

面向21世纪

高职高专系列教材

计算机安全 与防护技术

◎张宝剑 主编

◎朱艳丽 审



机械工业出版社
CHINA MACHINE PRESS



面向 21 世纪高职高专系列教材

计算机安全与防护技术

张宝剑 主编

朱艳丽 审



机械工业出版社

网络安全是目前比较热门而且重要的问题。本书完整地介绍了有关网络安全的基础知识和相关法规。全书分 7 章, 主要包括: 网络安全的相关法规、数据加密技术及在网络中的应用、防火墙技术及防火墙的设计与维护、网络病毒与防范措施、黑客入侵的方法与防范、网络安全实现的指导准则等内容。

本书可以作为计算机专业的教材, 也可以供计算机爱好者、网络管理员及安全软件开发人员阅读和参考。

图书在版编目 (CIP) 数据

计算机安全与防护技术/张宝剑主编. —北京: 机械工业出版社, 2003.1
(面向 21 世纪高职高专系列教材)

ISBN 7-111-11365-9

I. 计... II. 张... III. 电子计算机—安全技术—高等学校: 技术学校—教材 IV. TP309

中国版本图书馆 CIP 数据核字 (2002) 第 099062 号

机械工业出版社 (北京市百万庄大街 22 号 邮政编码 100037)

策 划: 胡毓坚

责任编辑: 汪汉友

责任印制: 路 琳

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2003 年 1 月第 1 版·第 1 次印刷

1000mm×1400mm B5·6.875 印张·267 千字

0001-5000 册

定价: 17.00 元

凡购本图书, 如有缺页、倒页、脱页, 由本社发行部调换

本社购书热线电话 (010) 68993821、68326677-2527

封面无防伪标均为盗版

面向 21 世纪高职高专

计算机专业系列教材编委会成员名单

顾问	曾玉崑 王文斌 陈瑞藻 李 奇 凌林海 林 东
主任委员	周智文
副主任委员	周岳山 (常务副主任) 詹红军 陈付贵 穆天保 赵佩华 黄甘洲 武文侠 吕何新
委员	郭曙光 王德年 刘瑞新 陈丽敏 孔令瑜 李 玲 鲁 辉 陶书中 赵增敏 马 伟 孙心义 翟社平 廖常武 于恩普 王春红 王娟萍 屈 圭 汤新广 谢 川 姜国忠 汪赵强 董 勇 梁国浚 张晓婷
秘书长	胡毓坚
副秘书长	陈丽敏 (兼)

出版说明

积极发展高职高专教育,完善职业教育体系,是我国职业教育改革和发展的一项重要任务。为了深化职业教育的改革,推进高职高专教育的发展,培养 21 世纪与我国现代化建设要求相适应的,并在生产、管理、服务第一线从事技术应用、经营管理、高新技术设备运作的高级职业技术应用型人才,尽快组织一批适应高职高专教学特色的教材,已成为各高职高专院校的迫切要求。为此,机械工业出版社与高职高专计算机专业、电子技术专业和机电专业教材编委会联合组织了全国 40 多所院校的骨干教师,共同研究开发了一批计算机专业、电子技术专业和机电专业的高职高专系列教材。

各编委会确立了“根据高职高专学生的培养目标,强化实践能力和创新意识的培养,反映现代职业教育思想、教育方法和教育手段,造就技术实用型人才为立足点”的编写原则。力求使教材体现“定位准确、注重能力、内容创新、结构合理和叙述通俗”的编写特色。

本套系列教材是由高职高专计算机专业、电子技术专业、机电专业教材编委会分别会同各院校第一线专业教师针对高职高专计算机、电子技术和机电各专业的教学现状和教材存在的问题开展研讨,尤其针对目前高职高专教学改革的新情况,分别拟定各专业的课程设置计划和教材选题计划。在教材的编制中,将教学改革力度比较大、内容新颖、有创新精神、比较适合教学、需要修编的教材以及院校急需、适合社会经济发展的新选题优先列入选题规划。在广泛征集意见及充分讨论的基础上,由各编委会确定每个选题的编写大纲和编审人员,实行主编负责制,编委会通过责任编委和主审对教材进行质量监控。

