普通高等教育计算机规划教材

网络安全技术及应用

刘京菊　王永杰　等编著

提供电子教案

下载网址 http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

普通高等教育计算机规划教材

网络安全技术及应用

刘京菊　王永杰　梁亚声　汪永益　编著

机 械 工 业 出 版 社

本书系统介绍了计算机网络安全技术原理和实际应用。主要内容包括：网络安全概念与体系结构、实体安全技术、数据加密与认证技术、防火墙技术、入侵检测技术、系统安全技术、网络应用安全技术、恶意代码防范技术、网络安全检测与分析技术、数据备份与恢复技术。本书内容新颖、全面，反映了典型的网络安全技术及其应用的最新进展，在内容安排上将技术原理和实际应用有机结合，不刻意深入论述技术原理，力求使读者看得懂、记得住、用得精。

本书可作为高等院校计算机、通信、信息安全等专业的教材，也可作为网络工程技术人员、网络管理人员、信息安全管理人员的技术参考书。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 免费注册，审核通过后即可下载，或联系编辑索取（QQ：241151483，电话：010-88379753）。

图书在版编目（CIP）数据

网络安全技术及应用/刘京菊等编著. —北京：机械工业出版社，2012.6
普通高等教育计算机规划教材
ISBN 978-7-111-38654-4

Ⅰ. ①网… Ⅱ. ①刘… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 117883 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：郝建伟 曹文胜
责任印制：乔 宇
三河市宏达印刷有限公司印刷

2012 年 8 月第 1 版 · 第 1 次印刷
184mm × 260mm · 15.5 印张 · 381 千字
0001－3000 册
标准书号：ISBN 978-7-111-38654-4
定价：33.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社 服 务 中 心：(010)88361066
销 售 一 部：(010)68326294
销 售 二 部：(010)88379649
读者购书热线：(010)88379203

网络服务
门户网：http://www. cmpbook. com
教材网：http://www. cmpedu. com

封面无防伪标均为盗版

出 版 说 明

信息技术是当今世界发展最快、渗透性最强、应用最广的关键技术，是推动经济增长和知识传播的重要引擎。在我国，随着国家信息化发展战略的贯彻实施，信息化建设已进入了全方位、多层次推进应用的新阶段。现在，掌握计算机技术已成为21世纪人才应具备的基础素质之一。

为了进一步推动计算机技术的发展，满足计算机学科教育的需求，机械工业出版社聘请了全国多所高等院校的一线教师，进行了充分的调研和讨论，针对计算机相关课程的特点，总结教学中的实践经验，组织出版了这套“普通高等教育计算机规划教材”。

本套教材具有以下特点：

1）反映计算机技术领域的新发展和新应用。

2）为了体现建设“立体化”精品教材的宗旨，本套教材为主干课程配备了电子教案、学习与上机指导、习题解答、多媒体光盘、课程设计和毕业设计指导等内容。

3）针对多数学生的学习特点，采用通俗易懂的方法讲解知识，逻辑性强、层次分明、叙述准确而精炼、图文并茂，使学生可以快速掌握，学以致用。

4）符合高等院校各专业人才的培养目标及课程体系的设置，注重培养学生的应用能力，强调知识、能力与素质的综合训练。

5）注重教材的实用性、通用性，适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班和自学用书。

希望计算机教育界的专家和老师能提出宝贵的意见和建议。衷心感谢计算机教育工作者和广大读者的支持与帮助！

机械工业出版社

前　言

随着计算机网络的广泛应用，网络安全问题日益引起人们的关注。保证个人、企业、国家机密信息的安全性和计算机网络系统的安全性是网络系统规划、建设和应用必须考虑的重要问题。然而，计算机网络安全问题错综复杂，涉及面非常广，有技术因素，又有管理因素；有自然因素，也有人为因素；有外部的安全威胁，还有内部的安全隐患。

