21世纪

高等学校精品规划教材

计算机网络与通信系列

# 计算机网络安全实用技术

主　编　葛彦强　汪向征
副主编　刘明亮　郭　磊　徐春华

中国水利水电出版社
www.waterpub.com.cn

21世纪高等学校精品规划教材

# 计算机网络安全实用技术

主　编　葛彦强　汪向征

副主编　刘明亮　郭　磊　徐春华

中国水利水电出版社
www.waterpub.com.cn

## 内 容 提 要

本书结合作者多年从事网络安全技术课程教学和实践工作的经验，针对应用型人才培养特点和社会需求编写，内容充实、思路清晰、实例丰富，突出了学以致用的原则，注重读者基本技能、创新能力和综合应用能力的培养，体现了高等教育的特点和要求。

全书共分 12 章，主要内容包括：网络安全概述、密码学基础和加密技术、数字签名和认证、防火墙技术和网闸技术、入侵检测技术、端口扫描与嗅探技术、黑客攻击和防范技术、计算机病毒及恶意代码、电子邮箱的使用及安全防范、网络操作系统安全、因特网服务的安全及安全网站的建设。能满足读者对服务器和个人电脑防护、安全配置和安全管理的需要。

本书介绍了大量的网络安全实用软件，包括各种技术中常用的软件。在各章后面配有课后习题，对每章的知识进行复习和巩固。

本书具有教材和技术资料双重特征，既可作为高等学校计算机及相关专业学生计算机网络安全技术课程的教材，也可作为网络安全技术人员的技术参考资料。

**本书配有电子教案，读者可以到中国水利水电出版社或万水书苑网站免费下载，网址：http://www.waterpub.com.cn/ softdown/或 http://www.wsbookshow.com。**

**图书在版编目（CIP）数据**

计算机网络安全实用技术 / 葛彦强，汪向征主编
-- 北京 : 中国水利水电出版社，2010.1

21世纪高等学校精品规划教材
ISBN 978-7-5084-6958-4

Ⅰ. ①计… Ⅱ. ①葛… ②汪… 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(2009)第205366号

**策划编辑：雷顺加　责任编辑：杨元泓　加工编辑：俞　飞　封面设计：李　佳**

| | |
|---|---|
| 书　名 | 21 世纪高等学校精品规划教材<br>**计算机网络安全实用技术** |
| 作　者 | 主　编　葛彦强　汪向征<br>副主编　刘明亮　郭　磊　徐春华 |
| 出版发行 | 中国水利水电出版社<br>（北京市海淀区玉渊潭南路 1 号 D 座　100038）<br>网址：www.waterpub.com.cn<br>E-mail：mchannel@263.net（万水）<br>sales@waterpub.com.cn<br>电话：（010）68367658（营销中心）、82562819（万水） |
| 经　售 | 全国各地新华书店和相关出版物销售网点 |
| 排　版 | 北京万水电子信息有限公司 |
| 印　刷 | 北京市天竺颖华印刷厂 |
| 规　格 | 184mm×260mm　16 开本　18.25 印张　456 千字 |
| 版　次 | 2010 年 1 月第 1 版　2010 年 1 月第 1 次印刷 |
| 印　数 | 0001—4000 册 |
| 定　价 | 29.80 元 |

# 前　言

随着计算机网络安全技术的广泛应用，社会对网络安全技术人才的需求量增加，培养网络安全技术人才成为高等教育的重要任务之一。学校培训需要实用型教材，要将枯燥难以理解的网络安全理论和技术变得容易掌握，充分体现学以致用的原则。本教材就是基于这一原则编写的，并且还能满足广大读者的自学需求。在保留足够的理论知识的基础上，密切联系实际应用，着重强调实用性和操作性，让读者既能通过本书学到实战经验，又能充分理解网络安全技术原理，轻松地掌握网络知识和技能，更好地促进有效性学习。

