计算机类

面向21世纪高等院校计算机系列教材

计算机网络安全技术与应用

彭新光 吴兴兴 等 编著

科学出版社
www.sciencep.com

面向21世纪高等院校计算机系列教材

计算机网络安全技术与应用

彭新光　吴兴兴　等　编著

科学出版社

北京

内 容 简 介

本书从计算机网络安全基础理论、工作原理、技术应用和研究前沿多个方面对计算机网络安全技术进行了全面与系统地介绍，内容基本覆盖了当前计算机网络安全领域的核心技术，书中介绍的各种网络安全技术可直接应用于网络安全工程。

本书采用理论、原理、应用和研究为主线的层次知识体系撰写风格，不仅可作为高等院校计算机、通信、信息及电子商务等专业高年级学生或研究生教材，也适用于网络安全技术培训或相关工程技术人员使用。

图书在版编目(CIP)数据

计算机网络安全技术与应用/彭新光，吴兴兴等编著. —北京：科学出版社，2005

（面向21世纪高等院校计算机系列教材）

ISBN 7-03-015937-3

Ⅰ.计… Ⅱ.①彭…②吴… Ⅲ.计算机网络-安全技术

Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2005）第079733号

责任编辑：陈晓萍/责任校对：郝 岚

责任印制：吕春珉/封面设计：三函设计

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

新蕾印刷厂印刷

科学出版社发行 各地新华书店经销

*

2005年9月第 一 版 开本：B5(720×1000)

2005年9月第一次印刷 印张：21

印数：1—3 000 字数：410 000

定价：28.00元

（如有印装质量问题，我社负责调换〈路通〉）

销售部电话 010－62136131 编辑部电话 010－62138978－8001（HI06）

面向21世纪高等院校计算机系列教材

编委会

序

在高度信息化的21世纪，人们越来越认识到信息教育的重要性。人们都迫切希望信息教育能有较大发展。教育信息化也是摆在我们面前的重要任务。教育部明确要求高等教育实行信息化，要求在未来5年内实现信息化教育课程的数量达到15%～30%。信息社会离不开计算机技术，知识经济需要大量的计算机高级人才。我国正在加强计算机的高等教育，正着眼于为新世纪培养高素质的计算机人才，以适应信息社会高速发展的需要。当前，全国各类高等院校都在各专业基础课程计划中增加计算机的课程内容，而作为与计算机科学密切相关的计算机、通信、信息等专业，更是在酝酿着教学的全面改革，以期规划出一整套面向21世纪的、具有中国高校计算机教育特色的课程计划和教材体系。

教育部《关于加强高等学校本科教育工作提高教育质量的若干意见》（教字【2001】4号）文件也强调指出："要大力提倡编写、引进和使用先进教材。教材的质量直接体现着高等教育和科学研究的发展水平，也直接影响本科教学的质量。高等学校要结合学科、专业的调整，加快教材的更新换代。"

为推动高校教学改革，提高教学质量，我们重点抓了21世纪高等教育教学改革项目，组织并支持了"面向21世纪计算机系列教材规划"研究课题。该课题组成员均由高校计算机系的专家教授组成。他们有多年丰富的教学经验，也具有很强的科研能力。该课题的主要目标是密切结合国民经济的需要，优化计算机教材体系结构，力求将国际、国内计算机领域的新概念、新理论、新技术吸收到本系列教材中，编写出具有科学性、先进性、系统性、实用性、实践性很强的教材，经过推广使用，反复修改，不断提高。

"面向21世纪计算机系列教材规划"课题以编写非计算机专业的计算机课程、计算机专业的计算机网络课程、计算机软件课程三个系列教材为主要内容，计划在三年内出版13～16种书，服务于本科生、专科生、研究生，以及网络学院和软件学院的学生。本课题把研究系列教材的重点放在影响和带动计算机学科发展的网络与软件，以及直接推动计算机普及和应用的非计算机专业三个方向上，目的是通过集中优势兵力，加强团队协作，能够在教材建设方面按系列有所突破。

