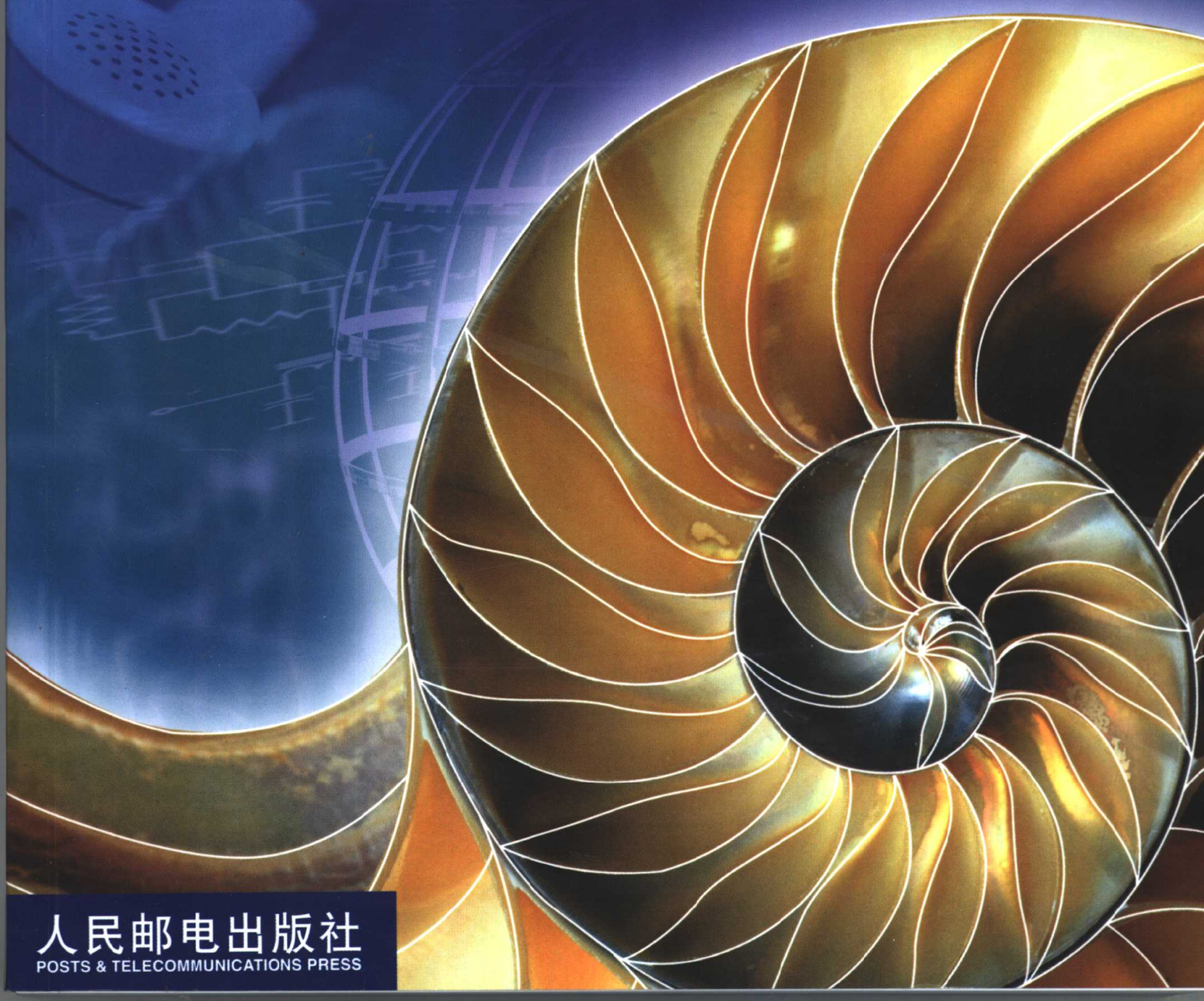
网络与现代通信技术丛书

网络与通信安全技术

刘东华等 编著



人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

网络与现代通信技术丛书

网络与通信安全技术

刘东华　等编著

人民邮电出版社

图书在版编目(CIP)数据

网络与通信安全技术/刘东华编著. —北京：人民邮电出版社，2002.11
（网络与现代通信技术丛书）
ISBN 7-115-09745-3

I. 网… II. 刘… III. 计算机通信网—安全技术 IV. TN915.08

中国版本图书馆 CIP 数据核字(2002)第 077873 号

内 容 提 要

本书在介绍网络与通信安全基本概念的基础上，重点讨论了实现网络安全的几项基本技术的原理和实现方法，并对网络和通信安全构成威胁的一些因素进行了详细地论述。全书共分为两大部分。第一部分为网络与通信安全技术，包括第一至第四章，主要介绍了各种密码技术、网络安全协议、防火墙技术；第二部分主要介绍对网络和通信安全构成威胁的关键因素，包括第五至第七章，主要介绍计算机病毒、特洛伊木马以及缓冲区溢出等问题。该书不追求面面俱到，而是重点突出，主要集中在对上述几个问题的探讨，力求原理解释清楚，语言通俗易懂。

本书的主要读者对象是从事计算机网络安全和通信安全研究和开发人员，同时也可供大专院校师生学习参考，或作为相关领域的培训教材。

网络与现代通信技术丛书

网络与通信安全技术

◆ 编　　著　刘东华　等
责任编辑　梁　凝

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67129258
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：25.25
字数：632 千字　　2002 年 11 月第 1 版
印数：1-4 500 册　　2002 年 11 月北京第 1 次印刷

ISBN 7-115-09745-3/TN・1798

定价：39.00 元

前　言

网络与通信安全所涉及的关键技术有很多，在一本书中如果面面俱到，难免空泛。因此我们将重点放在了安全技术和安全威胁两个方面上。在安全技术方面主要讲述典型的加密技术、安全协议以及防火墙技术；在安全威胁方面主要讲述了计算机病毒、特洛伊木马程序以及缓冲区溢出，同时针对每个问题给出了一些实例，希望能够为读者理解和具体化这些技术提供一些帮助。全书内容组织如下：

