新世纪

NEW CENTURY

计算机信息安全

教程

王宝会　王大印　范开菊　等编著

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

新世纪计算机信息安全教程

王宝会　王大印　范开菊　等编著

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

内 容 简 介

本书围绕信息安全领域的核心理论和技术，理论联系实际全面系统地介绍了信息安全相关的理论、实现技术及实用方法。全书共分 10 章，内容包括：信息安全的概念及内涵、IP 协议族的基本知识、各个协议的漏洞分析和对策、防火墙的原理及配置方法、虚拟专用网的概念及构建方法、入侵检测的概念及相关技术、密码学基础及实践、计算机病毒的防治、操作系统安全和攻击与取证技术。为了让读者更好地掌握书中的理论和技术，本书强调通过应用加深对理论的理解，并且反过来为应用提供指导。本书在内容的叙述过程中，理论和实践并重，结合初学者容易忽略的环节进行剖析，力求达到最佳的学习效果。

本书内容系统、完整、实用性较强，可作为各类职业院校信息安全课程的教材，也可供相关工程技术人员和大学及高等专业学校的学生自学参考。

图书在版编目(CIP)数据

新世纪计算机信息安全教程 / 王宝会等编著. —北京：电子工业出版社，2006.1
新世纪电脑应用教程
ISBN 7-121-01272-3

Ⅰ.计... Ⅱ.王... Ⅲ.电子计算机－安全技术－教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2005）第 050437 号

责任编辑：祁玉芹
印　　刷：北京市天竺颖华印刷厂
出版发行：电子工业出版社出版
　　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：787×1092　1/16　印张：21.75　字数：476 千字
印　　次：2006 年 1 月第 1 次印刷
印　　数：6000 册　　定价：28.00 元

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。

出 版 说 明

电脑作为一种工具，已经广泛地应用到现代社会的各个领域，正在改变各行各业的生产方式以及人们的生活方式。在进入新世纪之后，不掌握电脑应用技能就跟不上时代的发展，这已成为不争的事实。因此，如何快速、经济地获得使用电脑的知识和应用技术，并将所学到的知识和技能应用于现实生活和实际工作中，已成为新世纪每个人迫切需要解决的新问题。

为适应这种需求，各种电脑应用培训班应运而生，目前已成为我国电脑应用技能教育队伍中一支不可忽视的生力军。而随着教育改革的不断深入，各类高等和中等职业教育中的电脑应用专业也有了长足的发展。然而，目前市场上的电脑图书虽然种类繁多，但适合我国国情的、学与教两相宜的教材却很少。

2001 年推出的《新世纪电脑应用培训教程》丛书，正好满足了这种需求。由于其定位准确、实用性强，受到了读者好评，产生了广泛的影响。但是，三年多来，读者的需求有了提高，培训模式和教学方法都发生了深刻的变化，这就要求我们与时俱进，萃取其精华，推出具有新特色的《新世纪电脑应用教程》丛书。

《新世纪电脑应用教程》丛书是在我们对目前人才市场的需求进行调查分析，以及对高等院校、职业院校及各类培训机构的师生进行广泛调查的基础上，约请长期工作在教学第一线并具有丰富教学与培训经验的教师和相关领域的专家编写的一套系列丛书。

本丛书是为所有从事电脑教学的老师和需要接受电脑应用技能培训或自学的人员编写的，可作为各类高等院校及下属的二级学院、职业院校、成人院校的公修电脑教材，也可用做电脑培训班的培训教材与电脑初、中级用户的自学参考书。它的鲜明的特点就是“就业导向，突出技能，实用性强”。

本丛书并非目前高等教育教材的浓缩和删减，或在较低层次上的重复，亦非软件说明书的翻版，而是为了满足电脑应用和就业现状的需求，对传统电脑教育的强有力的补充。为了实现就业导向的目标，我们认真调研了读者从事的行业或将来可能从事的行业，有针对性地安排内容，专门针对不同行业出版不同版本的教材，尽可能地做到“产教结合”。这样也可以一定程度地克服理论(知识)脱离实际、教学内容游离于应用背景之外的问题，培养适应社会就业需求的“即插即用”型人才。

传统教材以罗列知识点为主，学生跟着教材走，动手少，练习少，其结果是知其然而不知其所以然，举一反三的能力差，实际应用和动手能力差。为了突出技能训练，本丛书在内容安排上，不仅符合“由感性到理性”这一普遍的认知规律，增加了大量的实例、课后的思考练习题和上机实践，使读者能够在实践中理解和积累知识，在知识积累的基础上进行有创造性的实践，而且在内容的组织结构上适应“以学生为中心”的教学模式，强调“学”重于“教”，使教师从知识的传授者、教学的组织领导者转变成为学习过程中的咨询者、指导者和伙伴，充分发挥老师的指导作用和学习者的主观能动性。

