全国职业教育计算机类系列教材

网络信息安全与防范技术

主　编　宁　蒙
参　编　（按姓氏笔画排序）
陈玉平　吴瑞强

东 南 大 学 出 版 社

内 容 提 要

本书采取网络信息安全理论和实际案例相结合的方式，全面系统地介绍了计算机网络信息安全及防范的基本概念、基本理论，并详细地介绍了网络信息安全的基本技术及防范的具体实现方法。本书主要内容包括：网络信息安全基础，网络信息安全威胁与防范策略，系统平台安全与访问控制，Internet 应用安全与防范，数据安全与加密技术，基于木马的攻击与防范，服务器安全及电子商务与政务安全，网络扫描与监听，计算机网络病毒防范技术，防火墙技术及应用，综合实训等内容。

本书以注重实用为原则，将理论知识与实际技术实现相结合，选材范围广泛、实例丰富、实用性强，力图做到易懂、易学、易用。通过对本书的学习，读者可以很容易地掌握网络信息安全防范的基本理论知识与具体实现方法。

本书可作为高职高专院校或中等职业技术学校计算机及相关专业的教材，也可供网络信息安全、网络管理、信息管理等相关领域的工程技术人员参考。

图书在版编目(CIP)数据

网络信息安全与防范技术/宁蒙主编. —南京：东南大学出版社，2005.6

ISNB 7-5641-0022-2

Ⅰ.网… Ⅱ.宁… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 044756 号

东南大学出版社出版发行

（南京四牌楼 2 号 邮编 210096）

出版人：宋增民

江苏省新华书店经销 印刷厂印刷

开本：787mm×1 092mm 1/16 印张：18.25 字数：452 千字

2005 年 6 月第 1 版 2005 年 6 月第 1 次印刷

印数：1—4000 册 定价：27.00 元

（凡有印装质量问题，可直接向发行部调换。电话：025—83795801）

前　言

随着 *Internet* 和 *Intranet* 的迅速发展，网络技术已被广泛应用于社会生活甚至军事战略等各个方面，人们的工作生活与网络关系日益密切。与此同时，各种网络黑客攻击活动日益猖獗，攻击的手段呈多样化和先进性，严重地影响了网络资源的安全和人们对网络的信任度。目前的情况是：很多人网络信息安全意识比较差，即便对网络信息安全有足够的重视，却又缺乏对网络信息安全问题的应对措施。而目前很多网络信息安全方面的教材、书籍，要么纯粹以理论为主，要么只介绍软件的使用方法，很显然对于高职高专和中职学生来说，单单重视其中某一个方面是不够的。网络信息安全的防范是一个系统的范畴，不能认为掌握某些安全软件的应用就够了，要想保障网络信息安全，必须建立完善的安全体系和制订正确的安全策略，软件的应用只是其中的一部分。当然也不能单靠理论学习就可以解决所有问题。在某种意义上，安全防范是一个经验的积累过程，因此，如何适应网络信息安全形式的要求，同时兼顾理论学习与安全防范技能的培养是一个很现实的问题。为此，结合几位教师多年的网络信息安全方面的教学和实践经验，我们编写了这本书。

本书采取网络信息安全理论和实际案例相结合的方式，全面系统地介绍了计算机网络信息安全以及防范的基本概念、基本理论，并详细地介绍了网络信息安全基本技术及防范的具体实现方法。

本书的主要内容包括：网络信息安全基础，网络信息安全威胁与防范策略，系统平台安全与访问控制，*Internet* 应用安全与防范，数据安全与加密技术；基于木马的攻击与防范，服务器安全及电子商务与政务安全，网络扫描与监听，计算机网络病毒防范技术，防火墙技术及应用，综合实训等内容。通过对本书的学习，读者可以很容易地掌握网络信息安全防范的基本理论知识与具体实现方法。

