中等职业学校电子信息类教材（计算机技术专业）

网络安全基础教程

王　韬　　向传杰　主编

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

内 容 简 介

网络安全既是计算机网络得以实际应用的前提，也是计算机及相关专业的从业人员不可或缺的基础知识。本书注重实用，兼顾基础，较为系统地介绍了网络安全领域的相关知识。全书共分 7 章，包括网络安全概述，TCP/IP 协议、安全缺陷及入侵检测，密码技术基础，防火墙，计算机病毒及其防治，网络数据库安全策略和网络安全策略。

本书可作为中等职业学校计算机及相关专业的教材，也可作为网络管理员、软件开发人员和 Internet 个人用户的学习参考用书。

本书配有电子教学参考资料包，包括教学指南、电子教案、习题答案，详见前言。

图书在版编目(CIP)数据

网络安全基础教程/王韬，向传杰主编．—北京：电子工业出版社，2005.1
中等职业学校电子信息类教材. 计算机技术专业
ISBN 7-5053-9971-3

Ⅰ. 网… Ⅱ. ①王…②向… Ⅲ. 计算机网络—安全技术—专业学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 127392 号

责任编辑：陈健德 特约编辑：汪荣萍
印　　刷：
出版发行：电子工业出版社
　　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：787×1 092 1/16 印张：9.75 字数：249.6
印　　次：2005 年 1 月第 1 次印刷
印　　数：5 000 册 定价：12.80 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。

前　言

随着电子邮件、IP 电话、网络查询和浏览，以及电子商务技术的迅速发展，网络正在成为现代社会正常运转不可或缺的组成部分。然而，网络在给人们带来种种益处的同时，也向人们提出了挑战，这就是网络的安全问题。电子邮件可能被偷看，商业机密可能被窃取，政府网站可能被恶意修改等，所有这些都是网络存在的安全隐患。

网络安全问题的解决方案涉及面很广，本书试图对其中的基本问题进行较为系统的介绍。全书共分 7 章。第 1 章是全书的引言，对网络安全的相关问题进行初步的介绍；第 2 章介绍 TCP/IP 协议及其安全缺陷，并详细介绍几种入侵检测系统；第 3 章介绍密码技术基础；第 4 章介绍防火墙；第 5 章介绍计算机病毒及其防治技术；第 6 章介绍网络数据库安全策略；第 7 章介绍网络安全策略。

本书由王韬、向传杰主编。刘键强、向阳霞、王昌盛、朱晓栋编写了部分章节，全书由王森教授审稿，在此，特向其表示感谢。

本书编者长期从事电子商务、电子政务和计算机网络相关技术的开发、管理和培训工作，有较强的实践经验。但由于编写时间紧、水平有限，书中难免存在不当和谬误之处，敬请广大读者批评指正。

作为教材，为了方便教师教学使用，本书配有教学指南、电子教案及习题答案（电子版），请有此需要的教师登录华信教育资源网（http://www.hxedu.com.cn）下载，或与电子工业出版社联系，我们将免费提供。电子邮件地址：ve@phei.com.cn。

编　者

2004.05

目　录

第 1 章　网络安全概述

知识要点

- 网络安全的概念
- 网络安全的层次结构
- 网络安全服务
- 网络安全机制
- 主要的网络安全技术

随着计算机技术、网络技术的迅猛发展，计算机网络与人们工作和生活的联系越来越紧密。特别是随着以 Internet 为代表的全球性信息化浪潮的日益高涨，网络技术的应用正日益普及和深入，应用领域从传统的小型业务系统逐渐向大型的关键业务系统扩展。伴随网络的普及，安全日益成为影响网络效能的重要因素，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对网络安全提出了更高的要求。

让我们先看几个网络安全历史上著名的案例。

1988 年 11 月 2 日，美国康乃尔大学的研究生罗伯特·莫里斯编制了一个被称为“蠕虫”（worm）的程序，并将它放入 Internet 中。该程序利用 UNIX 操作系统的一个缺陷，躲过计算机系统的安全检查，在网络中自由穿梭，大量地进行自我复制，到第二天凌晨，“蠕虫”从美国东海岸传到西海岸，使军方的 MIL 网和 APRA 网中的 6 000 台计算机受到感染，甚至欧洲连网的计算机都受到影响，直接经济损失近亿美元。这是自计算机问世以来最严重的一次计算机病毒侵扰事件，它引起了世界各国的广泛关注。

