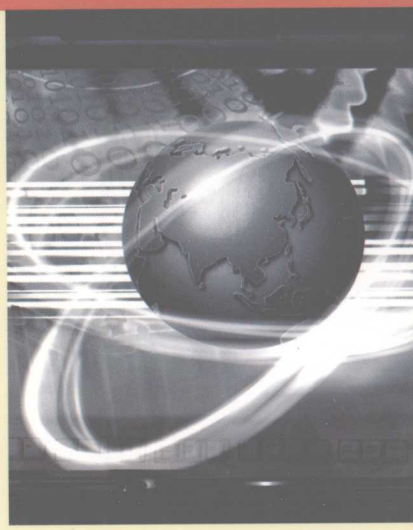
高等学校教材 · 计算机系列



Introduction to Information Security

信息安全概论

洪 帆 崔国华 付小青 编著

华中科技大学出版社
http://press.hust.edu.cn

高等学校教材 · 计算机系列

Introduction to Information Security

信息安全概论

洪 帆 崔国华 付小青 编著

华中科技大学出版社

图书在版编目(CIP)数据

信息安全概论/洪　帆　崔国华　付小青　编著
武汉:华中科技大学出版社,2005 年 9 月
ISBN 7-5609-3449-8

Ⅰ. 计…
Ⅱ. ①洪…　②崔…　③付…
Ⅲ. 计算机-信息安全
Ⅳ. TP309

信息安全概论　　洪　帆　崔国华　付小青　编著

责任编辑:沈旭日　　封面设计:潘　群
责任校对:刘　飞　　责任监印:熊庆玉

出版发行:华中科技大学出版社
武昌喻家山　　邮编:430074　　电话:(027)87557437

录　　排:华中科技大学惠友文印中心
印　　刷:湖北新华印务有限公司

开本:787×1092　1/16　　印张:14.25　　字数:315 000
版次:2005 年 9 月第 1 版　　印次:2005 年 9 月第 1 次印刷　　定价:19.80 元
ISBN 7-5609-3449-8/TP・576

内 容 提 要

本书是作者在多年从事计算机信息安全课程的教学和多年承担信息安全的研究、开发项目的基础上完成的。它系统地论述了计算机信息安全的基本概念、原理、技术和应用。主要内容有：访问控制、密码学、安全审计、数据库安全、网络安全、隐通道和计算机系统的安全评估标准等。

本书可作为高等院校计算机、信息安全、通信等专业本科生的教材使用，也可供从事与信息安全相关专业的教学、科研和工程技术人员参考。

前　言

随着网络与数据库技术的迅速发展及其应用的不断广泛和深入，社会对信息和信息技术的依赖性不断增强，信息安全已受到使用信息和使用信息技术的个人、机构和团体的高度关注，已关系到国家政治、军事、经济等各个方面乃至全社会的安全。因此，培养从事信息安全的专门人才已成为高等学校的一项重要任务。这也是编写本书的目的。

本书是作者在华中科技大学多年从事计算机信息安全课程的教学和多年承担信息安全的研究、开发项目的基础上完成的，比较全面、系统地论述了信息安全的基本概念、理论和基本技术。全书由以下两部分组成。

第一部分：信息安全的基本理论与技术。这一部分包括访问控制、密码学、安全审计、隐通道的分析与限制。访问控制和密码是信息安全的两大支撑技术，是对信息实施机密性、完整性保护，制止和检验系统中冒充、伪造、篡改和权限滥用等攻击的主要技术手段。在访问控制部分，系统地介绍了传统的自主访问控制、强制访问控制和基于角色的访问控制，并重点介绍了 BLP 多级安全的策略模型。在密码部分，全面地介绍了密码的基本理论，传统的对称密码、公钥密码、序列密码和哈希函数，并介绍了常用的几种鉴别技术。

第二部分：信息安全技术的应用。这一部分重点介绍了访问控制技术和密码技术在数据库安全和网络安全中的应用。数据库安全部分重点讨论了如何利用访问控制技术和密码技术保护数据库系统中数据的机密性、完整性和防止越权访问。网络安全部分重点讨论了传输加密、PKI、防火墙、IPSec。为了使读者对信息系统安全有全面的了解，最后还介绍了国内外关于计算机系统安全的一些评估标准。

