21世纪高等院校精品规划教材

刘华春　蒋志平　编　著

计算机网络安全技术教程

中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校精品规划教材

计算机网络安全技术教程

刘华春　蒋志平　编　著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书系统地介绍了计算机网络的安全体系，将安全理论，攻、防技术，安全程序设计，网络安全工具等有机地结合起来。全书从网络安全体系上共分为 4 个部分 10 章。第 1 部分是计算机网络安全技术基础，介绍计算机网络安全的基本概念和网络安全程序设计的内容。第 2 部分是信息加密技术，介绍密码学和信息加密原理，并对 DES、RSA 加密技术，散列函数，数字签名与数字证书进行全面的介绍。第 3 部分是网络安全技术，主要介绍网络入侵与攻击技术（网络漏洞与攻击、IP 欺骗、木马攻击、网络后门等攻击与入侵技术）、防火墙与入侵检测系统、身份认证与访问控制、IP 安全与 VPN 技术。第 4 部分是系统安全，介绍操作系统的安全、系统安全策略、病毒的分析与防范等内容。

本书可作为普通高等院校（尤其是应用型本科院校）、高等职业技术学院电子信息相关专业的网络安全课程教材，也可供各个企事业单位的网络管理维护人员和计算机工程技术人员作为自学参考书。本教程提供完整的教学 PPT 课件、教程中所有工具软件和源码及虚拟机演示软件，读者可以在中国水利水电出版社网站（http://www.waterpub.com.cn/softdown/）自行下载。

图书在版编目（CIP）数据

计算机网络安全技术教程 / 刘华春，蒋志平编著
. -- 北京 : 中国水利水电出版社，2010.4
21世纪高等院校精品规划教材
ISBN 978-7-5084-7301-7

Ⅰ. ①计… Ⅱ. ①刘… ②蒋… 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(2010)第039575号

书　　名	21 世纪高等院校精品规划教材 **计算机网络安全技术教程**
作　　者	刘华春　蒋志平　编　著
出 版 发 行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：sales@waterpub.com.cn 电话：68367658（营销中心）
经　　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643 全国各地新华书店和相关出版物销售网点
排　　版	北京英宇世纪信息技术有限责任公司
印　　刷	北京市兴怀印刷厂
规　　格	184mm×260mm　16 开本　19.25 印张　480 千字
版　　次	2010 年 4 月第 1 版　2010 年 4 月第 1 次印刷
印　　数	0001—3000 册
定　　价	32.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

前　言

随着政府上网、企业上网、教育上网及家庭上网的普及，计算机网络在经济、军事及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。如何保护个人、企业和国家的机密信息不被黑客和间谍入侵，如何保证网络系统安全、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。因此，使计算机网络系统免遭破坏，提高系统的安全可靠性，已成为人们关注和亟须解决的问题。每个单位的网络管理与维护人员、网络系统用户和工程技术人员都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全稳定地运行并提供正常而安全的服务。

本教程全面介绍了网络安全基础理论和网络安全应用技术，以面向应用为主线，以解决实际网络安全问题为内容进行内容组织。全书分为 4 大部分，第 1 部分（1、2 章）为计算机网络安全技术基础，主要介绍了网络安全技术的基础理论和网络安全程序设计的常用方法。第 2 部分（3 章）为信息加密技术，这部分对网络安全核心的基础设施——信息加密技术进行了的讲解，读者学习后面章节才能达到 “知其然，还能知其所以然”的目的。第 3 部分（4～7 章）为网络安全，主要面向实际的计算机网络安全应用，对各种网络安全中的应用问题进行专门的分析和讲解。第 4 部分（8～10 章）为系统安全，主要介绍操作系统的安全、病毒防范和数据安全。

在编者多年的网络安全课程的教学中，使用了多本网络安全的教材和参考书，发现目前市面上的网络安全书籍主要有两类：一类是纯粹面向高校教学的，多见于一些重点本科高校使用的教材，这部分教材的特点就是理论翔实，适合于深入学习和研究网络安全使用。而另一类，则是完全面向市场的网络安全技术的纯粹应用性书籍，这些书籍以介绍网络安全攻防工具的使用为主，以培养网络安全方面的速成人才为目标。其实，网络安全作为一门有一定技术难度又与现实应用结合紧密的学科，只有在理论基础与实际应用这两者之间找到最佳结合点，才能让学生真正学好这门课程，这就是我们编写本教材的目的。总体来讲，本教程的特点可以归纳为如下几点。

