# 计算机网络安全教程

主编 谭伟贤 杨力平

副主编 陈颖 张景生

国防工业出版社

# 计算机网络安全教程

主　编　谭伟贤　杨力平
副主编　陈　颖　张景生

国防工业出版社
·北京·

# 内 容 简 介

本书围绕计算机网络安全这个中心，对计算机信息系统安全保护的基本知识与常用技术作了比较全面的介绍，内容包括计算机网络安全的基本要求、网络安全防火墙、防范黑客攻击、网络安全策略、网络信息加密、数字签名与认证、防治网络病毒、计算机电磁辐射泄漏防护、网络平台安全、网络环境安全、系统安全管理与审计等。

本书力求通俗易懂，以帮助读者克服网络安全技术比较生涩难懂的困难，达到“入门”的目的。本书适合各行业从事计算机网络应用或管理的人士阅读、参考，也可供大专院校有关专业的学生作为辅助教材。

**图书在版编目(CIP)数据**

计算机网络安全教程/谭伟贤，杨力平主编.—北京：国防工业出版社，2001.1
ISBN 7-118-02417-1

Ⅰ.计… Ⅱ.①谭… ②杨… Ⅲ.计算机网络-安全技术-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2000）第 54054 号

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号）
（邮政编码 100044）
北京奥隆印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 12½ 285 千字
2001 年 1 月第 1 版 2001 年 1 月北京第 1 次印刷
印数：1－4000 册 定价：18.00 元

# 前　言

近年来，有关计算机安全以及网络安全的书逐渐增多，有翻译国外的，也有国内专家自己编著的，这些书都各有特点，为各层次的读者提供了宝贵的资料。那么本书的特点是什么呢？主要有以下三个方面：

首先是比较全面。本书以网络安全为重点，兼顾计算机信息系统安全保护的基础理论与知识，内容有我国计算机网络安全水平概况、网络防火墙、黑客问题、网络安全策略、加密和数字签名、电磁辐射泄漏的防护、防治网络病毒、网络平台及网络环境安全、安全管理与审计等。

其次是通俗易懂。网络本身技术性很强，网络安全比较生涩难懂，可能这是初入此道者翻了几本书后的共同心理。本书的特点是紧紧抓住“入门”这个中心，以通俗的语言和清晰的叙述方法，向读者介绍计算机及其网络安全的基本理论、基本知识和常用技术。同时，我们还在每章最后对有关应用方案和产品进行介绍，以使读者形成具体认识，帮助对基本理论和技术的理解，也帮助读者能尽快进入实用状态。此外，由于网络安全方面的许多资料是翻译过来的，因此国内有关专著和文献往往对同一个事物有不同的称谓和描述，常使读者感到困惑。本书在查阅多方资料的基础上，尽量使其趋于一致，或者将各种提法罗列出来让读者能够进行较全面的了解。

第三是资料新颖。计算机应用技术及网络技术的发展是非常迅速的，为了使本书能反映出最新的理论和技术，我们参阅了大量最新的资料，特别是许多资料来自 Internet 上的专业网站，以尽量靠近新知识、新技术的前沿，因此本书的资料来源比较新。此外，对于一些与网络安全有关的网站，以及安全产品的厂商，本书都尽量列出它们的网址，便于读者直接联系。

根据本书的特点，我们认为本书较适合各行业从事计算机网络应用或管理的入门者阅读、参考，也可供大专院校有关专业的在校学生作为辅助教材。在向读者们热情推荐本书的同时，我们也认识到计算机网络技术及应用可谓“博大精深”，而网络安全技术又号称是高科技中的高科技，发展十分迅速，以我们的现有水平很难在本书中全面、准确地反映出来，因此书中会有疏漏甚至错误，在此也恳请读者及有关专家批评指正。

在本书的编写过程中，得到了杨俊、朱震、李曼宁、李丹俐、苏菠、许阳、卢志辉、叶国泉、黄月玲、海俊、陈毅坚、陈志坚、陈肖琼、苏炽才、胡建瑜、赵国峰、陈坚、张明、容志林等同志在选题、编目、录入、绘图、修改、审校、制版等方面的具体帮助，在此一并表示衷心感谢。