本书以注重实用为原则，将理论知识与实际技术实现相结合，选材范围广泛、实例丰富、实用性强，力图做到易懂、易学、易用。本书可作为高职高专或中等职业技术学校计算机及相关专业课程的教材，也可供网络信息安全、网络管理、信息管理等相关领域的工程技术人员参考。

参加本书编写的有宁蒙（第 *1*、*2*、*5*、*6*、*7*、*8*、*9*、*12* 章）、陈玉平（第 *3*、*4* 章）、吴瑞强（第 *10*、*11* 章），全书由宁蒙主编。

在本书编写过程中，先后得到了本溪市电子工业学校计算机专业和网络管理中心多位教师以及山西综合职业技术学院电子分院教材科张隆德老师、计算机中心吴克强老师的帮助和指导，并参考相关专业书籍、文献 *20* 多本，查阅了大量网络信息安全方面的网络资料，在这里对各位老师及相关资料的编著者一并表示感谢。

由于时间仓促、篇幅限制，加之编者水平有限，书中难免有疏漏不妥之处，敬请读者批评指正。

编　者

2005.3

出 版 说 明

全国职业教育计算机专业建设研讨会于 2004 年 7 月 18 日在湖北三峡职业技术学院召开，来自上海、江苏、山西、辽宁、贵州、黑龙江等地的 40 多位职业技术院校的代表参加了会议。

在本次会议上，与会专家学者对目前职业教育的现状进行了深刻分析，特别对计算机专业建设提出了独到的见解。一致认为：计算机专业建设要与教学改革相结合，以市场需求为导向，以教材建设为基础。因此，会议决定为配合计算机专业建设，编写一套适合职业教育的计算机系列教材，要求突出职业特点，有创新思想，以“考证”为切入点，加强实践环节。

根据各校计算机专业建设和课程设置情况，本次会议由全国职业教育计算机类教材建设委员会秘书长孔繁华组织各院校计算机专业教师确定了首批教材建设的选题，以后还将随着专业建设的深入及计算机技术的发展，逐步形成一套完善的、切合实际的计算机职业教育系列教材。

全国职业教育电子信息类教材编委会的要求是：坚决贯彻职业教育的要求，即基础适度够用、加强实践环节、突出职能教育，把握职业教育电子信息类专业课程建设的特点；立足当前学生现状，面向用人单位（市场），打破条条框框，少一些理论，多一些技能教育；采取逆向思维的方式编写，即从市场需要什么技能来决定学生需要什么知识结构，并由此决定编写什么教材。

全国职业教育电子信息类教材编委会会员单位：

南京信息职业技术学院　　湖北三峡职业技术学院
本溪电子工业学校　　长沙市电子工业学校
扬州电子信息学校　　山西综合职业技术学院
河南信息工程学校　　北京信息职业技术学院
大连电子工业学校　　福建省电子工业学校
黑龙江信息技术职业学院　　山西省邮电学校
本溪财贸学校　　新疆机械电子职业技术学院
山西工程职业技术学院　　山东信息职业技术学院
四川省电子工业学校　　哈尔滨机电工程学校
锦州铁路运输学校　　上海机电工业学校
内蒙古电子信息职业技术学院　　贵州省电子工业学校
江苏海事职业技术学院　　南京交通职业技术学院
黑龙江农业经济职业学院　　扬州职业大学
南通纺织职业技术学院　　南通航运职业技术学院

全国职业教育电子信息类教材编委会

2005 年 1 月

目　　录

1 网络信息安全概述

随着 Internet 和 Intranet 的迅速发展，计算机网络对安全的要求已经越来越高。由于网络技术已被广泛应用于社会生活乃至军事战略等各个方面，因此网络信息安全问题已超越其本身而达到国家安全问题的高度。本章将介绍有关网络信息安全的概念、目标、网络信息安全体系结构、网络信息安全形式及发展趋势等知识。