第一章主要讲述网络与通信安全的基本概念，对于通信安全存在的威胁以及加密、确认、控制和协议等方面的概念进行了介绍。

第二章重点介绍当前比较通用的各种密码体制，包括传统密码和公钥密码、DES 和 RSA 加密算法、刘氏密码以及较新的椭圆密码算法等，并通过实例的形式进行了详尽的解释。

第三章主要讨论网络安全协议。主要讲述了计算机网络结构中应用层、网络层和传输层的安全性问题和 SSL、TSL 等安全协议。

第四章首先介绍了防火墙的基本原理，以及实现防火墙的两个基本技术：包过滤技术和代理技术。然后介绍了包过滤防火墙、基于代理的防火墙、屏蔽主机防火墙、屏蔽子网防火墙以及双宿主机防火墙，并给出了防火墙的一个实现实例。

第五章主要讲述计算机病毒。介绍了计算机病毒的概念、分类、命名、特点、产生原因、危害以及对计算机病毒的预防和处理。在分析计算机病毒工作机理的基础上重点讨论了常见的宏病毒的特点、发作形式及处理方法。

第六章简要介绍了对网络和通信安全造成威胁的另一个因素——特洛伊木马程序。在这一章里，我们主要介绍特洛伊木马的基本概念、木马的检测以及木马程序的解决方法，最后给出了一个特洛伊木马程序实例。

最后一章主要介绍缓冲区溢出原理、溢出程序的生成、溢出的保护方法并给出了缓冲区溢出的一个应用攻击程序实例。

承蒙灯芯工作室的孙兆林先生和余东峰先生为本书的出版提供了许多宝贵的具体意见，并进行了卓有成效的策划。国防科技大学电子科学与工程学院的张森强先生为本书的写作提供了许多有价值的参考资料，并与作者进行了多次有意义的讨论，这些思想在本书中都有所体现。作者所在工作单位的领导和同事为本书的写作提供了良好氛围和工作环境，在此一并致谢。

还要感谢胡耀华小姐为本书的录入、校正所作的大量烦杂工作。

在本书的编写过程中，参考了许多国内外网络与通信安全论著以及众多网络安全站点，在此向这些作者表示衷心的感谢。

由于编者的水平有限，书中不足甚至谬误之处在所难免，恳请各位专家、学者和读者批评指正。

目　录

第一章 概 论

跨入21世纪，Internet 技术带领信息科技进入了新的时代。网络改变了人们工作、生活的方式，使信息的获取、传播、处理和利用更加高效快捷。世界范围的信息革命激发了人类历史上最活跃的生产力，但同时也使得信息的安全问题日渐突出而且情况也越来越复杂。信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域。同时，信息安全问题也是人们能否保护自己个人隐私的关键。因此，认清网络的脆弱性和潜在威胁，采取强有力的安全策略，对于保障网络的安全性将变得十分重要。