本书紧密结合计算机网络安全技术的最新发展，从理论和应用两个层次，系统地介绍了计算机网络安全的基础理论、技术原理和应用方法，使读者对计算机网络安全及应用有一个系统、全面的了解。全书共10章。第1章主要介绍了计算机网络安全的相关概念和体系结构。第2章主要介绍了计算机网络的实体安全技术，包括环境安全、设备安全和媒体安全等。第3章主要介绍了数据加密与认证技术，包括数据加密技术的基本概念、常用数据加密算法的技术原理、数据加密技术的典型应用，以及认证技术的原理与应用。第4章主要介绍了防火墙技术，包括防火墙体系结构与技术原理，防火墙的应用部署和个人防火墙功能特点与应用。第5章主要介绍了入侵检测技术，包括入侵检测的原理、功能和方法，典型入侵检测系统Snort的体系结构与应用部署，以及入侵防护系统的基本概念与应用部署。第6章主要介绍了系统安全技术，包括操作系统安全的原理与措施、数据库安全技术原理与安全配置方法。第7章主要介绍了网络应用安全技术，包括VPN的原理与应用，TCP/IP和HTTP、FTP等典型网络应用协议的安全问题，Web、FTP、电子邮件等典型网络应用服务的安全问题与安全措施。第8章主要介绍了恶意代码防范技术，包括恶意代码的概念、分类和关键技术，恶意代码的检测技术，恶意代码的防范策略，以及典型的恶意代码检测与清除工具的功能与用法。第9章主要介绍了网络安全检测与分析技术，包括网络安全检测的目的与分类，网络漏洞检测技术、系统配置检测技术和系统状态检测技术。第10章主要介绍了数据备份与恢复技术，包括数据备份与恢复的基本概念，常用数据备份方案的原理，数据备份与恢复策略，以及常用数据备份方法的原理与应用。本书涉及的内容十分广泛，在教学时，可根据实际情况进行选择。

本书由刘京菊编写第2、3、7、9章，王永杰编写第5、6、8章，梁亚声编写第1、10章，汪永益编写第4章。全书由刘京菊统稿。

由于作者水平有限，书中难免存在不妥之处，敬请读者批评指正。

编　者

本科精品教材推荐

计算机网络应用教程 第3版

书号：978-7-111-08257-5　　定价：32.00元

作者：王洪　　配套资源：电子教案

推荐简言：

★ 北京市高等教育精品教材。

★ 本书以通俗易懂、循序渐进的方式叙述网络知识，结合作者的实际工作经验，全面、系统的阐述了计算机网络涉及的基本概念、原理，并通过具体实例讲解，将理论知识应用于实践，使读者学以致用，注重培养应用能力，强调知识、能力与素质的综合训练。

★ 教材中案例均采用现流行技术，使读者所学与市场接轨。

★ 每章附有大量的练习题，可供教学选用。

计算机网络——原理、技术与应用

书号：978-7-111-30641-2　　定价：39.00元

作者：王相林　　配套资源：电子教案

推荐简言：

★ 本书采用“自顶向下方法”，从应用层开始，介绍计算机网络五层体系结构，符合人们从应用开始接受、学习知识的习惯。

★ 在讲述网络知识内容的过程中提出问题，请读者试着分析解决引伸出的问题，同时指明相关知识应用时需要注意的地方，使对计算机网络知识的教与学达到“学思结合、知行统一、融会贯通”。

★ 写作力求反映最新的计算机网络理论、技术和应用知识。

★ 本书结构脉络清晰，知识讲授循序渐进，力求反映最新的计算

计算机网络安全教程

书号：978-7-111-24502-5　　定价：34.00元

作者：梁亚声　　配套资源：电子教案

推荐简言：

★ 本书重点分析了计算机网络存在的安全威胁，系统介绍了计算机网络安全的体系结构、基础理论、技术原理和实现方法。从理论和实际应用角度，对计算机网络的物理、链路、网络、应用等各层的安全技术进行了分析和介绍。