1.1 网络信息安全概况

自 1969 年美国国防部的 ARPANet 诞生以来，网络信息技术一直在飞速地发展着，伴随着万维网的兴起，将人类推向了一个崭新的信息时代。从商业机构到个人都将越来越多地通过互联网或其他电子媒介进行电子邮件发送、购物、炒股和办公等活动。这无疑给社会、企业乃至个人带来了前所未有的便利，这一切正是得益于互联网的开放性和匿名性的特点，然而这又不可避免地带来了各种安全隐患。截止 2005 年 1 月，中国已经有网民 9 400 万，上网计算机 4 160 万台，这一庞大的数字使得网络信息安全必须引起足够的重视。

网络信息涉及国家的政治、军事、文教等诸多领域，其中存贮、传输和处理的信息有许多是政府决策信息、商业经济信息、金融证券数据、科研数据等重要信息，还有很多是涉及国家和企业的机密信息，所以难免会吸引来自世界各地的各种人为的有目的的攻击（例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等）。同时，网络实体还要经受自然灾害等方面的考验。不安全因素既有人为的也有非人为的。

据权威机构对中小企业的网络信息安全产品现状的调查结果显示，目前超过 90％的中小企业客户认为尽管普遍采用了防病毒、防火墙产品，但其目前的安全系统并不能完全满足自身的网络信息安全需求。尽管有超过 80％的反馈客户都使用了病毒防护产品，接近 50％的反馈客户采用了防火墙产品，但调查结果仍显示：大多数中小企业目前所部署的这些单点网络信息安全产品并不足以应对当前日益复杂的各种网络威胁，包括像“冲击波”病毒、“震荡波”病毒、“求职信”病毒、木马攻击、拒绝服务、后门攻击等混合威胁。

很多企业在信息化过程中，将较多的资金和技术力量投入到对付外来的网络攻击上，这说明企业的安全意识已经得到了很大提高，可是他们却忽略了来自企业内部的网络攻击，结果造成了非常大的损失。此外，他们在防范技术上过多考虑如何利用现有的信息安全软硬件来防范攻击，但是信息安全技术人员的技术水平、经验以及网络信息安全管理措施的严重不足依旧使信息安全系统出现比较大的漏洞，仍然会造成信息安全管理失控。

相对而言，个人信息安全并没有被足够重视，然而一些相对低级的网络信息安全攻击行为同样会给个人的信息安全带来不可弥补的损失。很多人认为只要安装了防火墙、防病毒软件，给系统及时地打了“补丁”就可以高枕无忧了，然而不正确或不彻底的安全设置、策略设置将使这些安全措施形同虚设，麻痹的思想只会导致更严重的损失。

目前，网络信息安全问题已经引起国家各部门乃至整个社会的足够关注，各国都相继出台

了大量的政策、法规，积极推广网络信息安全的防范技术和监测技术。

1.1.1 网络信息安全的定义

一提到网络信息安全，不少人心里首先想到的应该是“某站点的主页被黑了”、“我的 QQ 号码或电子邮件地址被别人盗用”之类的网络信息安全事件，其实这些仅仅是属于其中的一类远程攻击。还有很多网络信息安全事件从表面上看没有发生的迹象，可是机密数据却被入侵者偷偷地读取或修改，造成不可弥补的损失。网络信息安全的含义应该超出我们想象的范畴。那么，什么是网络信息安全呢？

国际标准化组织(ISO)引用“ISO74982”文献中对安全的定义是这样的：安全就是最大限度地减少数据和资源被攻击的可能性。Internet 的最大特点就是开放性，然而对于安全来说，这又是它致命的弱点。

网络信息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。它主要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、泄露，系统连续、可靠、正常地运行，网络服务不中断。

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信息安全的研究领域。网络信息安全还关系到国家安全和主权、社会的稳定、民族文化的继承和发扬等重要问题。它正随着全球信息化步伐的加快而变得越来越重要。