编　者

2000 年 9 月

# 目　录

# 第1章 概 述

在20世纪后期，信息化的浪潮席卷全球。今天，世界正经历着以计算机网络技术为核心的信息革命，人类正在迈向一个崭新的时代。这场信息革命从技术广度上来说，可与蒸汽机的发明、电气化的出现相提并论，但从影响上来说，这场革命的意义却深远得多。信息网络将成为我们这个社会的神经系统，将改变人类传统的生产、生活方式。

今天的计算机网络不仅有局域网(LAN)，而且还通过网桥(Bridge)、网关(Gateway)、调制解调器、基带数传机、专用或公用交换机以及各种通信控制设备，实现了网络扩充与异型网互联，形成了跨越城市、国家的广域网(WAN)。计算机网络提供了资源的共享性，提高了系统的可靠性，通过分散工作负荷提高了工作效率，并且还具有可扩充性。这些特点使得计算机网络深入到科研、文化、经济与国防的各个领域，推动了社会的发展。但是，这种发展也带来了一些负面影响，比如，网络的开放性增加了网络安全的脆弱性和复杂性；信息资源的共享和分布处理增加了网络受攻击的可能性。目前，Internet网络延伸到全球五大洲每一个角落，覆盖的范围和密度还在不断地增大，这使得人们难以分清它所链接的各种网络的界限，难以预料信息传输的路径，更增加了网络安全控制和管理的难度。就网络结构因素而言，Internet包含了星型、总线型和环型三种基本拓扑结构，而且众多子网异构纷呈，子网向下又连着子网。结构的开放性带来了复杂化，为了实现异构网络的开放性，不可避免要牺牲一些网络安全性。这给网络安全带来很多无法避免的问题，从网络协议因素来看，大型网络的发展使单一的网络协议环境成为过去。而用户为保护原有的网络基础设施投资，使各种协议能够互联，对网络协议的兼容性要求越来越高，这在给厂商和用户带来方便和利益的同时，也带来了安全性的问题：在一种协议下运行的有害程序可能会很快传播到整个互联网；在一种网络结构和协议下实现以多种结构和协议的访问，也将危及信息的安全。从地理上来说，Internet遍布世界各地，所链接的各种站点地理位置错综复杂、点多面广，通信线路质量难以保证，可能对传输的信息数据造成失真或丢失，也给专事搭线窃听的间谍和黑客以可乘之机。

随着全球信息化的迅猛发展，国家的信息安全和信息主权已成为越来越突出的重大战略问题，关系到国家的稳定与发展；就企业来说，网络信息对于在日益激烈的市场竞争中是否取胜非常关键。因此，网络的安全问题正在引起国家、信息界乃至社会公众的注意和重视。网络应用技术日新月异，而对网络安全技术的研究，是在20世纪70年代中后期，由于出现了较严重的计算机犯罪和其他安全问题，才有少数国家开始研究和采取一些措施。所以，网络安全技术远远落后于网络应用技术的发展水平。1983年美国国防部公布了著名的桔皮书，对多用户计算机系统的安全等级的划分进行了规定，即“可信计算机系统评估标准”。在我国，计算机安全工作虽然始于1981年，但是不要说对网络安全的研究，就是对计算机安全的研究也只是在1989年计算机病毒出现后，才广泛引起计算机界的重视和社会的

关注。美国有关专家认为，当今计算机应用技术和计算机安全技术的发展差距，如同用显微外科手术治病与用放血术治病的差距。因此，我们必须下大力气研究网络的安全问题，以期能尽量适应网络应用技术发展的需要，通过保护网络的安全，使网络得以健康发展。

## 1.1 计算机网络安全要求

我国正处在计算机联网以及各行各业上网（Internet）的热潮中，人们在享受网络所提供的各种好处的同时，必须研究如何解决计算机网络的安全问题。计算机安全已发展为计算机科学的子学科，而计算机网络安全的内涵更加丰富，它至少涉及到法律学、犯罪学、心理学、经济学、应用数学和计算机基础科学、加密学及审计学等相关学科。同时，计算机网络安全已经派生为一门新的技术，越来越多的组织和个人在研究、应用这一技术，并推出一系列的产品，逐步形成了一项产业。