★ 本书提供了典型案例，每章都配备相应的习题，并提供完整的配套电子教案（可在机械工业出版社教材服务网下载）。

TCP/IP协议分析及应用

书号：978-7-111-20898-3　　定价：29.00元

作者：杨延双　　配套资源：电子教案

推荐简言：

★ 北京市高等教育精品教材。

★ 本书的结构、形式、内容是基于满足教学需要（本课程学时一般为40学时左右）和读者实际需求，涵盖需读者掌握的网络协议概念、TCP/IP的主要协议的原理和功能分析及应用的知识。

★ 注意限制全书的篇幅，内容详略得当且突出重点，按教与学的普遍规律安排教材的总体结构和章节，既便于教师备课、安排学时，又利于读者学习。

物联网技术概论

书号：978-7-111-33323-4　　定价：36.00元

作者：马建　　配套资源：电子教案

推荐简言：

★ 国内第一本涉及中国物联网标准制定的图书。

★ 写作大纲由国内近20家与物联网相关的企业、科研机构和知名高校共同讨论完成。

★ 本书概述了物联网的起源，辨析了物联网的概念与内涵；展示了物联网发展的现状以及战略意义，并介绍了物联网的典型应用；阐释了物联网体系架构，归纳了构建物联网发展的技术领域；指出了为实现物联网产业化和大规模商业应用必须面临的挑战。

无线移动互联网：原理、技术与应用

书号：978-7-111-36023-0　　定价：52.00元

作者：崔勇　　配套资源：电子教案

推荐简言：

★ 本书各个章节相对独立，各个章节的内容新旧结合，难易结合，错落有致。

★ 本书不仅仅介绍了学术界的最新论文和资料，还介绍了产业界的最新技术发明和产品，从学术成果和产业发明两个方面向读者全面展示最新研究进展。

★ 本书全面介绍了无线移动互联网各类技术的应用，力图让学习者学以致用，使得今后的学习、研究和工作更加得心应手。

目　录

第1章 概 论

随着计算机技术的迅速发展，计算机上处理的业务由基于单机的数学运算、文件处理，基于简单连接的内部网络的业务处理、办公自动化，发展到基于企业内部网（Intranet）、企业外部网（Extranet）、国际互联网（Internet）的世界范围内的信息共享和业务处理。计算机网络（简称网络）的应用领域已从传统的小型业务系统逐渐向大型关键业务系统扩展。随着政府上网、企业上网、教育上网、家庭上网……，互联网在经济、军事、文教等诸多领域得到了广泛应用。

计算机网络在为人们提供便利、带来效益的同时，也使人类面临着信息安全的巨大挑战。计算机网络存储、传输和处理着政府宏观调控决策、商业经济、银行资金转账、股票证券、能源资源、国防和科研等大量关系国计民生的重要信息，许多重要信息直接关系到国家的安全。如何保护个人、企业、国家的机密信息不受黑客和间谍的入侵，如何保证网络安全不间断地工作，是国家和单位信息化建设必须考虑的重要问题。据统计，近年来，我国每年因网络安全造成的损失高达上百亿美元。

有关计算机的安全技术研究始于20世纪60年代。当时，计算机系统的脆弱性已逐渐为美国政府和一些私营机构所认识。但是，由于当时计算机的速度和性能还比较落后，使用的范围也不广，再加上美国政府把它当做敏感问题而施加控制。因此，有关计算机安全的研究一直局限在比较小的范围内。

进入20世纪80年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机几乎遍及世界各个角落，并且人们利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。随之而来的计算机网络的安全问题就日益严峻，成为信息技术中最重要的问题之一。

1.1 计算机网络面临的主要威胁

计算机网络是颇具诱惑力的受攻击目标，无论是个人、企业，还是政府机构，只要使用计算机网络，都会感受到网络安全问题所带来的威胁；无论是局域网还是广域网，都存在着自然和人为等诸多脆弱性和潜在威胁。

1.1.1 计算机网络实体面临威胁

实体是指网络中的关键设备，包括各类计算机（服务器、工作站等）、网络通信设备（路由器、交换机、集线器、调制解调器、加密机等）、存放数据的媒介（磁带机、磁盘机、光盘等）、传输线路、供配电系统以及防雷系统和抗电磁干扰系统等。这些设备不管哪一个环节出现问题，都会影响网络的正常运行，甚至给整个网络带来灾难性的后果。