担任本套教材编写的老师们都是来自各高职高专院校教育第一线的教师,他们以高度的责任感和使命感,经过近一年的努力,终于将本套教材呈现在广大读者面前。由于高职高专教育还处于起步阶段,加上我们的水平和经验有限,在教材的选题和编审中可能出现这样那样的问题,希望使用这套教材的教师和学生提出宝贵的意见和建议,以利我们今后不断改进,为我国的高职高专教育事业的繁荣而共同努力。

高职高专系列教材编委会
机械工业出版社

前 言

随着网络技术的发展，特别是 20 世纪 90 年代以来国际互联网的发展，网络安全问题越来越受到人们的重视，网络安全成为计算机网络方面的一个研究热点。

网络安全对人们的工作和生活有着广泛的影响。近几年，随着电子商务的迅速发展，电子通信、电子银行、在线交易已经成为人们日常生活的重要组成部分，这就要求网络服务提供相应的安全措施，以保障广大用户的权益。网络的安全漏洞也为网络黑客们提供了广阔的生存空间。他们所开展的各种各样的攻击，会直接或间接地影响到网络的正常工作和人们的生活。同时，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。这种攻击与反攻击、侵入与反侵入的不断斗争的环境促使网络安全技术得到全面迅速的发展。

在实际的应用中，有多种方式可为网络的安全提供保护。各国也制定了有关网络安全的法规。法规与技术相结合，在一定程度上为网络的安全提供了保证。

本书共分 7 章。第 1 章作为网络安全的概述，介绍了网络安全的目的和功能、网络安全的威胁、网络安全的策略、网络安全的级别以及网络安全的相关法规；第 2 章介绍了相关的加密技术；第 3 章和第 4 章分别介绍了防火墙的技术和设计与维护；第 5 章介绍了病毒的工作原理及病毒实例；第 6 章详细分析了黑客入侵的方法、步骤及相应的应对措施；第 7 章介绍了安全实现指导准则。