信息和网络安全是一个系统的概念，所涉及的领域相当广泛。完善的安全体系必须协调法律、技术和管理三大要素。

对于整个信息与网络安全体系，从消息的层次来看，主要包括：

- 完整性：保证消息的来源、去向、内容真实无误。
- 保密性：保证消息不会被非法泄露扩散。
- 不可否认性：保证消息的发送和接收者无法否认自己所做过的操作行为。

从网络层次来看，包括：

- 可靠性：保证网络和信息系统随时可用，运行过程中不出现故障。若遇意外打击能够尽量减少损失并尽早恢复正常。
- 可控性：保证营运者对网络和信息系统有足够的控制和管理能力。
- 互操作性：保证协议和系统能够互相连接。
- 可计算性：保证准确跟踪实体运行达到审计和识别的目的。

从技术层次上讲，主要包括：

- 数据加密技术：提高信息系统和数据的安全性、保密性和防止秘密数据被破解。
- 防火墙技术：是软件和硬件的组合体，是用来加强网络之间访问控制的特殊网络互联设备。
- 攻击检测技术：利用攻击者的试图登录失败记录、试图连接特定文件、程序和其他资源的失败记录等信息，或者通过监视某些特定值表来有效地发现来自外部或内部的非法攻击。
- 数据恢复技术：对遭受攻击和破坏的数据进行有效的恢复。

从设备层次来看，包括

- 质量保证
- 设备备份
- 物理安全

从经营管理层次来看，包括：

- 人员可靠性
- 规章制度完整性

从行业层次来看，包含的内容主要有：

- 安全移动通信
- 安全数据通信
- 安全卫星通信
- 安全智能网
- 安全 ISDN
- 安全计算机
- 安全网络
- 安全多媒体安全 HDTV
- 安全数据库
- 安全路由器
- 安全浏览器

由此可见，信息安全的研究涉及到多个学科领域，其边界几乎是无法限定的。同时随着网络技术的发展，也还会有新的安全问题不断出现。

1.1 通信安全

确保信息的安全是通信安全的主要目标。通信安全主要包括两个方面：信息的传输安全和信息的存储安全。所谓信息的传输安全主要是指信息在动态传输过程中的安全。在网络系统中，任何调用指令和信息反馈都是通过网络来实现的，因此网络安全是通信安全中一个极其重要的方面。信息的存储安全指的是信息在静态存放状态下的安全。例如，数据是否被非法调用和窃取，这一般是通过设置访问权限、身份识别以及局部隔离等方法来实施。虽然人为因素和非人为因素都可以对通信安全构成威胁，但是精心设计的人为攻击威胁最大。攻击可分为主动攻击和被动攻击。

被动攻击不会导致对系统中所含信息的任何改动，而且系统的操作和状态也不被改变。因此被动攻击主要威胁信息的保密性，常见的被动攻击手段有：

（1）对网络和通信线路上信息的监听和偷窃

用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息，也即在信息传输链路上通过物理的或逻辑的手段对数据进行非法的截获和监听。例如，对通信线路中传输的信号进行搭线监听，或者利用通信设备在工作过程中产生的电磁泄露截获有用信息等。

（2）对监听或截获的数据进行分析

通过对系统进行长期监视，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。

主动攻击则意在窜改系统中所含信息，或者改变系统的状态和操作。因此主动攻击主要威胁信息的完整性、可用性和真实性。常见的主动攻击手段有：

（3）对用户身份的冒充

通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。一般是采用身份认证的方式进行防护。但是，用于用户身份认证的密码在登录时常常是以明文的方式在线路上进行传输的，因此很容易被攻击者截获，进而可以对用户的身份进行冒充，使身份认证机制被攻破。