自 2000 年 2 月 7 日起，连续数日，来历不明的黑客对“雅虎”（Yahoo）、“电子湾”（eBay）、“亚马逊”（Amazon）和微软公司的网站等美国众多知名网站实施连续大规模的网络袭击行动，使网络服务器无法运行，造成服务中断数小时。这个事件不仅引起了美国联邦政府和世界各大网络公司的高度重视，也令世人对网络安全问题给予了空前关注。它又一次向人们敲响了网络安全的警钟。

除了“网络侠客”兴风作浪以外，由于受政治、经济和军事目的的影响，计算机系统正日益成为被攻击的目标。在 1991 年的海湾战争中，美国第一次针对信息系统使用了计算机病毒武器，一种称为“AF/91”的计算机病毒，侵入伊军的计算机网络，使伊军的指挥系统失灵，削弱了伊军的战斗力。

1998 年，一连串的网络非法入侵事件改变了中国网络安全犯罪“一片空白”的历史。据公安部的资料，1998 年中国共破获计算机黑客案件近百起，利用计算机网络进行的各类违法犯罪行为在中国以每年 30%的速度递增，黑客的攻击方法已超过计算机病毒的种类，总数达

近千种。据公安部官员估计，目前已发现的黑客攻击案约占总数的15%，多数事件由于没有造成严重危害或商家不愿透露而未被曝光。有媒体报道，中国 95%的与 Internet 相连的网络管理中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构更是黑客攻击的重点。

根据权威机构统计，连入 Internet 的计算机之中，平均每 20 s 就被黑客成功地入侵一次，Internet 上防火墙有 1/3 以上被突破。一方面，通过计算机安全技术所构筑的信息安全屏障逐渐增多；另一方面，计算机犯罪活动十分猖獗，计算机犯罪所使用的技术手段越来越高明和巧妙。以计算机欺诈、计算机破坏、计算机间谍、计算机病毒和信用卡犯罪等为代表的计算机犯罪对社会造成了巨大损失。据美国联邦调查局统计，一起计算机犯罪的平均损失是 50 万美元，而一起刑事案件的平均损失是 2 000 美元。1995 年《计算机安全》杂志在全世界范围内抽样调查了 300 家典型公司，其中 69%的公司报告上一财政年度遇到过计算机网络安全问题，59%的公司报告上述安全问题所造成的经济损失超过 1 万美元，超过 25%的企业报告其损失高于 25 万美元。据 1995 年统计，以白领犯罪为特征的信息安全事件，共给全球造成经济损失高达 150 亿美元之巨。

从上述案例可以看出，网络必须有足够强的安全措施。无论是在局域网中还是在广域网中，网络的安全措施应能全方位地防范各种不同的威胁，并避免网络的脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

1.1 网络安全的概念

1.1.1 安全的历史回顾

同任何事物的发展历程相似，安全问题也有一个随着社会进步、技术更新和应用需求的发展而发展的过程。我们可以把安全的发展分为三个阶段，即通信安全、计算机安全和网络安全。

1．通信安全

在数据处理设备广泛应用之前，人们对于有价值的信息的安全保护主要是通过物理手段和管理手段实现的。例如，使用坚固的文件柜，对存储敏感文档的柜子加密码锁，对涉密人员严格审查等。

但是，如果文件在传递过程中被截获，那么文件上的内容就会被对手知道，这就产生了通信安全问题。解决这个问题的办法是对秘密文件进行加密，早在公元前 600 年，Julius Caesar 就发明了 Caesar 密码，以使报文即使被截获也无法读出。二战期间，德国军队也曾使用过一种称为“ Enigma ”的机器来加密报文。在著名的中途岛海战中，美国人和日本人在编码和破译方面展开了一场有关通信安全的对抗，对战争的胜负起了关键作用。

