墙可以抵御蠕虫。”另一个男子回答说，“我试图从微软网站上下载防火墙的补丁，但是蠕虫抢先入侵了我的电脑。”

Susan 迷惑了，她心想，“我不知道一个蠕虫病毒可以造成这么坏的影响。”但是她不能完全肯定这些问题全部是蠕虫造成的。毕竟，她的打印机由于墨用完了颜色变淡已经一个月了。Susan 开始怀疑她的电脑是否也已经被感染了。她很快离开了商店匆忙赶回她的公寓。

每一个计算机用户都听说过“攻击”这个词,攻击可能会威胁到他们的计算机。大量关于攻击所带来的威胁以及如何防止攻击的新词汇,已经以它们独特的方式进入我们的日常词汇中:修复盘、蠕虫、反病毒软件、防火墙和补丁,这样的词还可以列出很多。然而大多数的人仍旧没有办法使他们的计算机更安全。

你可以问自己这样一个问题:如果你知道一个令人特别厌恶的网络蠕虫病毒会在下一个小时被激活,你将会采取什么方法来防止你的计算机被感染?安装一个防火墙或者使用反病毒软件?下载一个补丁或者做一个修复盘?拔下你的调制解调器或者硬盘?或者就这么等着,直到你的计算机被感染,然后拿着它到商店去维修?

我们生活在一个与几年前很不相同的世界里。正如国家安全对一个国家来说一直是头等重要的,我们个人计算机安全的重要性也在增加。我们比以前更加依赖我们的计算机来处理每天的事务。计算机对于我们而言,在学校学习、在单位工作以及家庭管理中都是基本的工具。然而当计算机在我们生活中的重要性持续增长的同时,对我们计算机的攻击事件也同样在不断增长。在 2003 年的前 6 个月里,在计算机上发生了 76 404 件恶意攻击事件,远远超过了 2002 年全年的 21 756 件。对于今天的计算机用户来说,我们有必要拥有丰富的相关知识,对安全保护和防范攻击我们采取正确措施。在现实生活中,安全从没有比现在更重要。

在这章中我们主要介绍安全。首先,我们将定义什么是安全,说明其重要性。第二,我们讨论谁发起了计算机攻击以及这些攻击是怎样发生的。最后,我们将探讨一些信息技术安全的基本概念。

什么是信息安全?

多数人赞同计算机安全是不可缺少的。但是严格的计算机安全定义是什么?一般来说,**安全**(security)是一种脱离威胁和风险的自主状态。以国家安全为例。当一个国家采取措施减少恐怖分子攻击的风险时,它力图使自己远离危险,从而确保国家安全。然而没有哪个国家能够宣称它是完全远离危险的;相反,这是一个永不停止的保卫自己的战斗。由于保护措施的建立和维护,脱离危险还是有可能的。虽然宪法和军队都不能使一个国家完全安全,但宪法必须受到群众的支持和拥护,同时,军队为了公民的安全必须随时保持待命状态。

信息安全(information security),也称为**计算机安全**(computer security),是保护计算机系统免受有害攻击的过程。无论是一台独立的计算机或者一组互连的计算机(被称为**网络**(network)),信息安全都力图保护这些设备和存储在其中的信息。正如国家安全是国家所建立和执行的保护措施产生的结果一样,信息安全也是同样的道理。保护计算机数据并不是轻而易举的事,相反,为了确保计算机的安全性,各种程序必须到位并且要经常维护它们。