相信本套教材的出版必将对教学改革和教材建设起到很大的推动和示范作用。

2002年六月四日

前　言

随着 Internet 的迅猛发展和信息化建设的发展，计算机网络已经渗透到社会的政治、经济、文化、军事、意识形态和社会生活等各个方面。特别是近年来电子政务、办公自动化、电子商务和企业信息化建设的飞速发展，使网络攻击、计算机病毒、特洛伊木马、网络窃听、邮件截获和滥用特权等各种恶意行为频繁发生。针对重要信息资源和网络基础设施的蓄意破坏、篡改、窃听、假冒、泄露、非法访问等入侵行为给国家安全、经济和社会生活带来了极大的威胁，因此，计算机网络安全已成为当今世界各国共同关注的焦点。在此背景下，越来越多的计算机专业人员与非专业相关人员需要学习和掌握计算机网络安全技术与应用知识。

计算机网络安全是一个涉及计算机科学、计算机网络技术、通信技术、软件工程、密码技术、法律、法规、管理和教育等多个领域的复杂系统工程，本书按照计算机网络安全基础理论、工作原理、技术应用和研究前沿层次体系结构组织内容。对当前计算机网络安全领域的核心技术进行了全面与系统的介绍，内容包括计算机网络安全概述、信息加密技术基础、身份认证与访问控制、防火墙工作原理及应用、网络攻击技术分析、入侵检测系统、计算机病毒防治、安全通信协议、电子邮件系统安全和无线网络安全。在强调基础理论和工作原理的基础上，特别注重网络安全技术的工程实践，书中介绍的各种网络安全技术可直接应用于网络安全工程中。为方便读者学习、分析、设计和实践网络安全技术，多数应用实例均取自目前优秀的网络安全开放源码或非商业软件项目。在撰写风格上力求做到深入浅出、概念清晰且通俗易懂。

此外，本书备有采用 PowerPoint 制作的电子课件，既便于教师利用多媒体授课，也便于教师根据学时准备教案并裁减教学内容。本书配套的教学课件可从科学出版社网站（http://www.sciencep.com）免费下载。

本书由彭新光负责全书结构体系、内容范围、撰写风格的制定以及统稿、编著的组织工作，由余雪丽教授、陈俊杰教授担任主审。全书共 10 章，其中第 1 章、第 6 章、第 10 章由彭新光编写，第 4 章和第 8 章由吴兴兴编写，第 2 章、第 3 章和第 9 章由郭昊编写，第 5 章和第 7 章由王峥编写。

在编写本书的过程中，余雪丽教授、陈俊杰教授认真审阅了全书，同时提出了许多宝贵的修改意见并给予热心指导。段富教授对本书的编写也给予了大力支持和热心帮助。单晓波、杨帆、邵青、武燕、闫天杰、马援丽、靳燕、贾宁、康峰、魏博、王玲分别为各章精心制作了教学课件，谨向他们表示忠心的感谢。

尽管我们尽心尽力编写各章内容，但计算机网络安全技术涉及的知识面十分广泛，而且是一个发展迅速的领域，书中难免存在一些缺点和错误，恳请广大读者给予批评指正。

彭新光

2005 年 5 月

目　录

第1章　计算机网络安全概述

随着 Internet 的迅猛发展和网络社会化的到来，网络已经无所不在地影响着社会的政治、经济、文化、军事、意识形态和社会生活等各个方面。同时在全球范围内，针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量仍在持续不断增加，网络攻击与入侵行为对国家安全、经济和社会生活造成了极大的威胁。因此，网络安全已成为世界各国当今共同关注的焦点。

1.1　网络安全基本概念

1.1.1　网络安全定义

“安全”字典中的定义是为防范间谍活动或蓄意破坏、犯罪、攻击而采取的措施，将安全的一般含义限定在计算机网络范畴，网络安全就是为防范计算机网络硬件、软件、数据偶然或蓄意破坏、篡改、窃听、假冒、泄露、非法访问并保护网络系统持续有效工作的措施总和。

1. 网络安全保护范围

网络安全与信息安全、计算机系统安全和密码安全密切相关，但涉及的保护范围不同。信息安全所涉及的保护范围包括所有信息资源，计算机系统安全将保护范围限定在计算机系统硬件、软件、文件和数据范畴，安全措施通过限制使用计算机的物理场所和利用专用软件或操作系统来实现。密码安全是信息安全、网络安全和计算机系统安全的基础与核心，密码安全是身份认证、访问控制、拒绝否认和防止信息窃取的有效手段。网络安全与信息安全、计算机系统安全和密码安全的关系如图 1.1 所示。