从上面的事例可以看出，通信安全的主要目的是解决数据传输的安全问题，采取的主要措施是密码技术。

2．计算机安全

随着计算机技术的发展和广泛应用，人们把更多的信息以计算机文件或其他形式存储到

计算机上，以利用计算机对它们进行更为有效的处理。这样，计算机的安全问题就变得突出起来。

计算机安全的目标是要保证计算机的实体安全、运行安全和信息安全。

实体安全是研究和提供保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施和过程。

运行安全是研究为保障系统功能的安全实现所应提供的各种安全措施（如风险分析、审计跟踪、备份与恢复和应急技术等），以保护信息处理过程的安全。

信息安全是研究防止信息内容被故意或偶然地非授权泄露、更改和破坏，或防止信息被非法地辨识、控制的各种机制，以确保信息的完整性、保密性和可用性。

3．网络安全

网络安全同单个计算机的安全在目标上并没有本质的区别，然而，由于网络环境比单机环境更为复杂，其安全的保障相对于计算机的安全保障就增添了新的内容。特别是随着 Internet 的发展和普及应用，如何解决在开放网络环境下的安全问题更成为迫切需要解决的问题。

网络安全的主要目的是解决在分布式网络环境中信息载体及其运行所涉及的安全保护问题，主要措施是提供完整的信息安全保障体系，包括防护、检测、响应和恢复。

1.1.2　网络安全的概念

网络安全的概念在 20 世纪经历了一个漫长的历史阶段，在 20 世纪 90 年代得到了深化。那么，什么是网络安全呢？下面我们从不同的角度来对网络安全的概念加以介绍。

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、数论和信息论等多种学科的综合性学科。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改和泄露，系统连续、可靠、正常地运行，网络服务不中断。

网络安全从其本质上来讲就是网络上的信息安全。从广义的角度来说，凡是涉及到网络上信息的保密性、完整性和可用性等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随着“角度”的不同而不同。从用户（个人和企业）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，其保密性、完整性和真实性受到保护，避免其他人或对手利用窃听、冒充、篡改和抵赖等手段加以侵犯，同时也避免其他用户的非授权访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问和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、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，避免机要信息被泄露，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的角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成不良影响，必须对其进行控制。

1.1.3 网络安全工作的目的

网络安全工作的目的就是为了在安全法律、法规和政策的支持与指导下，通过采用合适的安全技术与安全管理措施，完成以下任务。

① “进不来”。使用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。

② “拿不走”。使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

③ “看不懂”。使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

④ “改不了”。使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而确保信息的完整性。

⑤ “走不脱”。使用审计、监控和防抵赖等安全机制，使得攻击者、破坏者和抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

1.1.4 网络安全要素

构成计算机网络安全的要素主要有以下五种。

① 实体安全。即系统设备及相关设施运行正常，系统服务适时，包括环境、建筑、设备、防电磁辐射、数据介质安全及火灾报警等。

② 运行安全。即系统资源和信息资源的使用合法，包括电源、空调、人事管理、机房管理、出入控制、数据与介质管理和运行管理等。

③ 数据安全。即系统的数据或信息完整、有效且使用合法，不被破坏和泄露，包括输入输出数据安全、进入识别、访问控制、加密、审计与追踪、备份与恢复等。

④ 软件安全。即软件（网络软件、操作系统等）完整，包括软件开发规程、软件安全测试、软件的修改和复制等。

⑤ 通信安全。即计算机通信和网络的安全，包括线路、传输、接口、终端与工作站以及路由器的安全等。

1.1.5 网络安全的保证措施

尽管技术问题是本书讨论的重点，但应该时刻意识到，单纯利用技术手段是不足以保证网络的安全的，必须辅之以配套的管理措施和法规等，形成一套完整的网络安全策略。安全策略是指在一个特定的环境下，为保证提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括建立安全环境的三个重要组成部分，即：

- 威严的法律。
- 先进的技术。
- 严格的管理。

安全的基石是社会法律、法规和手段。通过建立与网络安全相关的法律和法规，使不法分子慑于法律，不敢轻举妄动。

先进的安全技术是网络安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。

网络的安全管理包括确定安全管理等级和安全管理范围，制定有关网络操作使用规程和人员出入机房管理制度，制定网络系统的维护制度和应急措施等。各网络使用机构、企业和事业单位应建立相适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，提高整体的网络安全意识。