本书由张宝剑主编，另外参加编写工作的还有，张复兴、朱坤华由两位同志。由于网络技术发展迅速，书中不足之处希望广大读者批评指正。

作 者

目 录

出版说明

前言

第1章 计算机网络安全 1

1.1 网络安全的概念 1

1.1.1 数据 1

1.1.2 资源 1

1.1.3 声誉 2

1.2 网络安全的目的和功能 2

1.2.1 网络安全的目的 2

1.2.2 网络安全的功能和措施 3

1.3 网络安全的潜在威胁 11

1.3.1 安全威胁的基本概念 11

1.3.2 潜在威胁 13

1.4 网络安全的策略 15

1.4.1 最小特权原则 15

1.4.2 多道防线 15

1.4.3 阻塞点 16

1.4.4 最薄弱环节 16

1.4.5 失效保护机制 16

1.4.6 普遍参与 17

1.4.7 防御多样化 18

1.5 网络安全的级别 18

1.5.1 美国计算机安全级别 18

1.5.2 加拿大计算机安全
级别 20

1.6 网络安全的相关法规 21

1.6.1 信息安全立法 21

1.6.2 国外信息安全立法
概况 22

1.6.3 我国计算机信息系统安全
保护立法情况 23

1.7 小结 24

1.8 习题 24

第2章 数据加密技术 26

2.1 基本概念 26

2.1.1 密码学的有关概念 26

2.1.2 密码体制 27

2.1.3 密码分析 28

2.2 对称密码体制 28

2.2.1 DES 算法 29

2.2.2 托管加密标准 (EES) 36

2.2.3 高级加密标准 (AES) 36

2.2.4 RC4 37

2.3 公开密钥密码体制 37

2.3.1 公钥密码体制概况 37

2.3.2 RSA 公钥系统 38

2.4 数字签名 40

2.5 密钥管理 40

2.5.1 保密密钥的分发 41

2.5.2 公钥分配与证书 41

2.6 小结 41

2.7 习题 42

第3章 防火墙的主要技术 43

3.1 防火墙的概念 43

3.2 防火墙的作用和特性 44

3.2.1 防火墙的作用 44

3.2.2 防火墙的特性 45

3.3 防火墙技术与产品
发展的回顾 46

3.4 实现防火墙的主要
技术 48

3.4.1 数据包过滤技术 48

3.4.2 应用网关技术 51

3.4.3 代理服务技术 52

3.5 小结	56	5.1.4 网络病毒的传播途径	96
3.6 习题	57	5.2 常见的网络病毒	98
第4章 防火墙的设计与		5.2.1 宏病毒	98
维护	58	5.2.2 通过电子邮件传染的 蠕虫病毒	103
4.1 防火墙的体系结构	58	5.3 小结	106
4.1.1 双重宿主主机体系 结构	58	5.4 习题	106
4.1.2 屏蔽主机体系结构	59	第6章 黑客入侵与防范	107
4.1.3 屏蔽子网体系结构	61	6.1 IP 欺骗攻击与防范	107
4.1.4 防火墙体系结构的 组合形式	64	6.1.1 IP 欺骗的原理	108
4.2 内部防火墙	68	6.1.2 IP 欺骗的一般步骤	113
4.3 防火墙选择原则	68	6.1.3 IP 欺骗的防范	118
4.4 防火墙的安全技术分析、 功能评估及维护	72	6.2 端口扫描与防范	120
4.5 防火墙应用中的 新技术	77	6.2.1 有关端口	120
4.5.1 新型防火墙的主要技术与 功能	77	6.2.2 手工扫描常用的网络 相关命令	121
4.5.2 新型防火墙的技术实现 方法	79	6.2.3 使用端口扫描工具	121
4.5.3 新型防火墙的抗攻击 能力	81	6.2.4 一个简单的端口 扫描程序	124
4.6 防火墙技术的发展趋势 与需求展望	82	6.2.5 对端口扫描的防范	127
4.6.1 防火墙的发展趋势	82	6.3 缓冲区溢出与防范	130
4.6.2 防火墙技术的需求 动向	84	6.3.1 缓冲区溢出的危害	131
4.7 个人防火墙软件介绍	85	6.3.2 制造缓冲区溢出	132
4.8 小结	89	6.3.3 利用缓冲区溢出获得 系统 root 权限	135
4.9 习题	89	6.3.4 关于缓冲区溢出的 讨论	143
第5章 网络病毒与防范	91	6.4 拒绝服务攻击	145
5.1 网络病毒概述	91	6.4.1 过载攻击	146
5.1.1 病毒的概念	91	6.4.2 拒绝服务攻击的例子	150
5.1.2 病毒的作用原理	92	6.4.3 防止拒绝服务攻击	153
5.1.3 病毒的分类	94	6.5 网络监听与防范	154
		6.5.1 以太网中可以监听的 原因	154
		6.5.2 网络监听的目的	155
		6.5.3 常用的监听工具	157

6.5.4 怎样探测网络监听	169	7.2.3 违反方案时的响应	200
6.5.5 对于网络监听的防范	170	7.2.4 建立程序以防止安全 事故	202
6.6 口令破解与防范	171	7.3 关于网络安全的一些 技术问题	203
6.6.1 口令破解的可能性	172	7.3.1 网络上应运行何种 服务	203
6.6.2 口令破译器	173	7.3.2 连接	204
6.6.3 各系统的口令破解 方法	173	7.3.3 将要使用何种操作 系统	204
6.6.4 对口令破解的防范	182	7.3.4 建立服务与禁用不 必要的服务	205
6.7 黑客攻击的一般步骤	189	7.3.5 扫描网络查找安全 漏洞	209
6.8 小结	191	7.4 小结	210
6.9 习题	192	7.5 习题	211
第7章 安全实现指导准则	193	参考文献	212
7.1 相关概念	193		
7.2 整体安全解决方案的 规划	194		
7.2.1 建立一个正式的安全 方案	194		
7.2.2 方案特例	197		