1.1.2 计算机网络系统面临威胁

1986～1989年，原西德黑客组织——“汉诺威集团”，试图进入美国军事计算机网络刺

探机密，这一事件于1989年3月2日在德国电视上曝光后，引起媒体的连锁反应。1990年1月15日又发生了AT&T“一·一五”大瘫痪事件。这些事件使美国意识到黑客对计算机网络系统的严重威胁，1990年在全国范围内掀起了一场“扫黑大行动”。

网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公网传送的信息可能被他人窃听或篡改等。表1-1所列为典型的网络安全威胁。

表1-1　典型的网络安全威胁

威　胁	描　述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息以后，将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除、插入，再发送给接收者
非授权访问	通过假冒、身份攻击、系统漏洞等手段，获取系统访问权，从而使非法用户进入网络系统读取、删除、修改、插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
人员疏忽	授权的人为了利益或由于粗心将信息泄露给未授权人

1.1.3　恶意程序的威胁

以计算机病毒、网络蠕虫、间谍软件、木马程序等为代表的恶意程序时刻都在威胁着计算机网络系统的安全。

1988年11月发生了互联网络蠕虫（Worm）事件，也称莫里斯蠕虫案。22岁的罗伯特·泰潘·莫里斯是美国康奈尔大学计算机系研究生，其父鲍勃·莫里斯是美国安全局的首席安全专家。罗伯特从小喜爱计算机，非常熟悉UNIX系统。在恶作剧心态的操纵下，罗伯特利用UNIX系统中Sendmail、Finger、FTP的安全漏洞，编写了一个蠕虫病毒程序。11月2日晚，罗伯特将病毒程序安放在与ARPANET（国际互联网的前身）联网的麻省理工学院的网络上。由于病毒程序中一个参数设置错误，该病毒迅速在与ARPANET联网的几乎所有计算机中扩散，并被疯狂复制，大量侵蚀计算机资源，使得美国成千上万台计算机一夜之间陷入瘫痪。

1999年4月26日，CIH病毒爆发，俄罗斯10多万台电脑瘫痪，韩国24万多台电脑受影响，马来西亚12个股票交易所受侵害。

计算机病毒可以严重破坏程序和数据，使网络的效率和作用大大降低，许多功能无法正常使用，甚至导致计算机系统的瘫痪。目前，全球已发现6万余种计算机病毒，并且还在以每天10余种的速度增长。据统计，计算机病毒所造成的损失，占网络经济损失的76%，仅“爱虫”发作在全球所造成的损失就达96亿美元。虽然至今尚未出现灾难性的后果，但各种各样的计算机病毒层出不穷，并活跃在世界的各个角落。

1.1.4 计算机网络不安全原因

计算机网络系统安全的脆弱性是伴随计算机网络一同产生的。换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。要使网络方便快捷，又要保证网络安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围中寻找平衡点。因此，可以说任何一个计算机网络都不是绝对安全的。

1. 互联网具有不安全性

最初，互联网用于科研和学术目的，它的技术基础存在不安全性。互联网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性，这就对安全提出了更高的要求，主要表现在以下三个方面。

1）开放性的网络。网络技术是全开放的，使得网络所面临的破坏和攻击来自多方面。可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件实施的攻击。

2）国际性的网络。网络的攻击不仅仅来自本地网络的用户，而且可能来自互联网上的任何一台机器，也就是说，网络安全面临的是一个国际化的挑战。

3）自由性的网络。网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。

另外，互联网使用的 TCP/IP（传输控制协议/网际协议）、FTP（文件传输协议）、E-mail（电子邮件）、RPC（远程程序通信规则）、NFS（网络文件系统）等都包含许多不安全的因素，存在着许多安全漏洞。

2. 操作系统存在安全问题

操作系统软件自身的不安全性以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给危害网络安全的人留下了许多“后门”。