此外，网络信息安全的具体含义会随着“角度”的变化而变化。从个人和企业用户的角度来说，他们希望涉及个人隐私或商业利益的数据信息在网络上传输时受到保密性、完整性和真实性的保护，避免非授权人利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，例如个人的 QQ 号码、电子邮件地址、游戏账号不应被别人非法盗用。从网络运行和管理者角度来说，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“陷阱”、病毒、非法存取、拒绝服务、网络资源的非法占用和非法控制等威胁。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，避免因机要信息的泄露而对社会产生危害，给国家造成巨大损失。从社会教育和意识形态角度来说，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。

1.1.2 网络信息安全问题产生的原因

很显然，这个问题要从为什么网络信息会遭到非法的访问或破坏的原因谈起。网络系统是一个非常复杂的系统，任何一个环节，无论是操作系统、网络协议、硬件设备还是用户操作以及管理制度、安全策略等出现问题，都可能影响网络信息安全。常见的能影响网络信息安全的因素有很多，主要包括：

(1) 计算机犯罪　如网络银行账号被窃取。

(2) 人为失误　如用户使用不当、安全意识差等。

(3) 黑客攻击　是指黑客(Hacker)的入侵或侵扰，如非法访问、拒绝服务、计算机网络病毒、木马控制、口令窃取、非法链接等。

(4) 信息泄密　内部泄密与外部泄密、信息丢失以及传输过程中发生的泄密。

(5) 电子谍报　如信息流量分析、信息窃取等。

(6) 系统漏洞　包括网络协议中的缺陷(如 TCP/IP 协议中存在的安全问题等)、操作系

统的缺陷和后门(主要有系统漏洞、活动天窗)。

(7) 自然灾害　如地震、火灾造成系统破坏、数据破坏。

因操作系统、网络协议、应用软件的缺陷和漏洞造成的影响网络信息安全的行为和人为故意及非故意的失误操作(如权限设置错误、安全级别设置过低)是造成网络信息安全问题的主要原因。在这些问题中,有的可以以技术手段加以解决,有些却不能,例如因自然灾害或意外造成的信息资源破坏。不过,通过各种预防措施和后期补救,人们可以通过各种技术手段将网络信息安全问题的危害和损失降到最低点。

1.1.3　网络信息安全的目标

如今,人们开始意识到病毒、黑客、网络犯罪给网络信息安全造成的危害越来越大,害怕自己也会遭受网络攻击,但对网络信息安全的目标却认识不足,仍以为安装了防病毒软件、防火墙,而且数据没有丢失,系统也正常运行就算安全了。很显然,这不能算是真正的网络信息安全。什么才是真正的网络信息安全的目标呢?