1. 扎实理论 面向应用

以实际应用为导向介绍相应的理论基础，而不是所有理论都进行详细介绍，使读者“知其然，并知其所以然”。

2. 图文并茂 讲解通俗

为便于读者理解和加深印象，本教程每章都附有大量的操作图示，并以通俗易懂的语言进行专业讲解。

3. 经典案例 源码分析

教程选用了主流而经典的网络安全工具进行讲解和演示，对每一种不同的网络安全工具类

型都举1～2个例子，同时对一些重要的工具与技术，还通过分析其详细的实现源代码，达到深入理解和灵活使用的目的。

4．与时俱进 推陈纳新

这是本教程的一大特色，教程中所介绍的网络安全技术和工具，绝大部分都是本教程出版之前正在使用的主流工具和技术，对网络安全与病毒技术的分析，都采用了截至2009年的最新数据。

5．循序渐进 教学相宜

作为一本教程类书籍，结合编者多年来的教学经验，合理安排组织教学章节和进度，既有利于课堂教学的组织，又非常适合学生的自学。

本教程建议教学学时数为50～60学时，根据学时数目的多少可以对教材的4部分内容进行有选择性的学习。

本教程由刘华春、蒋志平共同编著，其中，第1章及第3～7章由刘华春执笔，第2章及第8～10章由蒋志平执笔，参与本教程编写工作的人员还有戴庆光、袁连海、段华琼、王建华、惠宏伟、杜华、徐显荣，全书由所有编委人员共同完成统稿与校对。本书的编写参考了国内外同行的一些研究成果与资料，尤其是来自于互联网的一些资料的作者，无法以明确的身份列入参考文献，在这里一并表示真诚的感谢！

虽然编者对本教程花费了大量的精力进行推敲和校对，但由于编者自身水平和时间的原因，教程肯定仍然存在着许多不尽如人意的地方，真诚地希望各位读者给予批评和指正。意见可以直接发邮件到szljhljh@163.com，谢谢！

编　者

2009年12月

目　录

第 1 部分　计算机网络安全技术基础

第 2 部分　信息加密技术

第 3 部分　网络安全技术

第 4 部分 系统安全

第 1 部分　计算机网络安全技术基础

第 1 章　网络安全概述

本章学习要点：

- 网络安全的基本内容、网络面临的主要威胁
- 网络安全的基本技术与策略
- 常用的网络协议、网络服务、网络命令
- 实验环境的配置

1.1　网络安全介绍

随着计算机网络的迅速发展，特别是 Internet 在全球的普及，计算机网络的安全问题已经引起人们的极大关注。由于计算机网络的安全直接影响到政治、军事、经济及日常生活中的各个领域，因此如何有效地保证网络安全，已经成为计算机研究与应用中一个重要的课题。

1.1.1　网络安全的定义

什么是网络安全呢？国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此可以这样理解计算机网络的安全：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

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、信息论等多门学科的综合性学科。从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

从广义上说，网络安全包括网络硬件资源及信息资源的安全性。硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等。要实现信息快速、安全的交换，一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性、真实性等是网络安全研究的重要课题，也是本书涉及的重点内容。

网络安全的具体含义会随着“角度”的变化而变化。例如，从用户（个人、企业等）的角度来说，他们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、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改和抵赖等手段侵犯其利益和隐私。从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作进行保护和控制，

避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、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，对国家造成巨大损失。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。

可见网络安全的内容是十分广泛的，不同的人群对其有不同的理解。在此对网络安全下一个通用的定义：信息的传输安全是指信息在动态传输过程中的安全。威胁信息传输安全的因素主要有：对传输信息的监听、篡改、否认、重发以及对用户身份的仿冒等。

1.1.2 网络安全的主要内容

网络安全包括网络系统的部件、软件、数据的安全，它通过网络信息的存储、传输和使用过程来体现。网络安全的目的是保护网络设备、软件、数据，使其免受非授权使用或访问。网络安全主要包括以下两方面的内容。

1. 网络设备安全

包括设备上运行的网络软件的安全，确保能够正常地提供网络服务。

2. 网络数据安全

在网络中存储和传输的信息的安全，即网络系统的信息安全。确保网络系统的信息安全是网络安全的重要目标。

对网络系统而言，信息安全主要包括两个方面的内容：信息的存储安全和信息的传输安全。信息的存储安全是指信息在网络节点上静态存放状态下的安全性。威胁信息存储安全的因素主要是网络内部或外部对信息的非法访问。因而，各种访问控制技术，如设置访问权限、身份识别和局部隔离等，是解决信息存储安全的主要途径。信息的传输安全是指信息在动态传输过程中的安全。威胁信息传输安全的因素主要有：对传输信息的监听、篡改、否认、重发以及对用户身份的仿冒等。