第1章 计算机网络安全

随着计算机技术、网络技术以及信息技术的迅猛发展，计算机网络与人们工作和生活的联系也愈来愈紧密。通过网络，人们可以和远在天涯的朋友互发函件；通过网络，人们可以浏览世界各地的报刊杂志，搜索自己所需的信息……。但与此同时人们也发现自己的计算机系统不断的受到侵害，其形式的多样化，令人防不胜防，给有关部门造成了巨大的损失。因此，为使计算机系统和计算机网络系统不受破坏，提高系统的安全性已成为必须解决的问题。因此，每个计算机用户都应该掌握一定的计算机网络安全技术以使计算机系统长时间、安全、稳定地运行。

1.1 网络安全的概念

计算机网络安全问题是一个错综复杂的问题，它涉及到系统故障以及有意或无意的破坏等。为了确保计算机网络安全，需要采取物理措施、管理措施和技术等多方面措施。

计算机网络安全保护对象主要是数据、资源和声誉。

1.1.1 数据

数据有3个独立的特征：保密性、完整性和可用性。其中保密性是头等重要的。每个单位的计算机系统里都会储存一些重要数据，如军事行动计划、产品的设计和配方、财务记录、人事档案等。有高度机密数据的机器很容易在网上被识别出来，换句话说，“黑客”很容易发现想要攻击的目标。

对于那些不需要保密的数据，还要考虑数据的完整性和可用性。如果数据文件被删除一部分，则该数据文件一般不能用，如果数据文件被篡改，则数据文件一般情况下绝对不可用。有时，数据不得不重建，但有时它们是不可重建的，这是因为有些数据是不可复得的。

无论是丢失数据还是数据被篡改，都会使系统遭受损失，有些损失则是在短时间内无法补救的，甚至永远无法补救，这些损失包括其他人员对系统管理者的信任和对其所属机构的信任。

1.1.2 资源

这里所说的资源是指计算机网络的硬件资源和软件资源。大多数用户都想单独使用自己的计算机或向其他的使用者收费使用，对于后一种情况，管理者则需要承

担安全性方面的责任。

入侵者绝非善意的使用者，他们入侵是想完成某一任务，例如大量占用被入侵者的内存、磁盘空间或 CPU 运行时间等。当被入侵者在运行某一程序时，就会因以上原因而无法运行。

计算机的所有者在计算机资源上花费了大量的时间、精力及金钱，因此有权利决定怎样使用这些资源，这样就对计算机系统提出了安全问题的要求。

1.1.3 声誉

有时，入侵者会冒充被入侵者的身份出现在因特网上，做出被入侵者不知道的事情，而这些看起来好像是被入侵者所为。结果可能会导致其他站点或法律机构责问被入侵者为什么正在试图破坏他们的系统，其后果有时候是严重的并往往使被入侵者遭受损失。入侵者也会盗用被入侵者的名义发送电子函件邮寄新闻消息。一般情况下，这些入侵者是故意的，是不可信任的，但即使只有少数人相信，也必然要耗费大量的时间和精力消除其影响，被入侵者和所在机构的形象也可能会因此受到严重损害。

伪造电子函件新闻是很容易的。如果它产生于外部伪造站点，将容易被发现，但如果它来自于一个已经获取站点访问权的入侵者，那么它看起来确实像是被入侵者发的。外部伪造者不能访问的各种细节，一个入侵者却可以访问到这些细节，他可以获取被入侵者全部的电子函件列表，并可以知道被入侵者给谁发过电子函件。

此外，大多数的入侵者会企图将被入侵者的机器连接到其他机器上，这将使下一个受害者以为被入侵者是入侵者。许多入侵者也会利用被入侵者的站点散布盗版软件或色情内容，使被入侵者的名字与盗版、入侵和色情等相联系，要想恢复清白更是不容易的。