本书由华中科技大学计算机信息安全研究室组织编写，洪帆教授负责全书的整体规划和结构设计。洪帆教授编写了第 1、2、4、5、7 章，崔国华教授编写了第 3 章，付小青副教授编写了第 6 章。研究室的其他教师根据自己的教学经验和体会对本书的编写也提出了有益的建议。本书在编写过程中参考了国内外许多文献和书籍，也从其他同行的工作中得到了启发，在此一并表示感谢。

在本书出版之际，感谢华中科技大学计算机学院的领导为作者提供了良好的研究和教学环境。对华中科技大学出版社对本书的出版所作的大量工作表示衷心的感谢。

由于编者水平所限，书中难免有些错误和不足之处，敬请读者和同行专家指正。

作　者

2005 年 6 月

目　录

第 1 章

概　述

伴随着科学技术的飞速发展，信息已成为推动社会前进的巨大动力。利用计算机和网络对信息进行收集、加工、存储以及交换等，越来越成为各行各业必不可少的手段，计算机已经渗透到了社会生活的各个方面，各种信息系统的建立和使用造成我们对计算机，尤其是对数据库和网络的事实上的依赖。但是，由于数据库中存储的数据、网络上传输的数据都是具有一定价值的信息，对这些信息的非法访问、窃取、篡改等行为必然导致计算机安全问题的出现。

20 世纪 80 年代末期，一场计算机病毒危机席卷全球，人们在震惊之余第一次意识到他们精心构建的计算机系统是如此的不堪一击。随着计算机和网络技术的广泛应用，计算机及其网络系统的这种脆弱性暴露得更加充分。计算机犯罪案件迅猛增加，已日益成为一种社会隐患。事实上，计算机系统的脆弱性是其本身所固有的。因此，从计算机诞生的那一天起，实际上就产生了对计算机系统安全进行研究的需要。

1.1　信息系统面临的主要威胁和系统的脆弱性

计算机信息系统是由计算机及其相关和配套的设备、设施和网络构成的，是按照一定的应用目标和规则对信息进行采集、加工、存储、传输和检索等处理的人机系统。信息系统可能遭受到各种各样的威胁，只有知道了系统可能受到的威胁以后，才能对其进行有效的防范。因此，在设计和开发安全的信息系统之前，必须探明系统可能受到的威胁。

1.1.1　信息系统面临的主要威胁

威胁信息系统安全的因素是多方面的，对于不同的应用环境，不同的威胁对系统的危害程度往往也是不同的。

1. 从总体看威胁信息系统安全的主要类型

(1) 窃取

威胁源未经许可却直接或间接获得了对系统资源的访问权，从中窃取有用的数据或骗取某种服务。最常见的例子是敏感信息在有意或无意中泄漏给了未授权的实体，如非法拷贝程序或数据文件。威胁源通过窃取口令获得合法用户的身份后，也可在系统中非法窃取所需要的信息。

未经许可的个人依靠窃听的方法从网络中获得数据的可能性也是存在的，有如下几种不同的窃听方法。

① 搭线窃听：利用硬线连接，对通信线路上各次传输的信息进行截收。

② 电磁窃听：利用无线电传输进行接收。例如，对无线电和微波传输，或对从电子设备辐射出来的带有信息的电磁能等进行截收。

③ 声音窃听：对人的语音或者由打印机和发送设备发出的声波进行截收。

(2) 篡改

威胁源虽然未经许可，但成功地获得了对系统某项资源的访问权并更改该项资源。如删除消息的全部或一部分；插入一些无意义或有害的消息；修改信息的流向、次序、内容或形式；更改数据的值，修改某个程序以使其完成一项特定的功能，甚至还可能格式化硬盘、更改硬件等。某些情形的更改可以用简单的措施检测出来，而一些更精妙的更改却很难发现或检测。

(3) 伪造

威胁源在未经许可的情形下，在系统中产生出虚假的数据或服务。例如，电子商务中，威胁源可能希望在网络通信系统中加上假的交易，或者在现有的数据库中增加记录。

(4) 拒绝服务

威胁源使系统的资源受到破坏或不能使用，从而使得数据的流动或所提供的服务被中止。

用户的误操作、软硬件出现故障等均可能引起系统内的数据或软件的破坏，因而使得计算机不得不停止工作。隐藏在计算机中具有破坏性的病毒程序被激活后，可能会毁掉系统中某些重要的数据，甚至可能删除系统中的所有数据且使其无法恢复，更严重的可能导致整个系统的瘫痪。又例如，一些不法分子通过断电设置障碍，采用纵火、爆炸、盗窃通信设备等手段导致计算机系统的硬件遭到破坏，使计算机及通信系统无法正常工作。