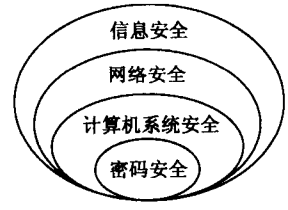

图 1.1　网络安全保护范围

2. 网络安全侧重点

事实上，网络安全也可以看成是计算机网络上的信息安全，凡涉及网络信息的可靠性、保密性、完整性、有效性、可控性和拒绝否认性的理论、技术与管理都属于网络安全的研究范畴，只是不同人员或部门对网络安全关注的侧重点有所

不同。网络安全研究人员更关注从理论上采用数学方法精确描述安全属性，通过安全模型来解决网络安全问题。网络安全工程人员从实际应用角度对成熟的网络安全解决方案和新型网络安全产品更感兴趣，他们更关心各种安全防范工具、操作系统防护技术和安全应急处理措施。网络安全评估人员较多关注的是网络安全评价标准、安全等级划分、安全产品测评方法与工具、网络信息采集以及网络攻击技术。网络管理或网络安全管理人员通常更关心网络安全管理策略、身份认证、访问控制、入侵检测、网络安全审计、网络安全应急响应和计算机病毒防治等安全技术，因为他们负责配置与维护网络在保护授权用户方便访问网络资源的同时，必须防范非法访问、病毒感染、黑客攻击、服务中断和垃圾邮件等各种威胁，一旦系统遭到破坏、数据或文件丢失后，能够采取相应的网络安全应急响应措施予以补救。对国家安全保密部门来说，必须了解网络信息泄露、窃听和过滤的各种技术手段，避免涉及国家政治、军事、经济等重要机密信息的无意或有意泄露；抑制和过滤威胁国家安全的反动与邪教等意识形态信息传播，以免给国家造成重大经济损失；甚至危害到国家安全。对公共安全部门而言，应当熟悉国家和行业部门颁布的常用网络安全监察法律法规、网络安全取证、网络安全审计、知识产权保护、社会文化安全等技术，一旦发现窃取或破坏商业机密信息、软件盗版、电子出版物侵权、色情与暴力信息传播等各种网络违法犯罪行为，能够取得可信的、完整的、准确的、符合国家法律法规的诉讼证据。军事人员则更关心信息对抗、信息加密、安全通信协议、无线网络安全、入侵攻击和网络病毒传播等网络安全综合技术，通过综合利用网络安全技术夺取网络信息优势；扰乱敌方指挥系统；摧毁敌方网络基础设施，以便赢得未来信息战争的决胜权。也许最关注网络安全问题的是广泛使用计算机网络的个人或企业用户，在网络为工作、生活和商务活动带来便捷的同时，他们更关心如何保护个人隐私和商业信息不被窃取、篡改、破坏和非法存取，确保网络信息的保密性、完整性、有效性和拒绝否认性。

1.1.2 网络安全目标

网络安全的最终目标就是通过各种技术与管理手段实现网络信息系统的可靠性、保密性、完整性、有效性、可控性和拒绝否认性。可靠性（reliability）是所有信息系统正常运行的基本前提，通常指信息系统能够在规定的条件与时间内完成规定功能的特性。可控性（controllability）是指信息系统对信息内容和传输具有控制能力的特性。拒绝否认性（no-repudiation）也称为不可抵赖性或不可否认性，是指通信双方不能抵赖或否认已完成的操作和承诺，利用数字签名能够防止通信双方否认曾经发送和接收信息的事实。在多数情况下，网络安全更侧重强调网络信息的保密性、完整性和有效性。

1．保密性

保密性（confidentiality）是指信息系统防止信息非法泄露的特性，信息只限于授权用户使用，保密性主要通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段。口令加密可以防止密码被盗，保护密码是防止信息泄露的关键。如果密码以明文形式传输，在网络上窃取密码是一件十分简单的事情。事实上，大多数网络安全防护系统都采用了基于密码的技术，密码一旦泄露，就意味着整个安全防护系统的全面崩溃。机密文件和重要电子邮件在 Internet 上传输也需要加密，加密后的文件和邮件即使被劫持，尽管多数加密算法是公开的，但由于没有正确密钥进行解密，劫持的密文仍然是不可读的。此外，机密文件即使不在网络上传输，也应该进行加密，否则，窃取密码就可以获得机密文件。对机密文件加密可以提供双重保护。