总之，网络安全的目的就是最大限度地保障计算机网络不受侵犯，使系统能够正常运行。

1.2 网络安全的目的和功能

1.2.1 网络安全的目的

计算机网络安全就是研究如何保障计算机资源的安全，即计算机的系统资源和信息资源的安全。影响计算机网络安全的主要因素有以下几种：

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、电磁辐射、数据介质安全及火灾报警等。

运行安全，即系统资源和信息资源使用合法。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、运行管理等。

数据安全，即系统的数据或信息完整、有效、使用合法，不被破坏和泄漏。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。

软件安全，即软件（网络软件、操作系统资料）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。

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、路由器的安全等。

1.2.2 网络安全的功能和措施

计算机网络安全问题是一个很复杂的问题，任何时候都不会有一劳永逸的解决措施。因为计算机的安全与反安全会一直地进行下去，故要使计算机网络具有较高安全性，需要将计算机系统的各种安全防护技术（如实体安全防护技术、防电磁辐射泄漏技术、硬软件防护技术、防火墙技术、数据保密变换以及安全管理与法律制裁等）结合使用，对计算机系统进行综合分层防护，从而提高计算机网络的整体防护水平。分层防护的原理见图 1-1，其中最外层是社会层，主要通过法律、管理、伦理道德教育等措施来减少犯罪几率；由外及内，分别是实体安全防护层、电磁防护层、硬软件防护层、通信和网络防护层、数据保密变换层等。

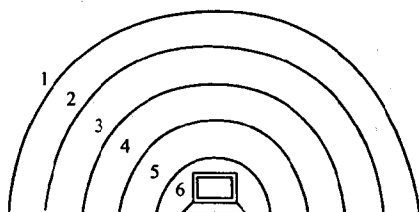


图 1-1 计算机及网络的分层防护

1—社会层 2—实体安全防护层 3—电磁防护层 4—硬软件防护层 5—通信和网络防护层 6—数据保密变换层

加强计算机安全管理的法规建设，建立和健全各项规章制度是保障计算机网络安全的重要一环。利用制定人员的管理制度，加强人员审查，在组织管理上避免单独作业，操作与设计分离等制度和措施降低了作案的可能性。

1. 实体安全防护

为了保障计算机系统的正常工作，首先是保护硬件环境，这包括不间断供电设备、空调、防静电设施和防火设施等。

建立物理屏障，阻止非法入侵者接近计算机系统是行之有效的防护措施。这些措施有进入识别、区域隔离和边界防护等。当今的进入识别技术有密码锁、磁卡等身份识别措施。为了防伪造，新型磁卡也称为“灵巧卡”带有智能化单片机（即微

处理器)。最近又出现了指纹识别、视网膜识别和语音识别等手段,这些手段有效的阻止了非法入侵事件的发生。以上所说的防护都属于边界防护的范畴。而所谓的边界防护是指设置障碍,构造安全警戒区等防护方法。

2. 软件安全环境防护

1978 年的美国佛罗里达计算机犯罪法是世界上第一部计算机犯罪法。首次将计算机犯罪定为侵犯知识产权罪。现在,计算机软件已列入知识产权的范畴,受到法律的保护。对计算机犯罪定罪和量刑产生的威慑力可使有犯罪企图的人产生畏惧心理,使计算机犯罪减少,有利于计算机网络的安全。

建立和健全计算机网络安全各项规章制度,是保障计算机安全的有力措施。另外,加强道德教育对于计算机网络安全也十分重要。

3. 电磁防护

(1) 电磁干扰和兼容 计算机是一种电子设备,在工作时向外辐射电磁波,同时又受到其他电子设备的干扰,这种干扰强到一定程度,就会影响计算机的正常工作。

电磁干扰有两种途径:电磁辐射和电磁传导。电子设备辐射的电磁波通过电路耦合引入到另一台电子设备中引起干扰。电磁传导是通过连接的导线、电源线、信号线等耦合而引起相互之间的干扰。