### 1.1.1 计算机网络安全的定义和内容

由于网络的定义有许多种，所以各种关于网络安全的定义也不同。有的定义说：网络安全就是保护网上保存和流动的数据，不被他人偷看、窃取或修改。也有的定义认为：网络信息安全是指保护信息财产，以防止偶然的或未授权者对信息的泄漏、修改和破坏，从而导致信息的不可信或无法处理。综合起来看，我们认为，计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，信息数据的保密性、完整性及可使用性受到保护。网络安全的主要目标是要确保经网络传送的信息，在到达目的站时没有任何增加、改变、丢失或被非法读取。要做到这一点，必须保证网络系统软件、应用软件系统、数据库系统具有一定的安全保护功能，并保证所有网络部件，如终端、调制解调器、数据链路等的功能不变，而且只有那些被授权的人们才可以访问。网络的安全性问题实际上包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而保护网络的信息安全是最终目的。就网络信息安全而言，首先是信息的保密性，其次是信息的完整性。另一个与计算机网络安全紧密相关的概念是拒绝服务。所谓拒绝服务主要包括三个方面的内容：系统临时降低性能；系统崩溃而需人工重新启动；因数据永久性丢失而导致较大范围的系统崩溃。拒绝服务是与计算机网络系统可靠性有关的一个重要问题，但由于计算机系统种类繁多，如果结合进来与计算机安全一起研究比较困难，所以拒绝服务一般不作为计算机安全研究的主要课题。

近年来利用广泛开放的物理网络环境进行全球通信已成为时代发展的趋势，但是如何在一个开放的物理环境中构造一个封闭的逻辑环境来满足部门或个人的实际需要，已成为必须考虑的现实问题。开放性的系统常常由于节点分散、难于管理等特点而易受到攻击和蒙受不法操作带来的损失，若没有安全保障，则系统的开放性将会带来灾难性的后果。网络的开放和安全本身是一对矛盾，如果我们想“鱼和熊掌”都能兼得，就必须对开放系统的安全性进行深入和自主的研究，找到并理清实现开放系统的安全性所涉及的关键技术环节，并掌握设计和实现开放系统的安全性的方案和措施。

在计算机网络中，安全威胁来自各个方面，甚至有些是由于我们自身的失误而产生的。影响并危害计算机网络安全的因素分自然因素和人为因素两类。自然因素包括温度、湿度、灰尘、雷击、静电、水灾、火灾、地震、空气污染和设备故障等因素。人为因素又有无意和故意

之分，例如，由于误操作删除了数据的疏忽或过失；人为故意的破坏，如黑客行为。由于网络中存储和流动着许多高度机密数据和电子财富，这早已是政治间谍、商业间谍及黑客窥测和行动的目标。网络安全的内容大致包括四个方面，见图 1-1。