此外，在网络通信中还可能出现以下几种情况。

(5) 重放

在网络通信中重放以前截收到的过时的信息，使收方落入陷阱。

(6) 冒充

一个实体假冒另一个实体的身份是一种常见的网络攻击手段。例如，在甲、乙双方通信时，可能是丙在冒充乙的身份与甲通信，而甲并不知道，由此引起甲受到经济上甚至政治上的损失。

(7) 抵赖

在网络通信中，用户可能为了自身的利益，否认自己曾经有过的行为，如否认发出过信息（如否认他发出的转账信息）或者否认收到了信息。

2. 从威胁源看威胁信息系统安全的主要类型

以上种种的威胁，从威胁源来看，又可分为两类，一类是由合法用户的操作失误或系统中软硬件故障引起的，另一类则是敌对分子或不法分子有意制造的对信息系统的攻击，以达

到个人的某种目的。后一类情形称之为“计算机犯罪”(Computer Crime)。广义地说,计算机犯罪是指一切“与计算机有关的犯罪”。具体地说,凡是故意篡改、毁坏或非法使用计算机数据、程序或计算机各种设备(包括通信设施)的非法行为都是计算机犯罪。它大致可分为以下两类。

(1) 以计算机系统资源为破坏对象的犯罪

其破坏方式有以下3种。

① “硬”攻击手段:利用物理方法,如使用炸弹、燃烧物或其他工具直接毁坏计算机的设备以至整个系统,或利用断电、盗窃计算机中的部件等方法造成计算机无法正常工作。

② “软”攻击手段:作案者利用自己所具备的计算机知识,对计算机系统中存储的程序、数据进行非法篡改、删除和破坏,使系统瘫痪或无法工作。这种软攻击造成的破坏和影响程度远比硬攻击大得多,而且隐蔽性很强,难以发现,是目前和今后对计算机系统攻击和破坏的主要手段。例如,在计算机中施放计算机病毒就是这种攻击的一个例子。1988年11月,美国康奈尔大学研究生莫里斯制造的计算机蠕虫事件造成6000台与Internet网络系统连接的计算机,包括美国国家航空航天局、军事基地和主要大学的计算机停止运行,直接经济损失达9600万美元。

③ 使用强电磁场干扰计算机的工作,销毁计算机系统磁性介质中存储的信息,这也是一种神不知、鬼不觉的破坏活动。

(2) 以计算机系统为工具的犯罪

这类罪犯大多是对计算机及网络技术十分精通或对计算机信息系统的应用业务非常熟悉的人。他们打入计算机及其网络系统,窃取其中的机密信息;修改系统中的程序以达到贪污或诈骗钱财的目的。例如,1978年美国某银行的计算机技术顾问,在掌握了银行当天的通行密码后,通过银行的自动转账系统,把1020万美元转到他的瑞士银行的账户中,从此过上挥金如土的生活。后来,当联邦调查局告诉该行的副总经理时,后者竟一无所知。又例如,美国某公司的一名计算机工作人员,在公司工资程序中设计了一段程序,一旦工资单中没有他的名字(即被解雇),该程序便启动,而该程序一旦启动,就会销毁计算机系统中的全部数据,从而使公司蒙受巨大损失,以此来迫使公司不得不以高薪继续聘用他。

恶意程序如病毒、蠕虫、特洛伊木马、逻辑炸弹等都是人为编制的一类特殊的程序。它们通常在用户不经意的情况下潜入系统,一旦激活便危害或破坏系统,其表现形式有多种多样。如破坏磁盘上的数据和文件;自身不断繁殖,抢夺系统资源,使系统的处理能力下降,运行速度变慢,造成网络堵塞甚至崩溃。20世纪90年代初期,计算机病毒被人们引入战争用来作为战争的武器。美国在海湾战争期间,派特工人员将带有病毒的芯片嵌入伊拉克防空系统的新型打印机中,使伊拉克防空指挥中心的主计算机指挥失灵。计算机病毒在军事上的应用实际上引入了电子战这种新型的战争形式。它利用计算机病毒袭击敌方的军事指挥系统,甚至电力、交通、医疗、通信等民用系统,使敌方全面处于瘫痪,从而赢得战争的胜利。