计算机及其元器件是在一定电磁干扰环境下工作的,所谓电磁兼容性就是电子设备或系统在一定的电磁环境下互相兼顾、相容的能力。如果设备的电磁兼容性很差,在电磁干扰的环境里就不能正常工作;如果是机载、弹载设备就会造成飞机、导弹失事。我国已将电磁兼容性作为强制性标准来执行。

(2) 现代战争与电磁防护 现代战争的重要特征之一是改变了传统的靠硬武器决胜的观念,而广泛采用电子战等作战手段。即以电子侦察、电子伪装和电子攻击等手段,与地面行动相配合,硬杀伤与软杀伤相结合,形成协同作战的整体威力。海湾战争是这方面的典型战例。

从 1991 年的 1 月 17 日开始到 1991 年 2 月 24 日的海湾战争中,由于以美国为首的多国部队事先采用了电子侦察、电子干扰和电子伪装,精确制导与反辐射武器,使伊军通信中断,指挥失灵。因此,在这场仅为 42 天的战争中,多国部队死伤 120 余人,而伊方死伤六七千人;多国部队损失飞机 43 架,而伊方损失 171 架;多国部队损失舰艇 2 艘,而伊方损失舰艇 50 余艘,坦克 3000 多辆,装甲车 1800 多辆,大炮 2000 门。伊方工事和防线半小时被突破。

这个战例说明,以电子信号欺骗和电子干扰为主的软杀伤武器已走向战场。以打钢铁为主的战争正向以打芯片为主的战争转化,如果电子设备没有电磁防护功能,很难取得战争的胜利。

(3) 电磁防护的措施 为提高电子设备的抗干扰能力,除在芯片、部件上提高抗干扰能力外,主要的措施有屏蔽、隔离、滤波、吸波和接地等,其中屏蔽是应用最多的方法。

电磁波经封闭的金属板之后,大部分能量被吸收、反射和再发射,最终传到板内的能量就很小了,这样内部的设备或电路就免受强电磁干扰从而得到保护。

滤波是另一种重要的方法。滤波电路是一种无源网络,它可让一定频率范围内的电信号通过而阻止其他频率的电信号,从而起到滤波作用。在有导线连接或阻抗耦合的情况下,进出线采用滤波器可阻止强干扰。

吸波是采用铁氧体等滤波材料,在空间很小的情况下起到类似滤波器的作用。

隔离是将系统内的电路分别处理,将强辐射源、信号处理单元等隔离开,单独处理,从而减弱系统内部和系统向外的电磁发射。

接地对电磁兼容来说十分重要。它不仅可起到保护作用,而且可使屏蔽体、滤波器等集聚的电荷迅速排放到大地,从而减小干扰,作为电磁兼容要求的地线需单独埋放。

(4) 计算机的信息泄漏 1985 年在法国举办的“计算机与通信安全”国际会议上,荷兰的一位工程师现场演示了用一套稍加改装的设备和黑白电视机还原 1Km 以外的机房内计算机显示屏上的信息。这说明计算机的电磁辐射造成信息泄漏的危险是存在的。

计算机信息泄漏主要是通过传导发射和向空间的发射、辐射传播出去的。由信息泄漏得到的情报比其他方式更为隐蔽、准确和及时,也更为危险。

美、俄等国经多年研究,研究出了“抑制信息处理设备的噪声泄漏技术,简称信息泄漏防护技术(TEMPEST 技术,美国 NACSIM5100A)。20 世纪 80 年代以来,美国市场上陆续出现了一种符合 TEMPEST 标准的军用通信设备,并逐步形成商品化、标准化生产。