1.2　网络安全的层次结构

国际标准化组织（ISO）在开放系统互连标准（OSI）中定义了七个层次的网络参考模型，它们分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。不同的网络层次之间的功能虽然有一定的交叉，但基本上是不同的。例如，数据链路层负责建立点到点通信，网络层负责寻径，传输层负责建立端到端的通信信道。从安全角度来看，各层均能提供一定的安全手段，针对不同层的安全措施是不同的。

在物理层，可以在通信线路上采用某些技术使得搭线偷听变得不可能或者容易被检测出来。

在数据链路层，点对点的链路可采用通信保密机进行加密和解密，即当信息离开一台机器时进行加密，而进入另外一台机器时进行解密。所有的细节可以全部由底层硬件实现，高层根本无法察觉。但是，这种方案无法适应需要经过多个路由器的通信信道。因为在每个路由器上都需要进行加密和解密，而在开放网络环境中并不能确定每个路由器都是安全的，在这些路由器上会出现潜在的安全隐患。当然，链路加密无论在什么时候都是很容易实现而且是有效的，也被经常使用，但是在 Internet 环境中并不完全适用。

在网络层，使用防火墙技术处理信息在内外网络边界的流动，确定来自哪些地址的信息可以通过或者禁止访问哪些目的地址的主机。

在传输层，连接可以进行端到端的加密，以及进程到进程间的加密。

应用层的安全主要是指针对用户身份进行认证并且建立起安全的通信信道。有很多针对具体应用的安全方案，它们能够有效地解决诸如电子邮件、HTTP 等特定应用的安全问题，能够提供包括身份认证、不可否认、数据保密、数据完整性检查以及访问控制等功能。但是在应用层并没有一个统一的安全方案。通用安全服务 GSS-API 的出现试图将安全服务进行抽象，为上层应用提供通用接口，在 GSS-API 接口下可以采用各种不同的安全机制来实现这些服务。

总结前面的讨论，可以用图 1.1 来表示网络安全的层次结构。

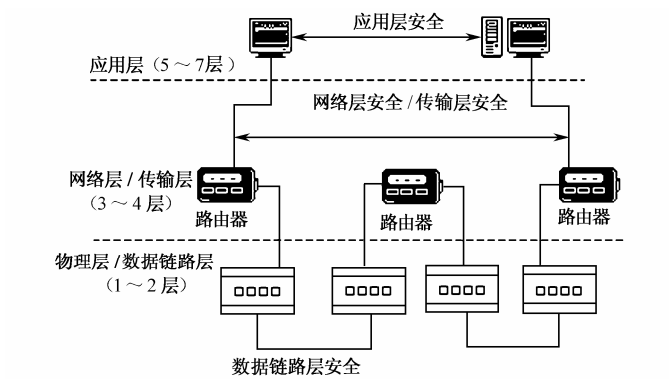

图 1.1　网络安全的层次结构

1.3 网络安全服务

在计算机网络中，主要的安全防护措施被称为网络安全服务。可使用一种或多种安全机制来提供这些服务。安全服务可分为以下六种：

① 保密性服务。保护信息不被泄露或暴露给未授权的实体（用户或系统）。
② 认证服务。提供某个实体的身份认证。
③ 数据完整性服务。保护数据以防止未授权的用户进行更改、删除或替代。
④ 非否认服务。防止参与某次通信交换的一方事后否认本次交换曾经发生过。
⑤ 访问控制服务。保护资源以免对其进行非法使用和操纵。
⑥ 可用性服务。保证信息与系统可被授权人正常使用。

1．保密性

保密性（confidentiality）服务是保护传输的信息不会泄露给非授权的用户。有两种基本的方法能够提供这种服务。一种方法是只信任已定义的安全域（security domains）中的实体。一个安全域包含所有的主机和资源，以及用来连接它们的传输媒体等，它们都遵守一个正式的安全策略并能够为用户提供一定的安全级别。安全域中的主机之间存在某种程度的信任关系，并且它们之间能够提供和获得某些服务，而在安全域以外的主机却无法得到。安全域中能够包含其他的网络和子网，并且它们也拥有相同的信任级别。另一种方法是使用加密技术，加密使得明文变换为密文，而只有拥有解密密钥的目的接收者才能将密文重新转换为明文格式。当从源主机发送的数据包离开当前的安全域而不得不经过中间网络到达目的主机时，就需要采用加密技术，以防止重要的信息在这些中间网络上传输时被截获。