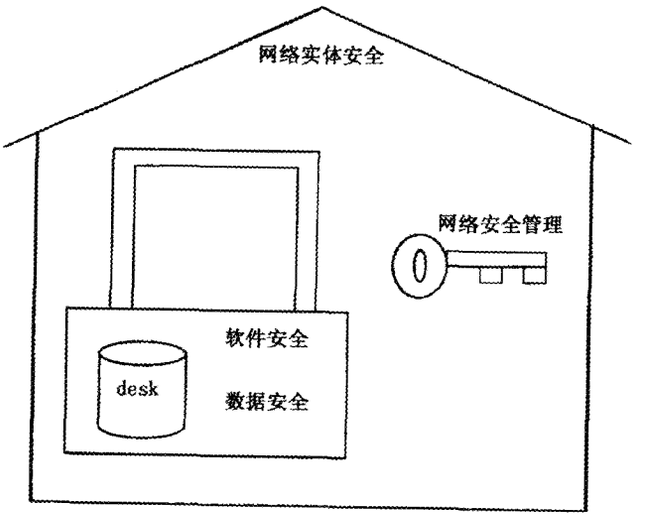


图 1-1　网络安全的内容

(1)网络实体安全

如计算机机房的物理条件、物理环境及设施的安全，计算机硬件、附属设备及网络传输线路的安装及配置等。

(2)软件安全

如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、不受病毒的侵害等。

(3)网络中的数据安全

如保护网络信息数据的安全、数据库系统的安全，保护其不被非法存取，保证其完整、一致等。

(4)网络安全管理

如运行时突发事件的安全处理等，包括采取计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等内容。

### 1.1.2　衡量网络安全的指标

衡量网络安全的指标是保密性、完整性和可使用性(三者简称 CIA)，具体如下：

(1)保密性

是指网络中有保密要求的信息只能供经过允许的人员以经过允许的方式使用。从技术上说，任何传输线路，包括电缆(双绞或同轴)、光缆、微波和卫星，都是可能被窃听的。对于电缆的窃听，可以是接触式的，也可以是非接触式的，即通过电磁感应或利用电磁辐射来窃听，现在已有灵敏度很高的特殊屏蔽设备。无线传输可以用天线接收，即使像微波那样的视

距传播，由于波束有一定的宽度，天线也可以放在射线中央以外地区接收。

(2)完整性

它是指网络中的信息是安全、准确与有效的，不因种种不安全因素而改变信息原有的内容、形式与流向。造成信息完整性破坏的原因也可分人为和非人为的两种。非人为因素包括通讯传输中的干扰噪声、系统硬件或软件的差错等。人为因素包括有意和无意两种，前者有非法分子对计算机的侵入，合法用户越权对网络内数据的处理，以及隐藏的破坏性程序对数据的破坏等。计算机病毒、时间炸弹、逻辑炸弹、逻辑陷井等都属于隐藏的破坏性程序。无意危害如操作失误或使用不当。对于大多数网络来说，对信息完整性的破坏是网络安全的主要危害。此外信息完整性是一个很广泛的问题，例如，分布式数据库中关于并发性操作或者对多个数据副本的更新操作所引起数据一致性问题；又如由于系统的设计不完善造成使用不当或操作失误所引起的数据完整性问题等，它涉及到数据库安全、分布处理、软件可靠性等领域。

(3)可使用性

它指网络资源在需要时即可使用，不因系统故障或误操作等使资源丢失或妨碍对资源的使用。网络可用性还包括具有在某些不正常条件下继续运行的能力。对网络可用性的影响包括合法的用户不能正常访问网络的资源，以及有严格时间要求的服务不能得到及时的响应等。影响网络可用性的因素包括人为与非人为两种。前者有非法占用网络资源、切断或阻塞网络通讯、病毒或"蠕虫"降低网络性能、甚至使网络瘫痪等等。后者有灾害事故(火、水、雷击等)和系统死锁、系统故障等等。

### 1.1.3 保护网络安全的主要措施

除了要制定和实施一系列的安全管理制度外，保护网络安全的技术措施主要有：

- 改进、完善网络运行环境；
- 堵塞网络系统和用户应用系统的技术设计漏洞；
- 防止网络和计算机系统口令被偷窃；
- 实施访问控制(存取控制)，进行身份认证，防止协议出错、认证出错；
- 防止电磁辐射造成信息泄漏；
- 建立网络安全防火墙，并以安全为目的优化网络结构；
- 定时进行系统备份和数据备份；
- 采用信息传输加密算法和电子签名，加强密钥管理等。

此外，在网络安全管理的基础上要进行审计，要定期进行风险分析，找出薄弱环节，采取措施予以消除。

## 1.2 计算机网络安全隐患

网络的安全隐患是多方面的。从网苗组成结构上分有计算机信息系统的，有通信设备、设施的；从内容上分有技术上的和管理上的；从管理上分又有内部的和外部的，等等。具体来说主要有五个方面的问题，如图 1－2 所示。