1.1.3 网络安全的目标

在美国国家信息基础设施（NII）的文献中，给出了安全的 5 个属性：可用性、机密性、完整性、可靠性和不可抵赖性。这 5 个属性适用于国家信息基础设施的各个领域，例如教育、娱乐、医疗、运输、国家安全、通信等。

1. 可用性

可用性是指得到授权的实体在需要时可以得到所需要的网络资源和服务。由于网络最基本的功能就是为用户提供信息和通信服务，而用户对信息和通信的需求是随机的（内容的随机性和时间的随机性）、多方面的（文字、语音、图像等），有的用户还对服务的实时性有较高的要求。网络必须能够保证所有用户的通信需要，一个授权用户无论何时提出要求，网络必须是可用的，不能拒绝用户的要求。攻击者常会采用一些手段来占用或破坏系统的资源，以阻止合法用户使用网络资源，这就是对网络可用性的攻击。对于针对网络可用性的攻击，一方面要采取物理加固技术，保障物理设备安全、可靠地工作；另一方面通过访问控制机制，阻止非法访问进入网络。

2. 机密性

机密性是指网络中的信息不被非授权实体（包括用户和进程等）获取与使用。这些信息不仅指国家机密，也包括企业和社会团体的商业秘密和工作秘密，还包括个人的秘密（如银行账号）和个人隐私（如邮件、浏览习惯）等。随着网络在人们生活中的广泛使用，使人们对网

络机密性的要求提高。用于保障网络机密性的主要技术是密码技术。在网络的不同层次上有不同的机制来保障机密性。在物理层上，主要是采取电磁屏蔽技术、干扰及跳频技术来防止电磁辐射造成的信息外泄；在网络层、传输层及应用层主要采用加密、路由控制、访问控制、审计等方法来保证信息的机密性。

3. 完整性

完整性是指网络信息的真实可信性，即网络中的信息不会被偶然或者蓄意地删除、修改、伪造、插入等破坏，保证授权用户得到的信息是真实的。只有具有修改权限的实体才能修改信息，如果信息被未经授权的实体修改了或在传输过程中出现了错误，信息的使用者应能够通过一定的方式判断出信息是否真实可靠。

4. 可靠性

可靠性是指系统在规定的条件下和规定的时间内，完成规定功能的概率。可靠性是网络安全最基本的要求之一。目前对于网络可靠性的研究主要偏重于硬件可靠性的研究，主要采用硬件冗余、提高研究质量和精确度等方法。实际上，软件的可靠性、人员的可靠性和环境的可靠性在保证系统可靠性方面也是非常重要的。

5. 不可抵赖性

不可抵赖性也称为不可否认性，是指通信双方在通信过程中，对于自己所发送或接收的消息不可抵赖，即发送者不能抵赖他发送过消息的事实和消息的内容，而接收者也不能抵赖其接收到消息的事实和内容。

1.1.4　网络安全问题的重要性

随着国内外计算机技术和通信技术及应用的飞速发展，目前传统电信网正向信息网迅速发展，人类进入了一个崭新的信息时代。在信息化社会中，计算机通信网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施建设已经成为反映信息社会特征最重要的基础设施建设。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和“财富”高度集中于计算机中。但是这些信息系统都是依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。随着网络的开放性、共享性、互连程度扩大，特别是 Internet 的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，比如电子商务（Electronic Commerce）、电子现金（Electronic Cash）、数字货币（Digital Cash）、网络银行（Network Bank）等，以及各种专用网的建设，比如金融网等，使得安全问题显得越来越重要，成了关键之所在。因此网络安全成了数据通信领域研究和发展的一个重要方向，对网络安全技术的研究成了现在计算机和通信界的一个热点，并且成为信息科学的一个重要研究领域，正日益受到人们的关注。

广义上的网络安全还应该包括如何保护内部网络的信息不被轻易泄露，如何抵御文化侵略，如何防止不良信息的泛滥等。例如英国实施的“安全网络 R-3”计划，其目的就是打击网络上的犯罪行为，防止 Internet 上不健康内容的泛滥。我们国家颁布了《计算机网络国际互联网安全保护管理办法》，主要用来制止网络污染，阻止危害国家安全，泄露国家机密，侵犯国家、社会、集体的利益和公民的合法权益的行为发生。