本教材共分为 12 章，主要内容介绍如下：

第 1 章首先介绍了网络安全的基本概念；然后分别介绍了网络所面临的各种威胁，以及导致网络不安全的因素；接着介绍了网络安全的策略、服务与机制；还介绍了网络安全的体系机构，其中重点说明 TCP/IP 的安全体系结构；最后介绍了网络安全的不同级别，并举例说明各个级别。

第 2 章首先简单介绍了密码学发展历史、概念和分类；然后详细介绍了对称加密技术和非对称加密技术；最后介绍了网络加密中的三种方法：链路加密、结点加密和端对端加密。

第 3 章首先介绍了 Hash 算法的定义、分类、安全性、结构和 MD5 算法及 SHA 算法；然后详细介绍了数字签名技术，包括基本原理、加密算法、问题及改进等；接着又详细介绍了身份认证，包括 Kerberos 认证协议和认证体系 x.509；还介绍了标准的密钥管理平台 PKI，包括 PKI 概念、PKI 提供的服务、PKI 的组成、PKI 的功能、密钥管理、信任模型和 PKI 的应用；最后简单介绍了授权管理基础架构（PMI）。

第 4 章首先简单介绍了防火墙的基本概念、作用、优点和缺点；然后详细介绍了防火墙的各种分类；接着又详细介绍防火墙的组成；还介绍了防火墙所采用的技术及三种体系结构；之后介绍了防火墙的实现以及常用的防火墙软件；最后简单介绍了网闸技术的概念、发展、对比及应用。

第 5 章首先介绍了入侵检测系统的定义、模型、功能和分类；然后介绍了入侵检测系统的原理，包括异常检测、误用检测以及特征检测等；接着分别介绍了基于主机的入侵检测系统、基于网络的入侵检测系统和基于分布式的入侵检测系统等三种不同的入侵检测系统；还介绍了 Snort 和 ISS RealSecure 的安装和使用；最后介绍了入侵检测系统目前的发展以及入侵检测的标准和功能评估。

第 6 章介绍了端口扫描和嗅探技术的基本原理和常用的工具。

第 7 章首先介绍了黑客攻击的基本步骤和拒绝服务的攻击与防御方法，最后介绍一些其他的攻击方式和防范方法。

第 8 章介绍了计算机病毒的定义、特征、分类、危害、传播途径、表现和发展趋势，还介绍了计算机病毒的基本机制以及网络蠕虫和木马的原理和防范。

第 9 章首先介绍了电子邮件的特点，重点介绍了电子邮箱的申请、使用与管理，并结合实例介绍了电子邮件的撰写与发送，以及 Outlook 的设置与使用，最后介绍了垃圾邮件、病毒

邮件的危害，以及安全防范措施。

第 10 章分为两大部分，第一部分主要阐述 Windows 的系统加固安全问题，第二部分阐述 Linux 系统的安全设置问题。第一部分主要介绍了加固 Windows 系统安全的几种方法，如安装更新包、关闭不必要的服务、账号安全管理等；在 Linux 系统的安全设置部分中主要介绍了用户账户的管理、服务进程的设置、文件的访问权限、日志系统的设置以及常用的安全工具。

第 11 章首先介绍了因特网上常见的服务；然后介绍了 Web 服务所面临的各种威胁，以及解决威胁的方法；接着介绍了 FTP 服务可能受到的攻击，以及防范攻击的方法；最后介绍了 DNS 服务器受到的威胁，以及如何去保护 DNS 服务器。

第 12 章首先介绍了如何对 Windows Server 2003 操作系统进行安全的配置；然后详细介绍了 Web 服务器的安全配置；接着又详细介绍 SQL Server 数据库的安全配置；又接着介绍了 Windows Server 2003 终端服务器远程程序配置，以及 Pcanywhere 的安装设置；然后介绍了磁盘镜像原理和管理，以及 NetStor DA 磁盘阵列备份系统；最后简单介绍了解决方法访问量过大的负载均衡。