除了上面所说的数据的保密性之外，还应该考虑通信流的保密性，例如数据的来源和目的地、频率、长度或其他特性，以防止非法用户通过通信流分析获得有价值的信息。

2．认证

认证（authentication）服务致力于保证信息的可靠性。认证服务提供了关于某个实体身份的保证，某个实体声称具有一个特定的身份时，认证服务将提供某种方法来证实这一声明是正确的。口令是一种提供认证的简单方法。

认证是对付假冒攻击的有效方法，通常可将认证服务分为实体认证和数据起源认证两种。

如果身份是由参与某次通信连接或会话的远端的一方提交的，这种情况下的认证服务被称做实体认证。这种认证只是简单地认证实体本身的身份，不会和实体想要进行何种活动联系起来。显然，它的作用是有限的（因为实体通常是希望在识别身份的基础上执行其他操作）。因此，在实际工作中，实体认证通常会产生一个明确的结果，允许实体进行其他活动或通信。例如，在实体认证过程中将产生一个对称密钥，可以用来解密一个文件进行读写，或者与其他实体建立一个安全通信通道。实体身份一旦获得认证，就可以和访问控制列表中的权限关联起来，决定能否进行访问。

如果身份是由声称它是某个数据项的发送者的那个实体所提交的，此身份连同数据项一起发送给接收者，这种情况下的认证服务被称做数据起源认证。这种认证就是认证某个指定

的数据项是否来源于某个特定的实体。这既不是孤立地认证一个实体，也不是为了允许实体执行下一步的操作而认证它的身份，而是为了确定被认证的实体与一些特定数据项有着静态的不可分割的联系。

在达到基本的安全目标方面，上述两种类型的认证服务都具有重要的作用。数据起源认证是保证部分完整性目标的直接方法，可保证知道某个数据项的真正的起源；而实体认证则采用以下各种不同方式，以达到安全目标。

① 作为访问控制服务的一种必要支持，访问控制服务的执行依赖于确认的身份（访问控制服务直接对达到保密性、完整性、可用性及合法使用目标提供支持）。

② 作为提供数据起源认证的一种可能方法（在它与数据完整性机制结合起来使用时）。

③ 作为对责任原则的一种直接支持，例如，在审计追踪过程中做记录时，提供与某一活动相联系的确认身份。

实体认证的一个重要的实例是人员认证，即对处于网络终端上的某个人进行认证。需要特别指出的是，在某个终端上，不同的人员之间容易互相替代。在区分单个人方面可以采用一些其他的技术。

3．数据完整性

数据完整性（data integrity）服务防止网络上发生破坏数据完整性的行为，其中包括非授权地篡改、增加和删除。

数据的完整性和保密性是有区别的。假设源机和目的主机分别是自动取款机（ATM）和银行。如果任何其他个人要通过搭线窃听获得用户的账号及个人身份号码，这就属于保密性问题。如果有人要修改 ATM 和银行之间的信息传输，使原本 100 元的交易让银行只划走 10 元，这就属于数据完整性问题。

与保密性服务一样，数据完整性服务的一个重要特征是它的具体分类，即对哪些数据采用完整性服务，它有以下三种重要的类型。

① 连接完整性服务。它对某个连接上传输的所有数据进行检验。

② 无连接完整性服务。它对构成一个无连接数据单元的所有数据进行完整性检验。

③ 选择字段完整性服务。它对某个数据单元中所指的字段进行完整性检验。

所有的完整性服务都能对付新增或修改数据的企图，但是它不一定都能对付复制和删除数据。复制是由重放攻击造成的。无连接和选择字段完整性服务主要是为了检测对部分数据的修改。连接完整性服务要求能够防止在某一连接内重放数据，但它仍然存在弱点，因为某个入侵者可能重放一个完整的连接。检测对某些数据的删除与检测重放攻击一样困难。

一个完整性服务也许会提供“恢复”的选择。在这种情况下，当在某个连接内检测到完整性被破坏的时候，该服务将试图“恢复”数据。例如，通信将返回到某一检测点并重新开始。

4．非否认

非否认（nonrepudiation）服务用于防止发送方或接收方否认消息的传送。即当消息发出时，接收方可以证实消息确实从声明的发送方发出；类似地，当接收到消息时，发送方也能证实消息确实由声明的接收方接收了。