1.1.2 信息系统的脆弱性

以计算机为核心的信息系统面临如此之多的威胁，反映出信息系统本身存在一些固有的弱点和脆弱性。它的脆弱性主要表现在以下几方面。

1. 硬件设施的脆弱性

除难以抗拒的自然灾害外，温度、湿度、尘埃、静电等都可以影响计算机系统的正常工作。

计算机系统工作时能够辐射出电磁波，任何人都可以借助并不复杂的设备在一定的范围内收到它，从而造成信息的泄露。这种电磁辐射在任何电子设备中都是存在的。

在一块小小的磁盘上或光碟上，可以存储大量的数据信息，而它们可以很容易放在口袋里带出办公室，数据存储的高密度为入侵者窃取信息带来了便利。

另外，这些存储介质也很容易受到损坏(有意或无意)，造成大量信息的丢失。

保存在存储介质上的数据可能会将存储介质永久地磁化，因此存储介质上的信息有时擦除不净或不能完全擦除掉，使得介质上留下可读的痕迹，这些信息一旦被利用就可能产生泄密。

另外，大多数计算机操作系统中，删除文件时仅仅只将文件名删除，并将相应的存储空间释放，而文件的内容还原封不动地保留在存储介质上，利用这一现象入侵者也可以窃取机密信息。

当获得单个、孤立的信息时，它的价值往往不大，但如果将大量相关的信息聚集在一起，经过筛选和分析，则可显出这些信息的重要性。计算机的特点之一就是能收集大量的信息并对其进行自动、高效的处理，这种聚生性可被入侵者利用来窃取他感兴趣的机密信息。

2. 软件系统的脆弱性

计算机信息系统的软件可分为3类：操作平台软件、应用平台软件和应用业务软件。它们以层次结构形式组成信息系统的软件体系。操作平台软件处于最底层，支持着上层软件的运行。因此，操作平台软件的安全是整个信息系统安全的基础，它的任何风险都将直接危及到应用平台软件和应用业务软件的安全。应用平台软件在维护自身安全的同时，必须为应用软件提供必要的安全服务。应用业务软件处于顶层，直接与用户打交道。对系统的许多攻击都是通过应用业务层来实施的，它的风险直接反映了系统的安全风险。

在软件的设计与开发过程中往往存在许多错误、缺陷和遗漏，从而形成系统的安全隐患，而且系统越大、越复杂，这种安全隐患就越多。据有关资料估计，微软开发的操作系统Windows的各种版本，平均每100行代码大约要出现0.5～1个错误或缺陷。

目前市场上尚无任何一个大型操作系统或数据库管理系统可以做到完全正确无误没有缺陷，所以这些系统的厂商都要定期地推出新的版本，其中包括数以千计修改过的语句和代码。这些改动大多数是为了纠正系统中的错误或弥补其缺陷而进行的。这些系统的设计者永远无法充满自信地宣布已经找到了系统中所有的漏洞。另一方面，入侵者们多

数不会公布他们的发现，因此，当你将重要的敏感信息委托给一个大型操作系统或网络中的一个计算机时，你没有理由不为你的信息的安全担忧，尤其是当这些信息对入侵者有足够的价值时。

虽然任何操作系统和数据库管理系统都有缺陷，但绝大多数系统是可用的，可以基本完成其设计功能。这就如一个墙上有洞的房间，虽能居住，却无法将盗贼拒之门外。

信息系统中后门是普遍存在的，它可能是生产厂家或程序员在生产过程中留下的，也可能是黑客入侵后在其中设置的。利用后门可以在程序中建立隐蔽通道，植入一些隐蔽的恶意程序、进行非法访问，达到窃取、篡改和破坏信息的目的。

3. 网络通信的脆弱性

网络系统中，通信线路很容易遭到物理破坏，也可能被搭线窃听，甚至于插入、删除信息。无线信道的安全性更加脆弱，因此通过未受保护的外部线路可以从外部访问到系统内部的数据。