计算机的安全是一个越来越引起世界各国关注的重要问题，也是一个十分复杂的课题。随着计算机在人类生活各领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络被

不断非法入侵，重要资料被窃密，甚至由此造成网络系统的瘫痪，已给各个国家以及众多公司造成巨大的经济损失，甚至危害到国家和地区的安全。因此计算机系统的安全问题成为一个关系到人类生活与生存的大事情，必须给予极大高度的重视。

1.2 计算机网络面临的威胁

随着 Internet 的发展，网络安全越来越受到很多方面的威胁。从层次体系上，可以将网络安全分成 4 个层次：物理安全、逻辑安全、操作系统安全、联网安全。在各个层次上，都存在安全的威胁。

网络的安全威胁来自于网络中存在的不安全因素。网络不安全的因素来自两个方面：一方面是网络本身存在的安全缺陷，主要因素有网络操作系统的脆弱性、TCP/IP 协议的安全性缺陷、数据库管理系统安全的脆弱性、网络资源共享、数据通信、计算机病毒等；另一方面是人为因素和自然因素，人为因素即人为的入侵和破坏，自然因素是一些意外事故，如发生地震而毁坏网络或服务器突然断电等。

1.2.1 人为因素的威胁

1. 人为的无意失误

（1）安全配置不当造成的安全漏洞。系统管理员设置资源访问控制的失误，而导致一些资源被偶然或故意地破坏，造成对网络信息保密性的破坏。

（2）无意的信息泄露。合法用户进入安全进程后中途离开而给非法用户提供可乘之机，口令、密钥等保管不善而为他人非法获得，用户安全意识不强、口令选择不慎、将自己的账号随意转借或与别人共享等都会给网络安全造成威胁。

（3）操作失误。删除文件、格式化硬盘、线路拆除等操作失误，系统掉电，“死机”等系统崩溃引起信息缺失，从而造成对网络信息完整性和可用性的破坏。

2. 人为的恶意攻击

这是计算机网络所面临的最大威胁，对手的攻击和计算机犯罪同属此类。此类攻击又可以分为两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性，是纯粹的信息破坏。这类积极攻击者通常截取网上信息包，对其进行更改使之失效，故意篡改信息，或者登录系统占用大量网络资源从而导致资源消耗，损害合法用户的利益。这类攻击者的破坏作用最大。另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息，这类攻击者称为消极攻击者。两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。人为恶意攻击具体可表现在以下几个方面：

（1）非授权访问。未经同意而使用网络或计算机资源被看做非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或者擅自扩大权限，越权访问信息等。其主要表现形式有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

（2）信息泄露或丢失。这是指敏感数据在有意或无意中被泄露出去或丢失，通常包括信息在传输中丢失或泄露（如“黑客”利用电磁泄露或搭线窃听等方式截获机密信息，或者通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息），以及信息在存储介质中丢失或泄露等。

（3）破坏数据完整性。以非法手段窃得对数据的使用权，删除、修改、插入或重发某些

重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

（4）拒绝服务攻击。不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序，使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入网络系统或不能得到相应的服务。

（5）利用网络传播木马和病毒。通过网络传播木马和计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

1.2.2　非人为因素的威胁

1. 网络操作系统的脆弱性

网络操作系统是计算机网络最基本的软件。无论哪一种操作系统，其体系结构本身就是一种不安全的因素。由于操作系统是可以动态连接的，包括 I/O 驱动程序与系统服务都可以用打补丁的办法进行升级和动态连接。这种打补丁的方法，生产该产品的厂商可以使用，“黑客”也可以使用，因而这种动态连接正是计算机病毒产生的温床。这种使用打补丁与渗透开发的操作系统是不可能从根本上解决安全问题的。由于操作系统支持的程序动态连接和数据动态交换是现代系统集成和系统扩展的必备功能，所以，操作系统的这种安全性弱点是无法避免的。

操作系统不安全的另一个原因在于它可以创建进程，即使在网络节点上同样也可以进行远程进程的创建与激活。更令人不安的是，被创建的进程具有可以继续创建进程的权利，这一点加上操作系统支持网络上传输文件，在网络上能加载程序，二者结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。如果把这种“间谍”软件以打补丁的方式“打入”合法用户，尤其是“打入”特权用户，那么，系统进程与作业监视程序根本监测不到“间谍”软件的存在。在 UNIX 与 Windows NT 中的 Daemon 软件实际上是一些系统进程，它们通常总是在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去。这类软件正是被“黑客”们所看中利用的。更令人担忧的是 Daemon 软件具有与操作系统核心层软件同等的权力。网络操作系统提供的远程过程调用（RPC）服务，以及它所安排的无口令入口也是“黑客”攻击网络的通道。凡此种种，充分暴露了操作系统在安全方面的脆弱性对网络安全已构成了威胁。