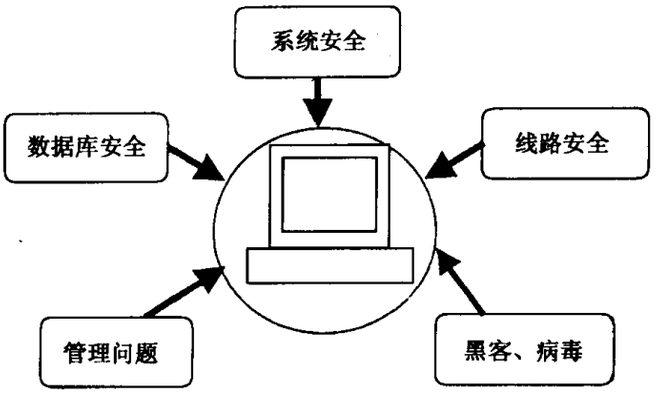


图 1-2　网络安全的隐患

### 1.2.1　网络系统软件自身的安全问题

网络系统软件的自身安全与否直接关系网络安全，网络系统软件的安全功能较少或不全，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都等于给危害网络安全的人和事留下许多“后门”。例如，美国微软公司就经常针对已发现的系统“破绽”发布“补丁”程序。同时，在同一系统软件中，低版本的往往比高版本的在安全性能方面差了许多，所以在服务器上要注意尽量使用高版本的操作系统，并应使用系统软件所能提供的最高安全级别。另外，值得注意的是操作系统的许多缺省值都已被黑客们盯上了，往往被用来作为侵入网络的突破口，所以应尽量避免使用系统缺省值。此外，还要注意的有：

(1)操作系统的体系结构造成其本身是不安全的，这也是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务，都可以用打“补丁”的方式进行动态连接。许多 Unix 操作系统的版本的升级、开发都是采用打补丁的方式进行的。这种方法既然厂商可以使用，那么黑客也可以使用，同时这种动态连接也成为计算机病毒产生的好环境。

(2)操作系统的一些功能，例如，支持在网络上传输文件的功能，包括可以执行的文件映象，即在网络上加载程序等，必然带来一些不安全因素。

(3)操作系统不安全的另一原因在于它可以创建进程，甚至支持在网络的节点上进行远程进程的创建与激活，更重要的是被创建的进程可以继承创建进程的权力。这一点与上一点(可在网络上加载程序)结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。若再加上把这种间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，系统进程与作业监视程序就都无法监测这些黑客和间谍软件的存在。

(4)操作系统运行时一些系统进程总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去，这都是黑客可以利用的。

(5)操作系统要安排无口令入口，这原本是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽信道。

(6)Internet 和 Intranet 使用的 TCP/IP(传输控制协议/网际协议)以及 FTP(文件传输协议)、E-mail(电子邮件)、RPC(远程程序通信规则)、NFS(网络文件系统)等都包含许多不安全

的因素，存在着许多漏洞。

### 1.2.2 网络系统中数据库的安全设计问题

网络中的信息数据是存放在计算机数据库中的，供不同的用户来共享。数据库存在着不安全性和危险性，因为在数据库系统中存放着大量重要的信息资源，在用户共享资源时可能会出现以下现象：授权用户超出了他们的访问权限进行更改活动；非法用户绕过安全内核，窃取信息资源等。因此提出了数据库安全问题，也就是要保证数据的安全可靠和正确有效。对数据库数据的保护主要是指针对数据的安全性、完整性和并发控制三方面。

数据的安全性就是保证数据库不被故意的破坏和非法的存取。数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果。并发控制即数据库是一个共享资源，在多个用户程序并行地存取数据库时，就可能会产生多个用户程序并发地存取同一数据的情况，若不进行并发控制就会使取出和存入的数据不正确，破坏数据库的一致性。

所以在数据库设计时，必须考虑到这些问题。通常可采取一系列的安全策略和安全机制，其中主要是解决存取控制问题。可是对数据的存取控制还不足以对数据库用户进行约束，所以还要增加作业授权控制，把作业授权控制结合到安全策略中，并用自主型和强制性的存取控制来处理用户对数据的访问。而作业授权控制是处理用户对作业以及作业对数据的访问，这种作业授权控制既提供了高可靠性，又提供了应用的灵活性。