2．完整性

完整性（integrity）是指信息未经授权不能改变的特性，完整性与保密性强调的侧重点不同。保密性强调信息不能非法泄露，而完整性强调信息在存储和传输过程中不能被偶然或蓄意修改、删除、伪造、添加、破坏或丢失，信息在存储和传输过程中必须保持原样。信息完整性表明了信息的可靠性、正确性、有效性和一致性，只有完整的信息才是可信任的信息。影响信息完整性的因素主要有硬件故障、软件故障、网络故障、灾害事件、入侵攻击和计算机病毒等，保障信息完整性的技术主要有安全通信协议、密码校验和数字签名等。实际上，数据备份是防范信息完整性受到破坏时的最有效恢复手段。

3．有效性

有效性（availability）是指信息资源容许授权用户按需访问的特性，有效性是信息系统面向用户服务的安全特性。信息系统只有持续有效，授权用户才能随时、随地根据自己的需要访问信息系统提供的服务。有效性在强调面向用户服务的同时，还必须进行身份认证与访问控制，只有合法用户才能访问限定权限的信息资源。一般而言，如果网络信息系统能够满足保密性、完整性和有效性三个安全目标，在通常意义下就可认为信息系统是安全的。

1.1.3 网络安全模型

为了实现网络安全目标，安全研究人员希望通过构造网络安全理论模型获得完整的网络安全解决方案。早期的网络安全模型主要从安全操作系统、信息加密、身份认证、访问控制和服务安全访问等方面来保障网络系统的安全性，但网络安全解决方案是一个涉及法律、法规、管理、技术和教育等多个因素的复杂系

统工程，单凭几个安全技术不可能保障网络系统的安全性。事实上，安全只具有相对意义，绝对的安全只是一个理念，任何安全模型都不可能将所有可能的安全隐患考虑周全。因此，理想的网络安全模型永远不会存在。

由因特网安全系统公司 ISS（Internet Security Systems）提出的著名 PPDR（policy protection detection response）网络安全模型在国际上被公认为具有一定的可操作性，ISS 公司最早提出的是 PDR（protection detection response）模型，PPDR 模型是 PDR 模型的改进版。许多网络安全公司出于商业策略考虑，也分别提出了各自的网络安全模型，但本质内容仍然来自 PPDR 模型。包括 ISS 公司也将 PPDR 模型改版为 PADIMEE 模型，PADIMEE 分别表示策略（policy）、评估（assessment）、设计（design）、履行（implementation）、管理（management）、应急响应（emergency response）和教育（education）。

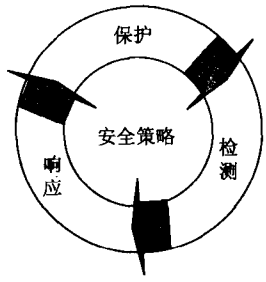

图 1.2　PPDR 网络安全模型

PPDR 网络安全模型如图 1.2 所示，包括策略、保护、检测和响应四个部分。安全策略是 PPDR 模型的核心；是围绕安全目标、依据网络具体应用、针对网络安全等级在网络安全管理过程中必须遵守的原则。安全策略的制定与实施依赖于安全技术、安全管理和法律法规，先进的网络安全技术为网络安全防范提供了技术保障；严格的网络安全管理为实施安全策略提供了基础；完善的法律法规为制定网络安全策略提供了坚强后盾。

安全保护是网络安全的第一道防线，包括安全细则、安全配置和各种安全防御措施，能够阻止绝大多数网络入侵和危害行为。安全细则是在安全策略基础上根据不同网络应用制定的规章制度；安全配置主要是在安全策略指导下确保服务安全与合理分配用户权限；安全防御措施主要包括信息加密、身份认证、访问控制、防火墙、病毒防治、风险评估和虚拟专用网 VPN（virtual private networking）等安全防范组件。入侵检测是网络安全的第二道防线，目的是采用主动出击方式实时检测合法用户滥用特权、第一道防线遗漏的攻击、未知攻击和各种威胁网络安全的异常行为，通过安全监控中心掌握整个网络的运行状态，采用与安全防御措施联动方式尽可能降低威胁网络安全的风险。发现恶意攻击或威胁网络安全的异常行为后，应急响应能够在网络系统受到危害之前，采用用户定义或自动响应方式及时阻断进一步的破坏活动。通过详细记录入侵过程为入侵跟踪和计算机取证奠定基础，应急响应通常还包括数据和系统恢复措施，以最大程度地减小破坏造成的损失。

1.1.4　网络安全策略

网络安全策略是保障机构网络安全的指导文件，一般而言，网络安全策略包