2. TCP/IP 协议的安全性缺陷

Internet 的基础是 TCP/IP 协议，该协议在实现上力求简单高效，而没有考虑安全因素。

（1）TCP/IP 是以明文（未加密）数据包的方式发送数据的，电子邮件口令、文件传输很容易被监听和窃取，而且可以实现监听和窃取行为的工具很多，在网上又是免费提供的。

（2）基于 TCP/IP 的应用服务都在不同程度上存在安全弱点。

（3）TCP/IP 在流程设计上也存在安全缺陷，缺乏安全策略。

（4）访问控制的配置十分复杂，易被错误配置，从而给“黑客”以可乘之机。

3. 数据库管理系统安全的脆弱性

由于数据库管理系统（DBMS）对数据库的管理是建立在分级管理概念上的，因此，DBMS 的安全是可想而知的。另外，DBMS 与网络操作系统之间存在不少接口，它的安全必须与操作系统的安全配套，这无疑是一个先天性的不足之处。由于 DBMS 是在操作系统上运行的，所以，这种安全性弱点是无法克服的。

4. 系统软硬件故障引起泄密

系统硬件或软件的故障也可能引起泄密。由于大多数共享的资源，往往同许多使用者

之间有相当一段距离（如网络打印机），这样就给窃取信息在时间和空间上创造了许多便利条件。

1.3 网络安全的基本技术与策略

网络安全是一项系统工程，针对来自不同方面的安全威胁，需要采取不同的安全对策。从法律、制度、管理和技术上采取综合措施，以便相互补充，达到较好的安全效果。而技术和策略是最直接的屏障。

1.3.1 网络安全的常用技术

1. 端口扫描技术

网络安全扫描技术是为使系统管理员能够及时了解系统中存在的安全漏洞，并采取相应防范措施，从而降低系统的安全风险而发展起来的一种安全技术。利用安全扫描技术，可以对局域网络、Web 站点、主机操作系统、系统服务及防火墙系统的安全漏洞进行扫描，系统管理员可以了解在运行的网络系统中存在的不安全网络服务，在操作系统上存在的可能导致遭受缓冲区溢出攻击或者拒绝服务攻击的安全漏洞，还可以检测主机系统中是否被安装了窃听程序，防火墙系统是否存在安全漏洞和配置错误等。

2. 网络嗅探技术

网络嗅探是利用计算机的网络接口截获目的地及其他计算机数据报文的一种技术。它工作在网络的最底层，把网络传输的全部数据记录下来。以帮助网络管理员查找网络漏洞和检测网络性能，还可以分析网络的流量，以便找出所关心的网络中潜在的问题。

3. 数据加密技术

加密是所有信息保护技术措施中最古老、最基本的一种手段。加密的主要目的是防止信息的非授权泄露。加密方法多种多样，在信息网络中一般是利用信息变换规则把可读的信息变成不可读的信息。既可对传输信息加密，也可对存储信息加密，把计算机数据变成一堆乱码数据。现代密码算法不仅可以实现加密，还可以实现数字签名、身份认证和报文完整性鉴别等功能，能有效地对抗截获、非法访问、破坏信息的完整性、冒充、抵赖和重放等威胁，因此，密码技术是信息网络安全的核心技术。

4. 数字签名技术

数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等安全问题。数字签名采用一种数据交换协议，使得数据的收发双方能够满足 3 个条件：①接收方能够鉴别发送方所宣称的身份；②发送方事后不能否认他发送过数据这一事实；③接收方事后不能伪造数字签名。数据签名一般采用非对称加密技术，发送方对整个明文进行加密变换，得到一个值，将其作为签名。接收方使用发送方的公开密钥对签名进行解密运算，如其结果为对方身份，则签名有效，证明对方身份是真实的。

5. 鉴别技术

鉴别的目的是验明用户或信息的正身。对实体声称的身份进行唯一地识别，以便验证其访问请求或保证信息来自或到达指定的源和目的。鉴别技术可以验证消息的完整性，有效地对抗冒充、非法访问、重放等威胁。按照鉴别对象的不同，鉴别技术可以分为消息源鉴别和通信双方相互鉴别；按照鉴别内容的不同，鉴别技术可以分为用户身份鉴别和消息内容鉴别。鉴别的方法很多，利用鉴别码验证消息的完整性，利用通行字、密钥、访问控制机制等鉴别用户身