操作系统的体系结构造成的不安全性是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，例如，I/O 的驱动程序和系统服务可以通过打“补丁”的方式进行动态连接，许多 UNIX 操作系统的版本升级、开发都是采用打补丁的方式进行的。这种动态连接的方法容易被黑客所利用，而且还是计算机病毒产生的好环境。另外，操作系统的一些功能也带来不安全因素。例如，支持在网络上传输可以执行的文件映像和网络加载程序的功能等。

操作系统不安全的另一个原因在于它可以创建进程，支持进程的远程创建与激活，支持被创建的进程继承创建进程的权利，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序都监测不到它的存在。

操作系统的无口令入口以及隐蔽通道（原是为系统开发人员提供的便捷入口），都可能成为黑客入侵的通道。

3. 数据的安全问题

在网络中，数据存放在数据库中，通常供不同的用户共享。然而，数据库存在着许多不安全性。例如，授权用户超出了访问权限进行数据的更改活动；非法用户绕过安全内核，窃

取信息资源等。对于数据库的安全而言，就是要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性和并发控制。数据的安全性就是防止数据库被故意破坏和非法存取；数据的完整性是防止数据库中存在不符合语义的数据以及防止由于错误信息的输入、输出而造成无效操作和错误结果；并发控制就是在多个用户程序并行地存取数据库时，保证数据库的一致性。

4. 传输线路安全问题

尽管在光缆、同轴电缆、微波、卫星通信中窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。

5. 网络安全管理问题

网络系统缺少安全管理人员，缺少安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控，是网络最大的安全问题之一。

1.2 计算机网络安全的概念

计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

1.2.1 计算机网络安全的定义

计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性及可使用性受到保护。要做到这一点，必须保证网络系统软件、应用软件、数据库系统具有一定的安全保护功能，并保证网络部件（如终端、调制解调器、数据链路等）的功能仅仅是被授权的人员才可以访问。网络的安全问题实际上包括，网络的系统安全和网络的信息安全两方面的内容，而保护网络的信息安全是最终目的。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、不可否认性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。从用户（个人、企业等）的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和不可否认性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯，即用户的利益和隐私不被非法窃取和破坏。从网络运行和管理者的角度说，希望对网络的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御黑客的攻击。对安全保密部门来说，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，避免给国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

1.2.2 计算机网络安全的目标

从计算机网络安全定义中可以看出，计算机网络安全应达到以下目标。

1. 保密性

保密性是指网络中的保密信息只能供经过允许的人员，以经过允许的方式使用，信息不

泄露给非授权用户、实体或过程，或供其利用。从技术上说，任何传输线路，包括电缆（双绞线或同轴电缆）、光缆、微波和卫星，都是可能被窃听的。

提供保密性安全服务取决的若干因素如下。

1）需保护数据的位置：数据可能存放于个人机器（如硬盘或服务器）中、局域网的线路上或其他流通机制（如软盘）上，也可能流经一个完全公开的媒体（如穿过互联网或通信卫星）。

2）需保护数据的类型：数据元素可以是本地文件（如口令或密钥）、网络协议所携带的数据、网络协议的信息交换（如一个协议数据单元）。

3）需保护数据的数量或部分：保护整个数据元素、部分数据单元，还是协议数据单元。

4）需保护数据的价值：被保护数据的敏感性，以及数据对用户的价值。

保密性的要素如下。

1）数据保护：防止信息内容的泄露（如网络中的数据流）。

2）数据隔离：提供隔离路径或采用过程隔离（COMPUSEC 技术等）。

3）通信流保护：数据的特征包括频率、数量、通信流的目的地等。通信流保护是指对通信的特征信息以及推断信息（如命令结构等）进行保护。

2. 完整性

完整性是指网络中的信息安全、精确与有效，不因种种不安全因素而改变信息原有的内容、形式与流向。确保信息在存储或传输过程中不被修改、不被破坏和丢失。

破坏信息的完整性既有人为因素，也有非人为因素。非人为因素是指通信传输中的干扰噪声，系统硬件或软件的差错等。人为因素包括有意和无意两种，前者是非法分子对计算机的侵入、合法用户越权对数据进行处理以及隐藏破坏性程序（计算机病毒、时间炸弹、逻辑陷阱）等；无意危害是指操作失误或使用不当。完整性被破坏是计算机网络安全的主要威胁。另外，信息完整性是一个很广泛的问题，例如分布式数据库中并发性操作或者对多个数据副本的更新所引起的数据一致性问题，由于系统的设计不完善造成使用不当或操作失误所引起的数据完整性问题等。