与其他安全服务不同，非否认服务的主要目的是保护通信用户免遭来自系统中其他合法用户的威胁，而不是来自未知攻击者的威胁。“否认”最早被定义成一种威胁，它是指参与某次通信交换的一方事后不诚实地否认曾发生过本次交换。非否认服务是用来对付这种威胁的一种服务。

非否认服务的出发点并不是仅仅因为在通信各方之间存在着相互欺骗的可能性，它也反映了这样一个现实，即没有任何一个系统是完备的，而且可能出现通信双方最终达不成一致协议的情况。

纸质文件（如合同、报价单、标书、订单、货运清单和支票等）在商业活动中发挥着巨大的作用，然而在对它进行处理的进程中，会发生许多问题。例如，邮递过程中的文件丢失，收信者在作出处理之前将收到的文件丢失，文件是由某个没有得到足够授权的人产生的，在某一机构内部或在机构间的文件传递活动被收买，伪造文件，有关某个文件有争议的签署日期等。为了系统地处理以上所出现的问题，采用了许多不同的机制，如签名、公证签名、收据、邮戳及挂号邮件等。

在进行电子化商业活动时，情况与此类似。非否认服务提供了保护机制。有时，电子化作业所出现的问题比纸张作业更难以解决，因为在处理文件时，常常涉及更多的人。然而，在某些方面，电子作业所出现的问题反而更容易解决，这主要是由于采用了较为复杂的技术——数字签名技术。

原则上，非否认服务适用于任何一种能够影响两方或更多方的事件。通常，这些纠纷涉及某一特定的事件是否发生了，是什么时候发生的，有哪几方参与了这一事件以及与此事件有关的信息是什么。如果我们只考虑计算机网络环境，服务的否认又可以分为以下两种不同的情况：

① 起源的否认。这是一种关于“特定的某一方是否产生了某一特定的数据项”的纠纷或关于产生时间的纠纷。

② 传递的否认。这是一种“某一特定的数据项是否被传送给某特定一方”的纠纷及关于产生时间的纠纷。

这两种服务的否认情况导致了两种不同的非否认服务。

5．访问控制

访问控制（access control）就是拒绝未授权者对计算机网络的任何资源进行访问。在网络环境中，访问控制能够限定和控制通过通信链路对主机系统和应用资源的访问。

6．可用性

可用性（assured usage）服务关注的是合法用户在所规定的服务级别上对网络资源能否使用的问题。所规定的服务级别通常是指服务质量，它应在安全策略中有明确的规定。

1.4 网络安全机制

网络安全机制定义了实现网络安全服务所使用的可能方法。按照 OSI 网络安全体系结构的定义，网络安全服务所需要的网络安全机制包括以下几类。

① 数据加密。数据加密机制是各种安全服务的基础，可分为隐蔽密钥加密和公开密钥

加密两大类。

② 数字签名。数字签名机制通常用于支持非否认服务和完整性保护服务，基于信息摘录技术和公开密钥加密技术。

③ 访问控制。访问控制常用的技术包括基于访问控制表和其他手段进行资源的访问控制。例如，对用户设置不同的访问权限。

④ 数据完整性。数据完整性保护机制涉及校验码技术、信息摘录技术和数字签名技术等。

⑤ 鉴别交换。它用于支持访问控制服务所需要的身份认证功能，如进行口令交换，包括单口令、多重口令和一次性密式口令等。

⑥ 流量填充。它是数据保密服务的一种辅助技术，用于对空闲信道进行填充，从而掩盖真正的数据流。

⑦ 路由控制。它是访问控制服务的支撑技术，包括对路由的选择进行限制和对路由信息进行鉴别。

⑧ 认证。它是非否认服务的支撑技术，是基于数字签名技术对数据传输的完整性、数据源、传输时间和数据宿主进行认证。

1.5　主要的网络安全技术

在网络应用环境中，用户在系统提供的安全服务保证下安全地进行各种网络应用，安全服务的基础是各种安全机制。而对用户而言，他们直接面对的是各种网络安全技术及产品。这些安全技术包括：防火墙技术、加密技术、鉴别技术、数字签名技术、安全协议技术、审计监控技术和病毒防治技术等。这里先对几种重要的网络安全技术做简要介绍，详细论述请参看本书的相关章节。