网络信息安全通常要求的目标至少有三个,即保密性、完整性和可用性,这也是信息安全的基本要素和安全建设所应遵循的基本原则。如图 1.1 所示。

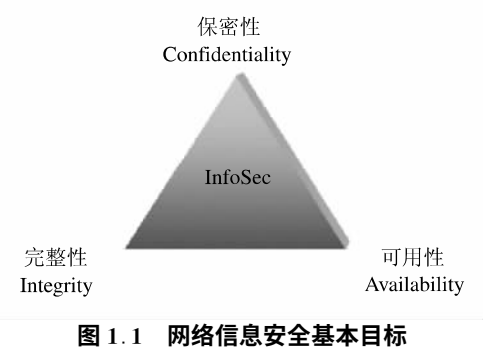

图 1.1　网络信息安全基本目标

(1) 保密性　确保信息不泄露给非授权用户、实体、过程或供其利用的特性。

(2) 完整性　确保信息数据未经授权不能进行改变的特性,即信息在存储或传输过程中保持不被修改、破坏和丢失的特性。

(3) 可用性　确保信息可以被授权实体访问并按需求使用的特性,即当需要时能存取和访问所需的信息。

1.1.4　网络信息安全面临的威胁

所谓网络威胁就是对网络系统缺陷的利用,这些缺陷可能导致非授权访问、信息泄露、资源耗尽、资源被盗或者被破坏等。网络信息安全最大的威胁来自网络信息系统自身的脆弱性,主要包括:在信息输入、处理、传输、存储、输出过程中存在的信息容易被篡改、伪造、破坏、窃取、泄漏等不安全因素;网络信息系统自身在操作系统、数据库以及通信协议等方面存在安全漏洞和隐蔽信道等不安全因素;其他方面如磁盘高密度存储受到损坏造成大量信息的丢失,存储介质中的残留信息泄密,计算机设备工作时产生的辐射电磁波造成的信息泄密,工作人员误操作等人为或偶然事故构成的威胁。网络信息安全的威胁既可以来自内部网又可以来自外部网,其种类有:

(1) 嗅探窃听　在广播式网络信息系统中,每个节点都能读取网上传输的数据,如搭线窃

听、安装通信监视器和读取网上的信息等。网络嗅探可以获得很多有价值的信息。

(2) 假冒欺骗　当一个实体假扮成另一个实体时就发生了假冒。

(3) 流量分析　是指通过对网上信息流的观察和分析推断网上的数据信息,如有无传输和传输的数量、方向、频率等。

(4) 破坏完整性　是指有意或无意地修改或破坏信息系统,或者在非授权和不能监测的方式下对数据进行修改。

(5) 拒绝服务　当一个授权实体不能获得应有的对网络资源的访问或紧急操作被延迟时,就发生了拒绝服务。

(6) 资源的非授权使用　即与所定义的安全策略不一致的使用。

(7) 特洛伊木马　通过替换系统合法程序或者在合法程序里插入恶意代码,以实现非授权进程,从而达到某种特定的目的。

(8) 计算机病毒　随着计算机技术的不断发展和人们对计算机系统以及网络依赖程度的增加,计算机病毒特别是网络病毒已经构成了对计算机系统和网络系统的严重威胁。

(9) 匿名诽谤　利用计算机信息系统的广泛互联性和匿名性,散布错误的消息以达到诋毁某个对象的形象和知名度的目的。

其实,作为网络信息安全隐患,包括网络系统软件自身的安全问题、网络系统中数据库及网络系统本身的安全设计问题、传输线路安全与质量问题、网络信息安全管理问题、其他威胁网络信息安全的典型因素等,归结起来还是由于人为故意和非故意的原因造成的。

需要注意的是,网络信息安全隐患中人的因素是非常关键的,因为人是信息资源的拥有者,信息安全规则制度的制定者、管理者,系统的设计者,因此,来自人的威胁也就是最大的。这里所说的人包括信息系统的管理者、使用者和决策者,信息系统的开发者、维护者以及外部黑客、竞争对手、网络恐怖组织、军事组织或国家组织等。

归纳起来,系统的安全威胁风险常表现为以下几个方面:

(1) 数据传输链路风险　数据在广域网线路上传输,很难保证在传输过程中不被非法窃取、篡改。入侵者在传输线路上安装窃听装置,通过监视网络数据获得敏感信息,造成信息泄密或者通过做一些篡改来破坏数据的完整性。

(2) 网络体系结构的安全风险　入侵者通过探测、扫描网络及操作系统存在的安全漏洞,并利用相应攻击程序对网络发起攻击。

(3) 系统的安全风险　目前的操作系统或应用系统往往留有“后门”,而且系统本身存在诸多安全漏洞,这些“后门”和安全漏洞都将存在巨大的安全隐患。

(4) 应用的安全风险　企业网络系统内部的办公自动化是一个共享资源,员工有意或无意地把硬盘中的重要信息共享就可能造成重要信息的泄密;电子邮件系统存在被黑客跟踪或收到一些特洛伊木马、病毒程序的风险。