提供完整性服务的要求与保密性服务的要求相似，包括需要保护的数据的位置、类型、数量及内容。

3. 可用性

可用性指网络资源在需要时即可使用，不因系统故障或误操作等使资源丢失或妨碍对资源的使用，是被授权实体按需求访问的特性。在网络环境下，拒绝服务、破坏网络和系统的正常运行等都属于对可用性的攻击。

网络可用性还包括在某些不正常条件下继续运行的能力。对网络可用性的破坏包括合法用户不能正常访问网络资源和有严格时间要求的服务不能得到及时响应。影响网络可用性的因素包括人为与非人为两种。前者是指非法占用网络资源，切断或阻塞网络通信，降低网络性能，甚至使网络瘫痪等；后者是指灾害事故（火、水、雷击等）和系统死锁、系统故障等。

保证可用性的最有效的方法是提供一个具有普适安全服务的安全网络环境。通过使用访问控制阻止未授权资源访问，利用完整性和保密性服务来防止可用性攻击。访问控制、完整性和保密性成为协助支持可用性安全服务的机制。

1）避免受到攻击：一些基于网络的攻击旨在破坏、降级或摧毁网络资源。解决办法是加强这些资源的安全防护，使其不受攻击。免受攻击的方法包括：关闭操作系统和网络配置中的安全漏洞；控制授权实体对资源的访问；防止路由表等敏感网络数据的泄露。

2）避免未授权使用：当资源被使用、占用、过载时，其可用性就会受到限制。如果未授权用户占用了有限的资源（如处理能力、网络带宽、调制解调器连接等），则这些资源对授权用户就是不可用的，通过访问控制可以限制未授权使用。

3）防止进程失败：操作失误和设备故障也会导致系统的可用性降低。解决方法是使用高可靠性设备，提供设备冗余和提供多路径的网络连接等。

4. 不可否认性

“否认”指参与通信的实体拒绝承认它参加了那次通信，不可否认是保证信息行为人不能否认其信息行为。不可否认性安全服务提供了向第三方证明该实体确实参与了通信的能力。

1）数据的接收者提供数据发送者身份及原始发送时间的证据。

2）数据的发送者提供数据已交付接收者（某些情况下，包括接收时间）的证据。

3）审计服务提供了信息交换中各涉及方的可审计性，这种可审计性记录了可用来跟踪某些人的相关事件，这些人应对其行为负责。

不可否认性服务主要由应用层提供。通常用户最关心的是应用程序数据（如电子邮件和文件）的不可否认性。在网络层之下提供不可否认性功能，仅能证明产生过的连接，而无法将流经该连接的数据同特定的实体相绑定。

5. 可控性

可控性是指对信息的传播及内容具有控制能力，保证信息和信息系统的授权认证和监控管理，确保某个实体（人或系统）身份的真实性，也可以确保执法者对社会的执法管理行为。

1.2.3 计算机网络安全的层次

根据网络安全措施作用位置的不同，可以将网络安全划分为4个层次，分别为：物理安全、逻辑安全、操作系统安全和联网安全。

1. 物理安全

物理安全主要包括防盗、防火、防静电、防雷击、防电磁泄漏和物理隔离等方面。关于物理安全的具体内容将在第2章中详细介绍。

2. 逻辑安全

计算机系统的逻辑安全主要通过口令密码、权限控制等方法来实现。例如，可以限制连续登录的次数或限制连续登录的时间间隔；可以用加密软件保护存储在计算机系统中的信息；通过身份验证技术限制对存储于计算机系统中的文件的访问。此外，可以通过一些安全软件跟踪可疑、未授权的访问企图。