资源共享是建立计算机网络的基本目标之一，但这也为系统安全的攻击者利用共享的资源进行破坏活动提供了机会，也为攻击者利用资源共享的访问路径对其他非共享资源进行攻击提供了机会。

计算机网络是一个复杂的系统，网络的可扩展性使得网络的边界具有不确定性，这使得网络的管理变得十分困难，构成了对网络安全的严重威胁。

信息传输时，一个节点到另一个节点可能存在多条路径，一份报文在从发送节点到达目标节点之间可能要经过若干个中间节点，这种路径的不确定性和中间节点的不确定性，使得仅有起始节点和目标节点的安全保密性还不足以保证信息的安全。

数据库技术和网络特别是 Internet 技术的兴起、发展和广泛应用极大地促进了社会信息化的进程，它使得信息可以超越时间和空间的界线达到最大限度的共享。现在，无论你在地球上什么地方，也无论什么时候，只要轻点一下计算机鼠标，就可以获得许许多多来自不同地方和部门的信息。人们在享受技术进步为我们工作、生活带来的这种方便和效率的同时，也感受到了它所带来的对系统中信息安全的威胁。当前，多平台、充分集成的分布式信息系统成为最流行的处理模式，而集中、分布相结合的处理方式也很受欢迎。21 世纪的信息系统将建立在庞大、集成的网络基础上，而在新的信息系统环境中，由于移动计算的普及，存取点将大大增加，从而信息系统的薄弱环节将分布更广。事实上，现代计算机领域中的任何一个大的技术进步都可能对计算机系统自身的安全构成一种新的威胁，所有这些威胁都需要研究出新的方法和技术来予以消除。

1.2 信息系统的安全

现代信息技术的飞速发展为社会带来了巨大的效益，高速计算机和高速网络的逐步政用化、商用化、军用化和民用化反映当今社会对信息及信息技术的巨大依赖性。信息已成为

人类宝贵的资源，它关系到国家的机密和企业的发展，甚至关系国家和企业的生死存亡。正因为信息在人类社会活动、经济活动中起着越来越重要的作用，因此信息的安全日益受到社会越来越广泛和深刻的重视。

所谓信息系统的安全，是指对于信息系统中的硬件、软件及数据进行保护，防止它们因偶然或恶意的原因而遭到破坏、更改或泄漏。为此，信息系统在获取、存储、处理、传输和控制信息的过程中，要建立和采取一些技术上和管理上的安全保护措施。

1.2.1 从保护对象考虑信息系统的安全

信息系统安全从需要保护的对象考虑，可分为外部安全和内部安全。外部安全是指构成信息系统的计算机硬件、外部设备以及网络通信设备的安全，使其不会丢失或受到毁坏，能为系统提供正常的服务。内部安全是指信息系统中程序、数据和服务的安全，使其不被破坏，更改和泄漏。无论是内部安全还是外部安全，信息系统安全的最终目标是要使得信息在系统内的任何地方、任何时间和任何状态下保持其安全性。相对来说，维护外部安全比维护内部安全简单一些，它主要是通过物理保护、加强管理和法律的手段来加以防范。但是对于内部安全来说，仅有上述保护措施是不够的，还必须在技术上采取一系列的措施来防范对系统中信息的攻击。

1.2.2 从保护方法上考虑信息系统的安全

从对信息系统安全的保护方法来考虑，信息系统安全可分为以下 4 类。

1. 物理安全

造成系统不安全的因素很多，如自然灾害，环境干扰等。因此，计算机应安置在安全可靠的地方，能防火、防水、防雷击、防盗、防尘、防电磁干扰等。例如，建立防护围墙、安装避雷设备、安装防电磁泄漏的屏蔽设备等。但是，仅仅使用物理安全控制措施不能解决分布式系统的安全问题，随着计算机网络节点的不断扩充，物理安全的作用在不断减小，我们很难保证任何系统都有完备的物理保护措施。

2. 人事安全

造成系统不安全的因素还可能来自于工作人员失误和管理不严。另外，如果内部工作人员入侵或者内部工作人员与外部人员勾结起来进行破坏，则会对信息系统构成特别严重的威胁，正所谓“家贼难防”。因此，在人事上必须加强管理，如派专人警卫，防止坏人对系统进行破坏或盗窃。严格对工作人员的审查，要求工作人员忠实可靠，制定工作人员必须遵守的规章制度，减少工作中的失误。