(5) 管理的安全风险　管理是网络系统中信息安全得到保证的重要组成部分,是防止内、外网络入侵所必需的部分。没有身份认证和权限认证的网络系统是不安全的。

1.2　网络信息安全体系结构及关键技术

ITU-TX.800 标准将“网络信息安全(Network Security)”进行了逻辑上的分别定义:

(1) 安全攻击　是指损害机构所拥有信息的安全的任何行为。

(2) 安全机制　是指设计用于检测、预防安全攻击或恢复系统的机制。

(3) 安全服务　是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统的安全和信息传输安全的服务。

在网络信息安全体系框架下,安全攻击、安全机制和安全服务之间的关系如表 1.1 所示。

表 1.1　安全攻击、安全机制、安全服务之间的关系

安全攻击						安全服务	安全机制							
释放消息内容	流量分析	伪装	重放	更改消息	拒绝服务		加密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公证
		★				对等实体认证	★	★			★			
		★				数据源认证	★	★						
		★				访问控制			★					
★						机密性	★						★	
	★					流量机密性	★					★	★	
			★	★		数据完整性	★	★		★				
						非否认服务		★		★				★
					★	可用性				★	★			

为了能够有效地了解用户的安全需求,选择相应的安全产品和策略,有必要建立一些系统的方法来进行网络信息安全防范。网络信息安全防范体系的科学性、可行性是其可以顺利实施的保障。网络平台需要网络节点之间的认证、访问控制。应用平台需要有针对用户的认证、访问控制;需要保证数据传输的完整性、保密性;需要有抗抵赖和审计的功能;需要保证应用系统的可用性和可靠性。针对一个网络信息系统,如果在各个系统单元都有相应的安全措施来满足其安全需求,则认为该网络信息系统是安全的。

1.2.1　物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提。物理安全是指保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故、人为操作失误或错误以及各种计算机犯罪行为的破坏的过程,它主要包括以下三个方面:

(1) 环境安全　对系统所在环境的安全保护,如区域保护和灾难保护。

(2) 设备安全　主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

(3) 媒体安全　包括媒体数据的安全及媒体本身的安全。

显然,为了保证网络信息系统的物理安全,除了在网络规划和场地、环境等方面的要求之外,还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而导致泄密的案例已经有很多了,在理论和技术支持下的验证工作也证实了这种截取距离在几百米甚至可达千米的复原显示给计算机系统信息的保密工作带来了极大的危害。为了防止系统中信息的扩散,通常是在物理上采取一定的防护措施,来减少或干扰扩散出去的空间信号。这将成为政府部门、军事部门、金融机构在兴建信息中心时首要设置的条件。为了提高物理安全,可以采

取的措施主要有：

（1）对主机房及重要信息进行存储，收发部门进行屏蔽处理。

（2）对本地网、局域网传输线路传导辐射的抑制。

（3）对终端设备辐射的防范。

1.2.2 网络信息安全

网络信息安全主要包括系统（主机、服务器）安全，如反病毒、系统安全检测、入侵检测（监控）、审计分析等；网络运行安全；备份与恢复应急；局域网、子网安全，如访问控制、网络信息安全检测等。具体保障措施有：

（1）内外网隔离及访问控制系统　在内部网与外部网之间，设置防火墙（包括分组过滤与应用代理）实现内外网的隔离。

（2）内网安全域的隔离及访问控制　通过防火墙来隔离内部网络中的某一个网段与其他网段。这样就能防止影响内部网络中的一个网段的问题穿过整个内部网络传播，限制局部网络信息安全问题对全局网络造成的影响。

（3）网络信息安全检测　定期对网络系统进行安全性分析，及时发现并修正存在的漏洞。

（4）审计与监控　审计是记录用户使用计算机网络系统进行所有活动的过程，用于确定是否有网络攻击的情况。审计信息对于确定问题和攻击源很重要。

（5）网络反病毒　网络反病毒技术包括预防病毒、检测病毒和消毒三种技术。网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁的扫描和监测；在工作站上用防病毒芯片；对网络目录及文件设置访问权限等。