本教材突出了以下特点：

（1）符合读者的认知特点。思路清晰，以计算机网络安全技术及应用为主线，包含网络安全的基本理论、网络安全技术、软件配置及使用、服务器配置与应用和网络安全维护等知识，为读者建立一个从理论到实践、从软件安装到配置使用和安全防护的层次清晰的知识体系。

（2）严格遵守专业务实、学以致用的原则，既注重理论基础，又突出实用性。知识全面、结构合理、内容充实，图文并茂。利用大量实例进行网络安全技术原理与应用的讲解，理论知识浅显易懂，实践内容随学随用，有非常强的实用性。

（3）从目前各种网络安全技术防护软件中选取大量的常用且实用的软件进行介绍，并配有简单或详细的使用及配置方法，方便教师教学、利于读者自学。

本书结构清晰、实用性强，具有教材和技术资料双重特征。既可作为高等学校计算机及相关专业学生计算机网络技术课程的教材，也可作为网络工程技术人员的技术参考资料。建议理论学时 56 学时，实验学时 52 学时。

本书由葛彦强、汪向征主编，刘明亮、郭磊、徐春华副主编。另外，张一、赵哲等也参加本书编写工作。李晗、翁雨、段鑫、邹芸等参与制作配套课件及网站。

计算机网络安全知识非常丰富，限于教材篇幅和作者水平，作者对有些知识的探讨和认识不够深入，书中难免有不妥之处，恳请读者批评指正。编者联系方式：geyanqiang@126.com。

编　者

2009 年 9 月

# 目　　录

# 第 1 章　网络安全概述


本章首先介绍网络安全的基本概念；然后分别介绍网络所面临的各种威胁，以及导致网络不安全的因素；接着介绍网络安全的策略、服务与机制；介绍网络安全的体系机构，其中重点说明 TCP/IP 的安全体系结构；最后介绍网络安全的不同级别，并举例说明各个级别。


- 网络安全的定义
- 网络面临的威胁
- 网络安全的策略、服务与机制
- TCP/IP 的安全体系结构
- 网络安全的级别分类

进入 21 世纪，计算机网络的飞速发展已经大大地改变了我们的生活方式，人类社会进入了信息时代。通过计算机网络，可以很方便地存储、交换以及搜索信息，给人们的工作、生活以及娱乐带来了极大的方便。然而，由于各种各样的原因，计算机网络也同时暴露出很多安全问题。这些安全问题对计算机网络的使用造成不小的影响，这些影响体现在个人生活、商务往来、经济活动、政治和军事等方面。计算机网络的安全研究就是为了克服这些安全问题，使计算机网络的使用更有保障而诞生和发展起来的。

由于其重要性和迫切性，计算机网络安全已经受到人们的极大关注，网络安全正在成为一个发展非常迅速的领域。在很短的时间内，各种网络安全技术纷纷问世并在不断地发展。网络安全技术作为一个独特的领域越来越受到全球网络建设者的关注。

## 1.1　网络安全的基本概念

网络安全作为一个新兴的领域，其中包含着各种各样的概念，在进行研究之前，有必要了解一下网络安全所包括的范围，以及网络安全的确切定义。

### 1.1.1　安全的基本概念

在了解网络安全之前，首先要清楚什么是安全，下面是两个机构对安全的定义。

国际标准化组织（ISO）：为数据处理系统建立和采取的技术、管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和显露。

我国安全保护条例：计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

### 1.1.2 什么是信息安全

知道了什么是安全，那么就来进一步了解什么是信息安全。

信息可以有多种存在方式，既可以写在纸上、储存在电子文档里，也可以用邮递或电子形式发送，同时也可以在电影上放映或者言语中提到。无论信息是以何种方式进行表示、共享和存储，都应适当地保护起来。