为了突出实用性，本丛书采用了项目教学法，以任务驱动的方式安排内容。针对某一具体任务，以“提出需求—设计方案—解决问题”的方式，加强思考与实践环节，真正做到“授人以渔”，使读者在读完一本书后能够独立完成一个较复杂的项目，在千变万化的实际应用中能够从容应对，不被学习难点所困惑，摆脱“读死书”所带来的困境。

本丛书追求语言严谨、通俗、准确，专业词语全书统一，操作步骤明确且采用图文并茂的描述方法，避免晦涩难懂的语言与容易产生歧义的描述。此外，为了方便教学使用，在每本书中每章开头明确地指出本章的教学目标和重点、难点，结尾增加了对本章的小结，既有助于教师抓住重点确定自己的教学计划，又有利于读者自学。

目前本丛书所涉及到的应用领域主要有程序设计、网络管理、数据库的管理与开发、平面与三维设计、网页设计、专业排版、多媒体制作、信息技术与信息安全、电子商务、网站建设、系统管理与维护，以及建筑、机械等电脑应用最为密集的行业。所涉及的软件基本上涵盖了目前的各种经典主流软件与流行面虽窄但技术重要的软件。本丛书对于软件版本的选择原则是：紧跟软件更新步伐，以最近半年新推出的成熟版本为选择的重点；对于兼有中英文版本的软件，尽量舍弃英文版而选用中文版，充分保证图书的技术先进性与应用的普及性。

我们的目标是为所有读者提供读得懂、学得会、用得巧的教学和自学教程，我们期盼着每个阅读本丛书的教师满意、读者成功。

电子工业出版社

前　言

当今的人类社会已经步入了信息时代，随着互联网技术的飞速发展，信息的地位也就变得越来越重要。目前，信息资源已成为最能代表一个国家综合国力的重要的战略资源。因此，如何确保信息内容的安全就成为一个重要的课题。我们必须把这一课题放在全球战略的高度加以考虑。信息安全技术是伴随着信息技术的发展和应用而兴起的，随着信息技术在全球政治和经济生活中地位的日益提高，众多发达国家不惜巨资支持在信息安全领域的研究，把在这一领域的技术创新和应用作为加强本国国际竞争力的重要手段。我国作为发展中国家，刚刚走上信息化的道路，并且在信息化建设中已经取得了初步的成果。因此，当前了解和掌握信息安全的相关知识和技术是非常必要和有意义的。

鉴于此，目前已经有越来越多的人希望了解并掌握信息安全领域的知识和相关技能。在这种强大需求的推动下，各大中院校纷纷开设了信息安全专业，同时加大了对信息安全领域科研的投入。

本书共分 10 章，理论联系实际全面系统地介绍了信息安全相关的理论、实现技术及实用方法。内容包括信息安全的概念及内涵，IP 协议族的基本知识、各个协议的漏洞分析和对策、防火墙的原理及配置方法、虚拟专用网的概念及构建方法、入侵检测的概念及相关技术、密码学基础及实践、计算机病毒的防治、操作系统安全和攻击与取证技术。为了能使读者更深入地理解信息安全的相关知识，并能熟练地将其运用于实践，在每章的最后还附有大量精心设计的习题。在内容方面，本书充分注意了知识的全面性、完整性、实用性和时效性，使读者不仅能够全面地掌握信息安全的基本知识，更能够快速地将其应用到实践中。本书语言简洁明了、结构清晰、具有较强的针对性。在准确地讲述各个相关原理的同时，通过结合大量的图片、表格，详细介绍了信息安全方面的知识，另外书中还包括许多典型的实例，使读者能够借此更深入地理解信息安全的内涵，使理论和实际能够有机地结合起来。

本书所包含知识的信息量大、覆盖面广，教师可以得心应手地使用它进行教学，学生也可以通过本书进行自学。本书既可以作为计算机及相关专业的教材使用，也可以作为已经学习和掌握典型 IT 技术的相关工程技术人员、网络系统管理人员的参考用书。对于希望快速掌握信息安全技术的入门者，本书也是一本不可多得的参考资料。

本书由王宝会、王大印和范开菊主持编写，其中范开菊编写本书的第 1 章和第 2 章，此外，参加编写的人员还有王亚丽、许鑫、樊昱、程琪、高宁、王优胜、薛艳菊、李南等，在此向他们表示真诚的感谢！由于作者水平有限，书中难免有不妥之处，欢迎广大读者提出宝贵的意见。