我们以著名的数据库 Oracle 和 Fox 或 dBASE 为例来说明。Oracle 数据库系统是一个非常有影响的分布式数据库系统，它不仅有国内广泛使用的微机版本，而且还支持许多不同的操作系统。Oracle 数据库系统体系非常庞大，在此，我们仅以 Oracle for NetWare 为例来说明其良好的自身保护机制。Oracle 是通过保护数据库的数据单元表(table)来保护信息资源不被其他程序进行非授权访问，从而达到保护自身的目的。Oracle 的 table 存储方式是由若干 table 组合在一起，以一个大文件的形式存放在 Novell 网络服务器的 Oracle 目录内的。这个文件的结构和加密方法对外均不公开，因而，其他用户程序是无法破解这些 table 信息的，而且 Oracle 对外也不提供访问的接口。相比之下，Fox 或 dBASE 的自身保护机制就差得多，甚至可以说没有一点自身保护机制。众所周知，Fox 或 dBASE 的 table 存放在以 DBF 结尾的文件里，而结构完全是公开的。存放在 DBF 文件内的信息没有任何加密处理，非授权用户可以不通过 Fox 规定的方式访问 DBF 文件，因而很易受到外来程序的攻击。这一点希望能引起所有基于 Fox 或 dBASE 建造的网络信息系统，尤其是金融、财务系统的管理人员的注意，对其每天都要运行的系统的安全性给予高度重视。

### 1.2.3 传输线路安全与质量问题

尽管在同轴电缆、微波或卫星通信中要窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通讯线路。

同时，无论采用何种传输线路，当线路的通信质量不好时，将直接影响联网效果，严重的时候甚至导致网络中断。例如，市内电话线路，主要电气指标有直流电气性能指标(环阻、绝缘电阻)；交流特性(线路衰耗、线路衰耗交流频率特征)；交流特性阻抗等。当通信线路中

断，计算机网络也就中断，这还比较明显。而当线路时通时断、线路衰耗大或杂音严重时，问题就不那么明显，但是对通信网络的影响却是相当大，可能会严重地危害通信数据的完整性。为保证好的通信质量和网络效果，就必须要有合格的传输线路，如，在干线电缆中，应尽量挑选最好的线对做为计算机联网专线，以得到最佳的效果。

### 1.2.4 网络安全管理问题

从加强安全管理的角度出发，可以认为，实质上网络安全首先是个管理问题，然后才是技术问题。你也许花了不少钱买了安全设备，但如果你将它束之高阁，或不按它的安全规范合理操作，认为有了安全的设备就会安全，而没有在落实上下功夫，那么再好的设备也不安全。

世界上现有的信息系统绝大多数都缺少安全管理员，缺少信息系统安全管理的技术规范，缺少定期的安全测试与检查，更缺少安全审计。我国许多企业的信息系统已经使用了许多年，但计算机的系统管理员与用户的注册大多还是处于缺省状态。

另一方面，也可以说网络的安全问题是天生的，这是由于“整体大于部分之和”的原因：网络由各种服务器、工作站、终端等集群而成，所以整个网络天然地继承了它们各自的安全隐患。各种服务器各自运行着不同的操作系统，各自继承着自身系统的不同安全特性。随着计算机及通信设备组件数目的增大，积累起来的安全问题将十分复杂。

这意味着要制定一个组织内部的有效的安全管理策略。如某公司的信息应当由管理者们作出决策，确定哪些信息是可共享的，哪些信息是内部机密，不得泄露，以免对公司利益造成损害。

通常安全管理领域涉及两类要求：一是安全管理，防止未授权者访问网络；另一个是管理安全(security of management)，防止未授权者访问网络管理系统。尽管这两种要求都十分重要，但该领域被认为不如故障管理、配置管理和性能管理那样迫切。随着计算机网络应用的深入，网络覆盖面越来越大，甚至于有些网络已成为全球网络，如 Internet，网络上信息的安全性越来越重要，网络安全管理也将成为网络管理中的重要领域。