（4）对传输信息的篡改

改变消息内容，删除其中的部分内容，用假消息代替原始消息，或者将某些额外消息插入其中。目的在于使用户误认为修改后的信息合法，从而无法获得准确、有用的信息。

（5）对发出信息的抵赖

这是一种来自合法用户的攻击，他对自己发出的信息进行恶意攻击。例如，否认自己曾经发布过的某条消息、伪造一份对方来信、修改来信等。

（6）其他攻击手段

对信息进行重发、非法登录、非授权访问、破坏通信规程和协议、拒绝合法服务请求、设置陷阱和重传攻击等等。

要保证通信安全就必须想办法在一定程度上克服以上的种种威胁。最后，需要指出的是无论采取何种防范措施都不可能保证通信系统的绝对安全。安全是相对的，不安全才是绝对的。在具体实用过程中，经济因素和时间因素也是判别安全性的重要指标。基于通信安全目标和各种因素的影响，实现通信安全首先要在安全、方便和代价之间做出均衡。对通信系统安全性的要求越高，对通信的限制和使用难度就不断加大，同时实现安全性的代价也随之提高。因此，实现通信系统安全的真正有效的途径是根据用户需求来对安全性要求进行正确的评估，也即用户针对自己的具体信息存取要求，对自身能力、可容忍的风险、增加安全的代价和通信系统体系结构等作出良好的评判和均衡。此外，通信安全与人为作用是密不可分的。所有的各种安全保密功能都是人设计的，同时人也是破坏和干扰各种安全保护功能的始作俑者。因此，通信安全技术仅仅是实现通信安全的一个环节，真正意义上的通信安全应集技术、管理和法律武器为一体。

1.2 网络安全

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。但由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互联性等特征，致使网络易受黑客、恶意软件和其他不轨的攻击，所以网上信息的安全和保密是一个至关重要的问题。对于军用自动化指挥网络、C^3I 系统和银行等传输敏感数据的计算机网络系统而言，网上信息的安全和保密尤为重要。因此，上述的网络必须有足够强的安全措施，否则该网络将是无用的、甚至会危及国家的安全。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素造成的脆弱性和潜在威胁。故此，网络的安全措施应能全方位地针对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

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。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；可能是外来黑客对网络系统资源的非法使用等。归结起来，针

对网络安全的威胁主要有：

（1）无意失误

如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带来威胁。

（2）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就属于这一类。此类攻击又可以分为以下两种：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；另一类是被动攻击，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漏。

（3）系统和软件漏洞

操作系统和应用软件不可能是百分之百的无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是网络攻击者进行攻击的首选目标，曾经出现过许多网络攻击者攻入网络内部的事件，这些事件大部分就是因为安全措施不完善所招致的苦果。

1.3 安全技术

通信和网络安全技术的种类很多，下面我们就技术比较成熟、在实际通信和网络系统中比较常用于保障通信和网络安全的技术进行简单的介绍。

1.3.1 物理安全技术

物理安全策略包括保护计算机系统、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。

1.3.2 信息加密技术

信息加密技术是保障信息安全的最基本、最核心的技术措施。信息加密也是现代密码学的主要组成部分。信息加密过程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唯一方法。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。

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—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唯一方法。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、NewDES 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。

DES 由 IBM 公司研制，并于 1977 年被美国国家标准局确定为联邦信息标准中的一项。ISO 也已将 DES 定为数据加密标准。DES 是世界上最早被公认的实用密码算法标准，目前它已经受住了长达 20 年之久的实践考验。DES 采用 56 比特长的密钥将 64 比特长的数据加密成等长的密文。在 DES 的加密过程中，先对 64 比特长的明文块进行初始置换，然后将其分割成左右各 32 比特长的子块，经过 16 次迭代，进行循环移位与变换，最后再进行逆变换得出 64 比特长的密文。DES 的脱密过程与加密过程很相似，只需将密钥的使用顺序进行颠倒。DES 算法采用了散布、混乱等基本技巧，构成其算法的基本单元是简单的置换、代替和模 2 加。DES 的整个算法结构都是公开的，其安全性由密钥保证。DES 的加密速度很快，可用硬件芯片实现，适合于大量数据加密。

在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能由加密密钥推导出脱密密钥。比较著名的公钥密码算法有：RSA、背包密码、McEliece 密码、Diffe-Hellman、Rabin、Ong-FiatShamir、零知识证明的算法、Elliptic Curve、ElGamal 算法等等。最有影响的公钥加密算法是 RSA，它能够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，尤其可方便地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技术。