TEMPEST 技术是综合性很强的技术,包括泄漏信息分析、预测、接收、识别、复原、防护、测试和安全评估等项技术,涉及到多个学科领域。它是在传统的电磁兼容理论的基础上发展起来的,但是比传统的抑制电磁干扰的要求要高得多,其技术实现上也更复杂。它所关心的是如何避免泄漏出有用的信息,即红信号。一般认为显示器的视频信号,打印机打印头的驱动信号、磁头读写信号、键盘输入信号以及信号线上的输入输出信号等为红信号,须重点保护。

电磁防护层主要是通过种种措施,提高计算机和电磁兼容性,提高设备的抗干扰能力,以使计算机能抵抗强电磁干扰,同时将计算机的电磁泄漏发射降到最低,不致将红信号泄漏出去。

4. 硬件软件防护

(1) 硬件防护 硬件是指计算机系统的物理构成,硬件防护一般是指在计算

机硬件上采取措施或通过增加硬件来防护。具体措施有为计算机加锁、加专门的信息保护卡，例如防病毒卡、防拷贝卡、加插座式的数据变换硬件和安装在并行口上的加密狗等。

(2) 软件防护 软件防护主要指通过计算机软件提供安全防护功能。系统软件是软件的重要组成部分，计算机系统的安全在很大程度上依赖于操作系统本身的安全和它为系统提供的安全防护功能。近年来按照可信计算机安全评估准则（TCSEC）的要求进行安全操作系统的改进，在安全防护方面增加了许多功能，有效地提高了系统的安全性。传统的 UNIX 操作系统经重新设计安全内核，达到了 B 级安全标准。

操作系统提供的安全防卫功能主要有个人身份鉴别、存取控制授权矩阵、隔离控制和监视程序控制等。这几种方法主要用于访问控制和系统隔离，系统要判定用户是否合法，享有何种特权，对计算机资源可进行什么类型的访问操作（读、写运行等），同时规定用户与信息密级和资源类型相适应的授权。另外，通过软件使系统隔离，避免安全隐患的扩散，从而保证信息系统的安全。

在国内外使用很普遍的防病毒软件是软件防护的一个例子。绝大多数网络系统均装有这类防护软件，一开机先扫描，通过后再继续执行。一旦有外来盘插入使用，要先详细检查，无问题后方可进入。

5. 计算机通信及互连网的安全防护

(1) 通信安全 计算机通信安全主要包括：线路安全、传输安全、数据保密变换、辐射安全、技术安全和终端安全。内部和外部通信线路是敌对势力窃取信息的重要目标。为保护线路安全，除采取物理防护措施外，还可采用报警等技术措施。

数据传输必须安全可靠，为此，对传输初始化、测试、校验和纠错等有一系列要求。对注册、语言保密和通信量分析等也要采取相应措施。

网络特别是因特网更加开放，有些防护措施，对网上站点、网上主机和工作站是适合的，而对于互连网上的内部网的安全，则应有更完善的技术手段来保证。

(2) 互连网的安全 防火墙是适应互连网的发展而出现的一种安全防护技术，它是内部网和外部网之间实施安全防范的系统，也是一种访问控制机制。防火墙通常安装在被保护的内部网与互连网的连接点上。从互连网或内部网上产生的任何活动都必须经过防火墙，并由防火墙来确定这些活动是否可以接受。

防火墙的防护规则是：一切未被允许的就是禁止的；一切未被禁止的就是允许的。

6. 密码技术

密码技术又称为数据保密变换，它是计算机系统对信息进行保护的最可靠方法。

密码保护层是计算机安全防护的最内层也是最重要的一层。物理环境防护, 电磁防护, 硬件和软件防护, 通信和网络防护, 可阻止了大部分入侵事件, 但它不是万无一失, 仍有个别入侵会成功, 故计算机系统仍存在着隐患。通过密码技术可将信息屏蔽起来, 虽然极少数人可窃取到信息, 但由于密码技术的保护, 使这些加密信息很难识别, 即使可以识别, 也因要花极大的代价而无实际意义。