安全管理必须回答下列基本问题：需要保护什么？为什么需要保护？怎样保护？何时保护？在哪里保护？显然上述问题有的涉及实现技术，而有的是管理者的决策。另外，安全性和使用方便性又是一对矛盾，两者不可兼得，强调了安全性，使用方便将受影响；强调使用方便，则安全性可能减弱，这也需要管理者作出决策。国际标准化组织(ISO)把网络管理划分为五个领域，分别是：故障、性能、配置、记账和安全。“故障管理”负责检测或发现异常的网络运转，隔离并控制网络问题。“性能管理”负责分析网络出错率及网络吞吐率，以建立合理、优化的网络运行状态。“配置管理”负责检测物理的和逻辑的配置，了解和控制网络状态。“记账管理”负责搜集资源、处理资源和利用数据。“安全管理”负责控制各种对网络的访问。

此外，对网络运行的环境、操作人员的管理也是网络安全管理的重要方面。不得不正视这样的一个事实，网络用户大多数不具备计算机的专业知识，他们只是将计算机视为一个工具，由于他们缺乏安全操作的常识或对安全不够重视，他们在安全操作方面的失误往往造成对网络的侵害，如将上网口令取为自己或亲朋的姓名、生日、出生地等易猜信息，或者将口令随意标在机器上、机器旁的纸片上及自己的记事簿上，或贴在机房里。再如，有多少用户在

完成一天的工作后，会将工作站锁上呢？有多少用户在暂时离开办公桌，去开一个短会、去吃饭或去卫生间时会关闭应用系统呢？当一个系统未关闭而被非法用户侵入时，它的全部权力和钥匙将被无保留地非法盗用。虽然我们无法完全模仿入侵者如黑客们的全部手段，但必须正视这一事实：我们工作活动的空间正是黑客们游荡、窥测的地方。

### 1.2.5 其他威胁网络安全的典型因素

主要有以下几方面：

- 计算机黑客(将在后面的章节专门介绍)。
- 内部人员作案，有的员工可能会利用工作机会报复上司；此外如果系统管理员也成了黑客那麻烦就大了。
- 窃听。同轴电缆、双绞线、光纤或无线方式引入了新的物理安全暴露点，被动方式如搭线窃听或主动方式的如无线仿冒；利用计算机通信设备天然存在的电磁泄露进行窃取活动，也是一个重要的安全隐患。
- 部分对整体的安全威胁，任一单一组件的失密都可能造成整个网络的安全失败。
- 程序共享造成的冲突，共享同一程序可能会造成死锁、信息失效或文件不正确的开关状态。
- 对互联网而言可能有更多潜在的威胁，即使各网均能独立安全运行，联网之后，也会发生互相侵害的后果。
- 计算机病毒。由于网络的设计目标是资源共享，所以网络是计算机病毒滋生和传播的理想家园。

## 1.3 我国计算机网络安全概况

我国在20世纪80年代特别是进入90年代以来，计算机网络应用飞速发展，网络以其独特的优越性日益深入社会各方面并影响到国民经济、政府事务、科研教育事业等各行各业。现实中各种资金、财物和社会资料信息乃至个人隐私等都转化为计算机数据在网络上流通，网络正在逐步成为整个国家政府机构运转的命脉和社会活动的支柱。

### 1.3.1 我国网络安全技术水平

我国的网络安全技术虽然与世界先进水平有不小的差距，但毕竟已经起步并形成相当的规模，与发展中国家相比具有一定的水平。

**1. 规范网络安全保护及安全产品的管理和检测认证**

这方面的工作得到国家的重视，近年来进展较快，主要有：

(1)制定了一系列有关计算机安全的国家标准，并产生了一批有关计算机安全的规范性技术文件。国家标准主要有：《计算机信息系统安全专用产品分类原则》(GA163－1997)、《计算机机房用活动地板技术条件》(GB6650－86)、《计算机场地安全要求》(GB9361－88)、《计算机场地技术条件》(GB2887－89)、《电子设备雷击保护导则》(GB7450－87)、《信息技术设备的