信息也是一种资产，与其他资产一样，应受到保护。信息安全的作用就是要保护信息不受大范围的威胁所干扰，使机构业务能够顺畅，减少损失及提供最大的投资回报和商机。

判断一个信息是否安全，至少应需要具有如下特性：

（1）保密性：保证信息只让合法用户访问；计算机系统不被非授权实体使用；信息不泄露给非授权的个人和实体。

（2）完整性：信息在存储或传输过程中保持不丢失的特性。信息完整性是网络信息安全的基本要求。

（3）真实性：信息不被恶意修改的特性。破坏信息的真实性是影响网络信息安全的常用手段。

（4）可用性：保证合法用户在需要时可以访问信息及相关资产，即当需要时能存取所需信息。

（5）可控性：对信息的传播及内容具有控制能力。

（6）可靠性：对信息的来源进行判断，判断来自对方的信息是否可信、是否可靠。

### 1.1.3 计算机网络安全的定义

网络安全从其本质来讲就是网络上的信息安全。它涉及的领域相当广泛，这是因为目前的公共通信网络中存在着各种各样的安全漏洞和威胁。从广义上来说，凡是涉及网络上信息的保密性、完整性、可用性和可控性的相关技术和理论，都是网络安全的研究领域。

网络安全是指网络系统的硬件、软件及数据受到保护，不遭受偶然的或者恶意的破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从用户的角度来说，他们希望涉及个人隐私和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、抵赖等手段对自己的利益和隐私造成损害和侵犯。同时他们希望自己的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运营商和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源的非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击。

因此，人们在不同的网络环境和网络应用中对网络安全的理解是不同的。网络安全在不同的环境和应用中有不同的解释。

（1）运行系统安全：即保证信息处理和传输系统的安全，包括计算机系统机房环境的法

律、政策的保护，计算机结构设计上的安全性考虑。硬件系统的安全运行，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统的正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏，产生信息泄露，干扰他人（或受他人干扰），本质上是保护系统的合法操作和正常运行。

（2）网络上系统信息的安全：包括用户口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

（3）网络上信息传播的安全：即信息传播后果的安全。包括信息过滤、不良信息的过虑等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公共通信网络上大量自传输的信息失控。本质上是维护道德、法则和国家利益。

（4）网络上信息内容的安全：即我们讨论的狭义的“信息安全”。它侧重于保护信息的机密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

### 1.1.4　计算机网络安全的属性

网络安全有自己特定的属性，主要有机密性、完整性、可用性和可控性这四个方面。

（1）机密性是为了使信息不泄露给非授权用户、非授权实体或非授权过程，或供其利用，防止用户非法获取关键的敏感信息或机密信息。通常采用加密来保证数据的机密性。

（2）完整性是为了使数据未经授权不能被修改，即信息在存储或传输过程中保持不被修改、不被破坏和不被丢失。它主要包括软件的完整性和数据的完整性两个方面的内容。

- 软件完整性是为了防止对程序的修改，如病毒。
- 数据完整性是为了保证存储在计算机系统中或在网络上传输的数据不受非法删改或意外事件的破坏，保持数据整体的完整。

（3）可用性是为了被授权实体访问并按需求使用，即当用户需要时能够在提供服务的服务器上进行所需信息的存取。例如：网络环境下拒绝服务、破坏网络和破坏有关系统的正常运行等，都属于对可用性的攻击。

（4）可控性是为了对信息的传播及内容具有控制能力。任何信息都要在一定传输范围内可控，如密码的托管政策等。

## 1.2　网络面临的威胁

计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。

### 1.2.1　威胁的分类

1. 威胁的分类

首先来看网络资源的划分，以及这些资源面临的潜在威胁。一般来说网络中存在四种资

源，即本地资源、网络资源、服务器资源、数据信息资源。

本地资源指的是本地局域网中的个人计算机操作系统，或者是服务器的应用操作部分，这部分资源会受到黑客的直接攻击。个人用户在使用应用程序或者操作系统时下载或者打开了含有病毒或后门的程序，都会对本地计算机的操作系统构成威胁，使操作系统崩溃，计算机无法使用。

网络资源，即网络系统，是本地资源与广域网进行数据交流的手段，黑客可以利用 IP 欺骗的手段使自己获得新的 IP 从而进入那些本来不能进入的地区，比如校园网、小区内部局域网等。对于个人服务器来说，因为不当使用服务器（例如不按要求下载，随意删除文件等）而被禁止和封杀 IP 的计算机，会通过这个方法重新进入服务器进行破坏活动。