RSA 加密算法诞生于 1978 年，目前它已被 ISO 推荐为公钥数据加密标准。RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但是想分解它们的乘积却极端困难，因此可以将乘积公开作为加密密钥。RSA 的算法结构相当简单，其优点是不需要密钥分配，但缺点是速度慢。

当然在实际应用中人们通常是将常规密码和公钥密码结合在一起使用，比如：利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特数来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特，而后者则先将信息序列分组，每次处理一个组。

加密技术用于网络安全有两种方式，一是面向网络，一是面向应用服务。前者通常工作

在网络层或传输层，使用经过加密的数据包传送，认证网络利用及其他网络协议所需要的信息，从而保证网络的连通性和可用性不受到侵害。在网络层上使用的加密技术对网络应用层的用户是透明的，此外，通过适当的密钥管理机制使用这一方法还可以在公众的互联网络上建立虚拟专用网络。面向网络应用服务的加密技术则是目前最为流行的加密方法。例如，使用 Kerlberos 算法的 telnet，NFS，rlogin 等，及用作 E-mail 加密的 PEM 和 PGP，这类方法的优点在于实现简单。

密码技术是网络安全最有效的技术之一。加密网络不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。

1.3.3 网络控制技术

网络控制技术种类繁多而且还相互交叉。虽然没有完整统一的理论基础，但是在不同的场合下，为了不同的目的许多网络控制技术确实能够发挥出色的功效。下面简要介绍一些常用的网络控制技术。

1．防火墙技术

它是一种允许接入外部网络，但同时又能够识别和抵抗非授权访问的网络安全技术。防火墙可分为外部防火墙和内部防火墙。前者在内部网络和外部网络之间建立起一个保护层，从而防止网络入侵者的侵袭，其方法是监听和限制所有进出通信，挡住外来非法信息并控制敏感信息被泄露；后者将内部网络分隔成多个局域网，从而限制外部攻击造成的损失。防火墙是用以阻止网络中的非法用户访问网络信息的屏障，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。目前的防火墙主要有以下三种类型。

（1）包过滤防火墙

包过滤防火墙设置在网络层，可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表，信息过滤表是以其收到的数据包头信息为基础而建成的。信息包头含有数据包源 IP 地址、目的 IP 地址、传输协议类型（TCP、UDP、ICMP 等）、协议源端口号、协议目的端口号、连接请求方向、ICMP 报文类型等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问，也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包，无法实施对应用级协议的处理，也无法处理 UDP、RPC 或动态的协议。

（2）代理防火墙

代理防火墙又称应用层网关级防火墙，它由代理服务器和过滤路由器组成，是目前较流行的一种防火墙。它将过滤路由器和软件代理技术结合在一起。过滤路由器负责网络互联，并对数据进行严格选择，然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时，代理服务器接受申请，然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务，如果接受，它就向内部网络转发这项请求。代理防火墙无法快速支持一些新出现的业务（如多媒体）。现在较为流行的代理服务器软件是 WinGate 和 Proxy Server。

（3）双缩主机防火墙

该防火墙是用主机来执行安全控制功能。一台双缩主机配有多个网卡，分别连接不同的网络。双缩主机从一个网络收集数据，并且有选择地把它发送到另一个网络上。网络服务由双缩主机上的服务代理来提供。内部网和外部网的用户可通过双缩主机的共享数据区传递数据，从而保护了内部网络不被非法访问。

2．访问控制技术

它允许用户对其常用的信息库进行适当权利的访问，限制用户随意删除、修改或拷贝信息文件。访问控制技术还可以使系统管理员跟踪用户在网络中的活动，及时发现并拒绝网络攻击者的入侵。访问控制采用最小特权原则：即在给用户分配权限时，根据每个用户的任务特点使其获得完成自身任务的最低权限，不给用户赋予其工作范围之外的任何权力。Kerberos存取控制是访问控制技术的一个代表，它由数据库、验证服务器和票据授权服务器三部分组成。其中，数据库包括用户名称、口令和授权进行存取的区域，验证服务器验证要存取的人是否有此资格，票据授权服务器在验证之后发给票据允许用户进行存取。

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、用户帐号的缺省限制检查。三道关卡中只要任何一关未过，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帐号使用、访问网络的时间和方式。用户名或用户帐号是所有计算机系统中最基本的安全形式。用户帐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、口令的唯一性、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，再进一步履行用户帐号的缺省限制检查。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帐号加以限制，用户此时应无法进入网络访问