我们的电子邮件地址是：qiyuqin@phei.com.cn。

作　者

2005 年 11 月

编 辑 提 示

《新世纪电脑应用教程》丛书自出版以来，受到广大培训学校和读者的普遍好评，我们也收到许多反馈信息。基于读者反馈的信息，为了使这套丛书更好地服务于授课教师的教学，我们为本丛书中新出版的每一本书配备了多媒体教学软件。使用本书作为教材授课的教师，如需要本书的教学软件，可到下面的网址 www.firstarcicl.com.cn 下载。如有问题，可与电子工业出版社天启星文化信息公司联系。

通信地址：北京市海淀区翠微东里甲 2 号为华大厦 3 层　　鄂卫华(收)

邮编：100036

E-mail：qiyuqin@phei.com.cn

电话：(010) 68253127(祁玉芹)

目　录

第 1 章

信息安全概要

教学目标：

通过对本章的学习，需要掌握信息安全的含义及其需要满足的 4 种特性，了解目前存在的对网络信息安全构成威胁的对手和各种攻击方法，掌握信息安全系统的体系结构，准确理解安全服务与安全机制的内容以及两者之间的关系，了解几个重要的安全标准的内容及适用场合，最后要对密码学在信息安全领域的地位及加密/解密的一般操作过程有一个粗略的了解。

教学重点与难点：

1. 正确理解信息安全的含义。
2. 掌握安全服务与安全机制的内容。
3. 准确理解安全服务与安全机制的关系。
4. 掌握加密/解密的一般过程。

1.1 信息安全定义及特性

在定义信息安全之前，首先应该了解信息的概念。什么是信息，这是一个看似简单的问题，但事实却并非如此。信息无处不在、无时不有，它是如此复杂，以至于在众多信息论相关的著作中，对信息的定义和描述各不相同、不一而足。从广义上讲，信息是人类在认识和改造客观世界的过程中，获取到的各种消息、数据和知识。这些信息反映了物质由于时空运动，而在其特征上反映出的差异。从狭义上讲，各个领域所研究的信息的含义是不同的。尽管在学术界中对信息的概念没有一个统一的认识，但通俗地讲，信息就是指数据、消息等可以用符号传送的报道，并且这些报道的内容是接收符号者预先不知道的。

当今的人类社会已经迈入了信息时代，信息也就变得越来越重要。信息资源已成为最能代表一个国家综合国力的重要的战略资源。因此，如何确保信息内容的安全就成为一个重要的课题。我们必须把这一课题放在全球战略的高度加以考虑。信息安全技术是伴随着信息技术的发展和应用而兴起的，随着信息技术在全球经济中地位的日益增强，众多发达国家将在信息安全领域的技术创新和应用作为加强本国国际竞争力的重要手段。我国作为发展中国家，刚刚走上信息化建设的道路，并且在信息化建设中也已经取得了一定的成果。因此，讨论信息安全问题的含义和相关技术是极其有意义的。

那么，究竟何谓“信息安全”呢？信息安全是指：保证信息系统中的数据在存取、处理、传输和服务过程中的保密性、完整性和可用性，以及信息系统本身能连续、可靠、正常地运行，并且在遭到破坏后还能迅速恢复正常使用的安全过程。

20 世纪 90 年代以后，人类社会进入了网络时代，信息共享成为了网络时代最基本的特征。信息安全也就主要体现为面向网络的信息安全。近年来，互联网逐渐发展为世界上最为复杂的系统之一，它将分散在世界各地的数百万台计算机连接到了一个复杂得令人难以想像的物理网络上。在每台计算机上，又有几十、几百个软件在运行，这些程序可能与本机上的其他程序相互作用，也可能通过互联网与其他计算机上的程序相互作用。这个庞大的系统，可能同时接收数百万个用户的输入，并做出响应。互联网规模和容量的不断增加在带来效益的同时，也引起设备的复杂化以及管理的复杂化，为网络带来新的安全隐患。这使得信息安全的概念范围更广，内容更多，系统更复杂。

为保证网络信息的安全，安全系统要满足以下需求：保密性、完整性、可用性和不可否认性。

保密性表示对信息开放范围的控制，指把信息按指定要求不泄露给非授权的个人、实体或过程，或提供其利用的特性，即杜绝有用信息泄露给非授权个人或实体，强调有用信息只为授权对象使用的特征。

完整性要保证信息处于一种未受损的状态，指信息在传输、交换、存储和处理过程中保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储和传输。

可用性是指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。