服务器资源就是指服务器上开设的各种服务（如 Web、FTP、E-Mail 等），黑客会利用这些服务器的漏洞，入侵服务器，获得各种权限，从而对服务器或局域网进行控制。

数据信息资源指的是一些个人 Web 中的访问者信息、好友信息、客户信息等，相对于公司的数据信息来讲个人数据信息受到的入侵威胁要小很多。

根据资源面临的威胁不同，威胁可以分为两类，一类是偶然性威胁。这是由于系统设备的原因，例如突然断电、重新启动、线路中断等原因使某些用户获得了高级权限，从而进入没有授权给他的地域，获取他平常无法得到的信息，这类用户没有特殊的目的，而且事件发生的几率很小，一般不会对系统造成很大的伤害。而另一类威胁则会造成很大的危害，入侵者有备而来，使用各种工具、方法去试探系统漏洞，然后从这些漏洞侵入系统，获取他们需要的资料或修改数据，给系统造成无法挽回的损失。

2. 攻击类型

在第二类威胁中，主要包括以下几种攻击类型：

（1）拒绝服务攻击。这是目前最常见的攻击方式，一般是通过程序占用了主机上所有的资源，或者是在短时间内向主机发送大量数据包，影响其他正常数据交换，从而造成系统过载或系统瘫痪。网络蠕虫是目前最为常见的影响最大的实现拒绝攻击服务的方法。此外通过中止 TCP 握手过程和邮件炸弹也可以实现拒绝服务攻击。

（2）前门攻击。这种攻击方式最为直接，黑客会试图以系统承认的合法用户的身份登录系统进行访问。他们会试图直接利用字母组合去破解合法的用户名及密码。由于使用了配置强大的计算机运算的破解程序，前门攻击对于高级黑客来说也不是什么难事，所以当服务器日志中出现了大量登录失败的信息后，就说明很可能已经有黑客开始光顾服务器的前门了。

天窗攻击和特洛伊木马攻击。两者很相似，前者是直接利用管理员留下的后门（就是用于系统检测或故障维护的特殊用户通道）侵入系统；而后者是通过一些驻留内存的程序（后门病毒．代码炸弹等），为非法入侵者打开一个随时出入的特殊通道。

（3）IP 欺骗和中间人攻击是另外两种类似的攻击手段。第一种是通过新生成的 IP 报头非法进入合法网络进行通信。而中间人攻击则是首先通过 IP 欺骗获得合法身份，然后截取网络中的数据包，获取其中的数据，从这些数据中窃取合法的用户名和密码。

### 1.2.2 网络可能遇到的威胁

1. 非授权访问

非授权访问是指没有预先经过同意，就使用网络或计算机资源，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，或擅自扩大权限，越权访问信息。非授权访问主要有以下几种形式：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. 信息泄漏或丢失

信息泄漏或丢失是指敏感数据在有意或无意中被泄漏出去或丢失。它通常包括：信息在传输中丢失或泄漏（如“黑客”利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息），信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息等。

3. 破坏数据完整性

破坏数据完整性是指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

拒绝服务攻击是指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计算机网络系统或不能得到相应的服务。

5. 利用网络传播病毒

利用网络传播病毒是通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

### 1.2.3　对网络产生威胁的因素

1. 环境因素

计算机网络通过有线线路或无线电波连接不同地域的计算机或终端，线路中经常有信息传送。因此，自然环境和社会环境对计算机网络都会产生巨大的不良影响。对于自然界，如恶劣的温度、湿度、灰尘、地震、风灾、火灾等天灾以及事故都会对网络造成严重的损害和影响；强电、磁场会毁坏传输中的信息载体上的数据信息；计算机网络还极易遭雷击，雷电能轻而易举地穿过电缆，损坏网络中的计算机，使计算机网络瘫痪。对于社会，社会不安定，没有良好的社会风气也会造成对网络的人为破坏，给系统带来毁坏性的打击。