份，防止冒充、非法访问。当今最佳的鉴别方法是数字签名，利用单方数字签名，可实现消息源鉴别、访问身份鉴别、消息完整性鉴别。利用收发双方数字签名，可同时实现收发双方身份鉴别、消息完整性鉴别。

6. 访问控制技术

访问控制的目的是防止非法访问。访问控制是采取各种措施保证系统资源不被非法访问和使用。一般采用基于资源的集中式控制、基于源和目的地址的过滤管理及网络签证技术等来实现。

7. 安全审计技术

计算机安全审计是通过一定的策略，通过记录和分析历史操作事件发现系统的漏洞并改进系统的性能和安全。

8. 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互连环境中。在大型网络系统与 Internet 互连的第一道屏障就是防火墙。防火墙通过控制和监测网络之间的信息交换和访问行为来实现对网络安全的有效管理，其基本功能为过滤进、出网络的数据，管理进、出网络的访问行为，封堵某些禁止行为，记录通过防火墙的信息内容和活动，对网络攻击进行检测和警告。

9. 入侵检测技术

网络入侵检测技术也叫网络实时监控技术，它通过硬件或软件对网络上的数据流进行实时检查，并与系统中的入侵特征数据库进行比较，一旦发现有被攻击的迹象，立刻根据用户所定义的动作作出反应，如切断网络连接，或通知防火墙系统对访问控制策略进行调整，将入侵的数据包过滤掉等。通过入侵检测技术，可监视登录到系统用户的一切行为，当用户试图对系统造成安全威胁时，自动发出报警或切断网络。

10. 病毒诊断与防治技术

病毒对计算机及网络造成的威胁是巨大的，一个安全的计算机网络系统，必须要有强大的病毒诊断能力和防范措施。

1.3.2　网络安全的基本策略

安全策略是指在某个安全区域内，所有与安全活动相关的一套规则，这些规则由此安全区域内所设立的一个权威建立。如果说网络安全的目标是一座大厦的话，那么相应的安全策略就是施工的蓝图，它使网络建设和管理过程中的安全工作避免盲目性。但是，它并没有得到足够的重视。国际调查显示，目前 55%的企业网没有自己的安全策略，仅靠一些简单的安全措施来保障网络安全，这些安全措施可能存在互相分立、互相矛盾、互相重复、各自为战等问题，既无法保障网络安全可靠，又影响网络的服务性能，并且随着网络运行而对安全措施进行不断的修补，使整个安全系统愈加臃肿不堪，难于使用和维护。

网络安全策略包括对企业的各种网络服务的安全层次和用户的权限进行分类，确定管理员的安全职责，如何实施安全故障处理、网络拓扑结构、入侵和攻击的防御和检测、备份和灾难恢复等内容。在本书中我们所说的安全策略主要指系统安全策略，主要涉及 4 个大的方面：物理安全策略、访问控制策略、信息加密策略、安全管理策略。

1. 物理安全策略

制定物理安全策略的目的是保护路由器、交换机、工作站、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击；验证用户的身份和使用权限，防止

用户越权操作；确保网络设备有一个良好的电磁兼容工作环境；建立完备的机房安全管理制度，妥善保管备份磁带和文档资料；防止非法人员进入机房进行偷窃和破坏活动。

2. 访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。下面我们分述各种访问控制策略。

（1）入网访问控制。入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为 3 个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查。三道关卡中只要任何一关未通过，该用户便不能进入该网络。对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才能继续验证用户输入的口令；否则，用户将被拒之网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密。经过加密的口令，即使是系统管理员也难以得到它。用户还可采用一次性用户口令，也可用便携式验证器（如智能卡）来验证用户的身份。

（2）网络的权限控制。网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。可以根据访问权限将用户分为以下几类：特殊用户（即系统管理员）；一般用户，系统管理员根据他们的实际需要为他们分配操作权限；审计用户，负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用一个访问控制表来描述。

（3）目录级安全控制。网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可以进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有 8 种：系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限（File Scan）、存取控制权限（Access Control）。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8 种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

（4）属性安全控制。当使用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。属性往往能控制以下几个方面的权限：向某个文件写数据、复制一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

（5）网络服务器安全控制。网络允许在服务器控制台上执行一系列操作。用户使用控制台可以进行装载和卸载模块、安装和删除软件等操作。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录