（6）网络备份系统　备份系统的目的是尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。

1.2.3 信息安全

信息安全主要涉及用户身份的鉴别、信息传输的安全、信息存储的安全以及对网络传输信息内容的审计等几方面。可以采取的措施主要有：

（1）信息传输安全　对于在网络系统内信息传输的安全，根据其实际需求与安全强度要求的不同，可以有多种解决方案。如链路层加密、IP 层加密、应用层加密等。

（2）信息存储安全　在网络系统中存储的信息主要包括纯粹的数据信息和各种功能信息两大类。对纯粹数据信息的安全保护，以数据库信息的保护最为典型。

（3）信息完整性鉴别　主要是要明确信息发自谁，以防止假冒以及信息发出后的不可抵赖性。一般采取数字证书和数字签名技术来实现。

1.2.4 网络信息安全关键技术

目前可以利用很多现成的技术来实现网络信息安全，当然，最重要的前提是避免人为因素造成的损失，加强管理，提高安全意识。

为防止攻击，比较有效的方法是实现隔离。隔离的方法有两种：一种是物理隔离，另一种是逻辑隔离。物理隔离的思路就是不安全就不联网，要绝对保证安全；而逻辑隔离的思路是在保证网络正常使用的情况下，尽可能保证安全。物理隔离的思路，源于两台完全不相连的计算机，使用者通过软盘从一台计算机向另一台计算机拷贝数据，有时候大家形象地称之为“数据

摆渡”。由于两台计算机没有直接连接，就不会有基于网络的攻击威胁。当然，这要牺牲有些用户的方便性。物理隔离实现起来最有效的方法就是利用物理隔离网闸。

一种叫做安全隔离网闸的设备可以完全模拟人工拷盘的工作模式，阻断所有网络协议连接，具有最高的安全特性。它能针对文件传输、邮件传输和数据库传输，通过专用的安全协议进行协议分析和内容过滤，可以有效防止病毒代码和恶意程序对网络系统的破坏。如图 1.2 所示。

图 1.2　某型号的安全隔离网闸外观图

不过，由于很多情况下网络信息安全的要求级别没有那么高，因此，相对不重要的网络信息安全防范主要还是利用如下手段来实现的：

(1) 防火墙技术。
(2) 数据加密技术。
(3) 抗攻击网关。
(4) 防病毒网关。
(5) 安全路由器。
(6) 虚拟专用网(VPN)。
(7) 安全服务器。
(8) 电子签证机构(CA)。
(9) 入侵检测系统(IDS)。
(10) 安全数据库。
(11) 安全操作系统。

在上述主要的发展方向和产品种类中，都包含了数据加密的应用，很多的安全功能和机制的实现都是建立在密码技术的基础之上，甚至可以说没有密码技术就没有安全可言。

网络信息安全和数据保护防范措施都有一定的限度，并不是越安全就越可靠。因而，在判断一个内部网是否安全时不仅要考察其安全手段，更重要的是对该网络所采取的各种防范措施，其中不光是物理防范措施，还有人员的素质等其他“软”因素进行综合评估，从而得出是否安全的结论。

信息安全并不是“非黑即白”的绝对值，它实际上存在着许多的灰色地带。对某个应用环境而言，相关的安全机制是够用的，但把同样的机制转移至其他的应用环境时，却可能无法满足应用需求。针对特定场合、特殊需求，在实际运作时选用的安全机制可能会因为方便性、效率、经费、法令限制等原因而有所取舍。一般用户与服务提供端之间，对于如何决定应用系统的安全等级，必须依赖相关契约或法令的规范，提供相应程度的安全机制。

1.3　网络信息安全的标准体系

1.3.1　网络信息安全标准体系及评估要求

网络信息安全的保护涉及人员、技术和法规三个方面，因此，网络信息安全防护体系在总