2. 数据通信

计算机网络要通过数据通信来交换信息，这些信息是通过物理线路、无线电波以及电子设备进行的。这样，在通信中传输的信息极易遭受损坏，如搭线窃听、网络线路的辐射等都对信息的安全造成威胁。

3. 计算机病毒

计算机网络可以从多个节点接收信息，因而极易感染计算机病毒，病毒一旦侵入，在网络内再按指数增长进行再生和传染，很快就会遍及网络各节点，短时间内可以造成网络的瘫痪。

4. 资源共享

计算机网络实现资源共享，包括硬件共享、软件共享、数据共享、通信线路共享。每个终端可以访问主计算机的资源，各终端也可以共享资源，这也为异地用户提供了巨大方便，同时也给非法用户窃取和破坏信息创造了条件，非法用户有可能通过终端或节点进行非法浏览、修收。此外硬件和软件故障也会引起泄密。同时，大多数共享资源（如网络打印机）同它们的

许多使用者之间有相当一段距离，这样就给窃取信息在时间和空间上提供了便利条件。

5. 网络管理

网络系统的正常运行离不开系统管理人员对网络系统的管理。对系统的管理措施不当会造成设备的损坏及保密信息的人为泄露，而这些失误主要是人为因素造成的。

## 1.3 网络安全策略、服务与机制

### 1.3.1 网络安全策略

1. 物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限、防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

抑制和防止电磁泄漏（即 TEMPEST 技术）是物理安全策略的一个主要问题。目前主要防护措施有两类：一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护，这类防护措施又可分为以下两种：一是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；二是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

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非常访问。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三个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的缺省限制检查。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，加密的方法很多，其中最常见的方法有：基于单向函数的口令加密，基于测试模式的口令加密，基于公钥加密方案的口令加密，基于平方剩余的口令加密，基于多项式共享的口令加密，基于数字签名方案的口令加密等。经过上述方法加密的口令，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。

网络管理员应该可以控制和限制普通用户的账号使用、访问网络的时间、方式。用户名或用户账号是所有计算机系统中最基本的安全形式。用户账号应只有系统管理员才能建立。用户口令应是每个用户访问网络所必须提交的“证件”、用户可以修改自己的口令，但系统管理员应该可以控制口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后，再进一步履行用户账号的缺省限制检查。网络应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应能对用户的账号加以限制，用户此时应当无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

（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。受托者指派和继承权限屏蔽（IRM）可作为其两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。可以根据访问权限将用户分为以下几类：

1）特殊用户（即系统管理员）。

2）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。

3）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）。用户对文件或目标的有效权限取决于以下两个因素：用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。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。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、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装载和卸载模块，可以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时间限制、非法访问者检测和关闭的时间间隔。

（6）网络监测和锁定控制。网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形或文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

（7）网络端口和节点的安全控制。网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护，并以加密的形式来识别节点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

（8）防火墙控制。防火墙是近期发展起来的一种保护计算机网络安全的技术性措施，它是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

3. 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全；端一端加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是由形形色色的加密算法来具体实施，它以很小的代价提供很大的安全保护。在多数情况下，信息加密是保证信息机密性的方法。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。

在常规密码中，收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有：美国的 DES 及其各种变形，比如 Triple DES、GDES、New DES 和 DES 的前身 Lucifer；欧洲的 IDEA；日本的 FEAL-N、LOKI-91、Skipjack、RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。在众多的常规密码中影响最大的是 DES 密码。

常规密码的优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。

在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有：RSA、背包密码、McEliece 密码、Diffe-Hellman、Rabin、Ong-Fiat-Shamir、零知识证明的算法、椭圆曲线、ElGamal 算法等。最有影响的公钥密码算法是 RSA，它能抵抗到目前为止已知的所有密码攻击。

公钥密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便的实现数字签名和验证，但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公钥密码算法将是一种很有前途的网络安全加密体制。