3. 操作系统安全

操作系统是计算机中最基本、最重要的软件，是计算机系统安全的基础。操作系统安全主要包括用户权限控制、安全漏洞修复等内容。

4. 联网安全

联网安全主要通过以下安全措施来实现。

1）访问控制：用来保护计算机和网络资源不被非授权使用。

2）通信安全：用来保证数据的保密性和完整性以及各通信方的可信赖性。

1.2.4 计算机网络安全的原则

现代信息系统都是以网络支撑，相互连接的。要使信息系统免受攻击，关键要建立起安全防御体系，从信息的保密性（保证信息不泄露给未经授权的人）拓展到信息的完整性（防止信息被未经授权的用户篡改，保证真实的信息从真实的信源无失真地到达真实的信宿）、信息的可用性（保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝服务，或为敌手可用）、信息的可控性（对信息及信息系统实施安全监控管理）、信息的不可否认性（保证信息行为人不能否认自己的行为）等。在进行计算机网络安全设计、规划时，应遵循以下原则。

（1）需求、风险、代价平衡分析的原则

对任意网络来说，绝对安全难以达到，也不一定必要。对一个具体网络要进行实际分析，对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。保护成本及被保护信息的价值必须平衡，价值仅 1 万元的信息，如果用 5 万元的技术和设备去保护是一种不适当的保护。

（2）综合性、整体性原则

运用系统工程的观点和方法，分析网络的安全问题，并制定具体措施。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络包括人、设备、软件、数据等环节。其在网络安全中的地位和影响，只有从系统综合的整体角度去看待和分析，才可能获得有效、可行的措施。

（3）一致性原则

这主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络的安全需求相一致。实际上，在网络建设之初就考虑网络安全对策比等网络建设好后再考虑要容易，而且花费也少得多。

（4）易操作性原则

安全措施要由人来完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。此外，采用的措施不能影响系统的正常运行。

（5）适应性、灵活性原则

安全措施必须能随着网络性能及安全需求的变化而变化，要容易适应、容易修改。

（6）多重保护原则

任何安全保护措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他保护层仍可保护信息的安全。为此需要构建全方位的安全体系。全方位安全体系的主要包括以下内容。

1）访问控制：通过对特定网段、服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。

2）检查安全漏洞：通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝

大多数攻击无效。

3）攻击监控：通过对特定网段、服务建立的攻击监控体系，可实时检测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）。

4）加密通信：主动的加密通信，可使攻击者不能了解、修改敏感信息。

5）认证：良好的认证体系可防止攻击者假冒合法用户。

6）备份和恢复：良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。

1.2.5 计算机网络安全所涉及的内容

网络安全所研究的主要内容包括以下方面。

1）网络安全体系结构。

2）网络的攻击手段与防范措施。

3）网络安全设计。

4）网络安全标准，安全评测及认证。

5）网络安全检测技术。

6）网络安全设备。

7）网络安全管理，安全审计。

8）网络犯罪侦查。

9）网络安全理论与政策。

10）网络安全教育。

11）网络安全法律。

概括起来，网络安全包括以下三个重要部分。

1）先进的技术：先进的安全技术是网络安全的根本保障，用户通过风险评估，决定所需的安全服务种类，选择相应的安全机制，集成先进的安全技术。

2）严格的管理：使用网络的机构、企业和单位建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

3）威严的法律：安全的基石是社会法律、法规与手段，通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

1.3 计算机网络安全体系结构

研究计算机网络安全的体系结构，就是研究如何从管理和技术上保证网络的安全得以完整准确地实现，网络安全需求得以全面准确的满足。

1.3.1 网络安全模型

网络安全的基本模型如图 1-1 所示。通信双方在网络上传输信息时，首先需要在收、发方之间建立一条逻辑通道。为此，就要先确定从发送方到接收方的路由，并选择该路由上使用的通信协议，如 TCP/IP 等。