密码设计的基本思想是伪装信息, 它使无关人员无法理解信息的真正意义。密码设计的核心是密码算法和密钥。密码算法是一些公式和运算关系等, 密钥是算法中的可变参数。改变了密钥也就改变了明文和密文之间的数学关系。所谓加密就是将明文变成密文, 而解密是将密文恢复为明文。

对于密码算法来说, 衡量其好坏的尺度是保密强度。如果总推不出明文, 此算法即为理论上不可破译。如果推出明文需在时间和经济上付出不可能付出的代价, 则此算法实际上不可破译。

现代密码学的一个基本原则是: 一切秘密寓于密钥之中, 加密算法可以公开, 密码设备可以丢失, 但密钥绝对不可丢失。

7. 网络安全服务

网络安全服务是主要的安全防护措施。下面是五种通用的安全服务。

(1) 认证 认证服务提供了关于某个实体(人和物)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常用方法。

认证是一种重要的安全服务。它是其他安全服务的第一关。认证是对付假冒攻击的有效方法, 它分为两种情形:

1) 身份由参与某次通信连接或会话远端的一方提交。这种情况下的认证服务称作实体认证。这种认证只是简单地认证实体本身的身份, 不会和实体将要进行什么活动联系起来。因此, 它的作用是有限的。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的密钥, 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。

2) 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称作数据起源认证。它认证某个指定的数据项是否来源于某个指定的实体。它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操作而认证他的身份, 而是为了确定被认证的实体与一些特定数据项之间不可分割的联系。

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。其中数据起源认证是保证部分完整性目标的直接方法, 即保证知道某个数据项的真正

起源。

实体认证的一个重要实例是人员认证，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，不同人员之间容易互相替代。在区分单个人方面，可以采用一些特别技术。

(2) 访问控制 访问控制就是拒绝未授权者对计算机网络的任何资源进行访问。未授权访问包括未经授权的使用、泄漏、修改、销毁以及颁发指令等。访问控制直接支持机密性、完整性、可用性以及合法使用的安全目标，它对机密性、完整性和合法使用所起的作用是十分明显的。它对可用性所起的作用取决于对以下几种用户进行有效的控制：

- 1) 影响网络可用性的网络管理指令的颁发者。
- 2) 滥用资源以达到占用资源目的的人。
- 3) 可以用于拒绝服务攻击信息的获得者。

访问控制既是通信安全的问题，又是计算机操作系统的安全问题。由于必须在系统之间传输访问控制信息，所以它对通信协议具有很高的要求。访问控制的一般模型假定一些主动的实体，称为发起者或主体。他们试图访问的一些资源，称作目标或客体。

授权决策控制着哪些发起者在何种条件下，为了什么目的，可以访问哪些目标。这些决策以某一访问控制策略的形式反映出来。访问请求通过某个访问控制机制而得到过滤。一个访问控制机制模型由实施功能和决策功能两部分组成，OSI 访问控制模型（ISO/IEC10181-3 标准）就使用了这些概念，如图 1-2 所示。实际上，这两个组成部分的物理构成可能差别很大。通常，某些构成是将两个组成部分放在一起的，然而，在这些组成部分之间常常要传输访问控制信息，访问控制服务为这一通信提供了保证。

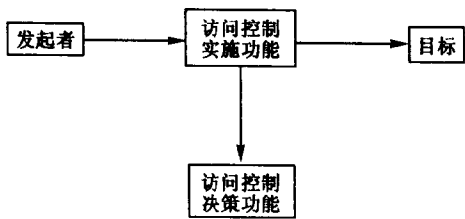


图 1-2 访问控制模型的基本组成

访问控制的另一个作用是保护敏感信息不经过有风险的环境传送。这涉及到对网络的业务流或消息所实施的路由控制。所谓路由控制是指选路规则，选择或绕过指定的网络、连接或中继。访问控制服务的深入讨论依赖于两个因素：访问控制策略的类型和各组成部分的物理构成。

(3) 机密性 机密性服务就是保护信息不泄漏或不暴露给那些未授权的人或