1.5.1　防火墙技术

防火墙是指设置在不同网络（如可信任的企业内部网络和不可信任的公共网络）或网络安全域之间的一系列部件的组合。

防火墙的作用主要表现在以下几个方面：

① 防火墙是网络安全的屏障。防火墙作为一个阻塞点和控制点，能极大地提高内部网络的安全性，并通过过滤不安全的服务而降低风险。

② 防火墙可以强化网络安全策略。通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。

③ 对网络存取和访问进行监控、审计。如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并做日志记录，同时也能提供对网络使用情况的统计数据。

④ 防止内部信息的外泄。通过利用防火墙对内部网络的划分，可实现内部网络重点网段的隔离，从而限制了局部重点或敏感网络的安全问题对全局网络造成的影响；另外，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。

除了安全作用，防火墙还支持具有 Internet 服务特性的虚拟专网技术 VPN（virtual private network）。通过 VPN，可将企事业单位在地域上分布在世界各地的 LAN 或专用子

网，有机地连成一个整体。

防火墙技术的实现通常是基于所谓“包过滤”技术，而进行包过滤的标准通常是根据安全策略制定的。除了包过滤技术，防火墙还可以利用代理服务器软件实现。早期的防火墙主要起屏蔽主机和加强访问控制的作用，现在的防火墙则逐渐集成了网络安全技术中的最新研究成果，一般都具有加密、解密和压缩、解压等功能，这些技术增加了信息在 Internet 上的安全性。现在，防火墙技术的研究已经成为网络安全技术的主要研究方向。

当然，网络的安全性通常是以网络服务的开放性、便利性和灵活性为代价的，对防火墙的设置也不例外。防火墙的隔断作用一方面加强了内部网络的安全，另一方面却使内部网络与外部网络的信息系统交流受到阻碍，增大了网络管理的开销，减小了信息传递的速率。

1.5.2 加密技术

防火墙实际上是一种访问控制机制，它能够保证不让未授权用户对所保护的网络及其资源进行非法访问。而加密技术则可以保证即使非法用户获得了网络及其资源的访问权，也无法理解其内容。加密技术是保障信息安全的最基本和最核心的技术。

加密和解密的传统方法是使用一个对称算法，在这个算法中加密信息的发送方和接收方要求拥有相同的密钥，对称算法的缺点在于算法和密钥必须保密。另外，密钥必须从一个人传达到另一个人，这就产生了安全性威胁。然而，该算法的主要优点是可以建立某种鉴定系统，减少由于伪造信息所带来的问题。

1.5.3 安全协议技术

在网络协议层次上解决网络的安全性是一种比较彻底的网络安全解决方案。目前广泛使用的 TCP/IP 协议在设计之初，并没有将安全性作为一个重要指标，这就是导致目前网络应用不安全的一个重要因素。安全协议可以实现身份鉴别、密钥分配、数据加密、防止信息重传和非否认等安全机制。

安全协议的设计和改进有两种方式：

① 对现有网络协议进行修改和补充，如 IPSec（在 TCP/IP 协议的网络层协议 IP 和传输层协议 TCP 之间增加的一层安全协议）作为在 IPv4 及 IPv6 上的加密通信框架，已为大多数厂商所支持。

② 在应用层和传输层之间增加安全子层，如安全协议套接字层（SSL），安全超文本传输协议（SHTTP）等。

1.5.4 计算机病毒防治技术

计算机病毒是一种人为编制的特殊的程序，具有自我复制和传播的能力，借助于媒体潜伏并能够在特定条件下激活自己，对计算机系统或网络实施攻击和破坏。计算机病毒是危害计算机系统和网络安全的一个非常重要的因素。

近几年来，利用操作系统和应用程序的漏洞，以多种传播方式传播的在网络上爆发的网络病毒越来越多。这些新一代的病毒所使用的技术可以充分体现网络时代的网络安全与病毒的巧妙结合，它们将“网络蠕虫”、计算机病毒和“木马”程序合为一体，对世界范围的网络和主机造成了很大的危害。

需要强调的是，网络安全是一个系统工程，不是单一的产品或技术可以完全解决的。这