3. 法律安全

系统的不安全因素更多的是来自于人为的破坏，包括对硬部件及对软件、数据的破坏和

窃取。入侵者的主观愿望虽然各异，但对信息系统破坏是相同的。除了加强安全管理之外，还应借助于法律手段来对信息系统实施保护。自 1946 年世界上第一台计算机问世后，直到 1973 年，瑞典才率先制定了世界上第一部国家性的《瑞典国家数据保护法》，并成立了国家数据监察局负责这方面的工作。

随后，美国、法国、英国、德国、加拿大和日本等几十个国家，相继制定了有关数据安全和计算机犯罪的法律和法规。

美国是世界上拥有计算机及网络最多、应用最广泛、普及程度最高的国家，也是计算机犯罪最严重的国家，因而拥有较多的针对计算机犯罪的法律。除 31 个州均已制定了这方面的法律外，在联邦法律中，与计算机犯罪有关的就有：1974 年的《个人秘密法》、1978 年的《防止向国外的不正当支付法》、《资金电子调拨法》、《金融秘密法》、1986 年的《计算机欺诈和滥用法》、《电子通信秘密法》、1987 年的《计算机安全法》、1989 年的《计算机病毒消除法》等等。在这些法律中规定：利用计算机获取非法利益；非法得到计算机系统的服务；用非法手段侵入计算机系统和网络进行盗窃、破坏、篡改数据和文件，或扰乱系统功能；利用计算机或计算机技术知识和技巧窃取金钱、数据和信息等行为，均为计算机犯罪，根据情节将处以罚款、监禁或两罚并用。现在美国国会制定的对付计算机犯罪的联邦法律有 3 种，一是《计算机病毒防治法》、二是《计算机保护法》、三是《计算机网络保护法》。

我国政府也十分重视计算机信息系统的安全，1992 年，我国颁布了《计算机软件保护条例》，又颁布了《中华人民共和国计算机信息系统安全保护条例》，在这之后，又陆续颁布了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国公众多媒体通信管理方法》、《国际联网安全保护管理方法》，并在《刑法》中增设了关于计算机犯罪的条款。

4. 技术安全

技术安全是指计算机系统本身在运行过程中，采用具有一定安全性质的硬件、软件来实现对信息的安全保护，以使得在整个系统中，在一定程度上甚至完全可以保证系统在无意或恶意的软件或硬件攻击下仍能使得系统内的信息不被破坏、增加、丢失和泄漏。

随着数据库和网络技术的迅速发展和广泛应用，国家的政治、军事机密和财富高度集中在各种信息系统中，窃取或破坏这些信息已成为当今社会犯罪分子的主要攻击目标。因此，保护信息系统中信息的安全实际上已成为保护信息系统安全的最重要的目标。在技术层面上，对信息系统安全的种种保护方法就是适应系统的这种安全需要而产生的。

在这里，信息主要是指存放在信息系统中的程序和数据。信息安全则是指这些程序和数据在被存储、处理、执行和传输中的安全，主要包括以下几个方面。

(1) 保密性

信息的保密性是指保护信息使之不被未得到授权的实体所获取，即防止信息在非授权情况下的泄漏。保密性是信息系统是否安全的一个重要标志。随着 Internet 网络的联通，信息可以跨地区、跨国界地共享，信息保密性的问题变得更为突出。

(2) 完整性

信息的完整性是指信息在未被授权的情形下，保持不被篡改、不被破坏和不丢失的特

性，并且能够判别数据是否已被改变。它可分为软件完整性和数据完整性。

软件的优点是无论在开发还是在实用的过程中都可以随时更改以使系统具有新的功能，但这种灵活易变性给系统的安全带来了威胁。因此，选择值得信任的系统设计者是一个非常重要的问题，一个不忠实的设计者可以在软件中留下陷阱或圈套，以备将来修改软件对系统进行攻击。计算机病毒通过附加一部分病毒程序代码到系统或应用软件上，从而进行病毒传播，如果对软件有一个较好的完整性保护措施，那目前绝大部分病毒就不能蔓延。我们需要采用软件测试工具来检查软件的完整性，并保证这些软件不会被轻易地修改。

数据的完整性是应用计算机系统进行信息处理的用户，特别是商业部门和金融部门的用户十分关心的一个问题，也是怀有恶意的人进行攻击的主要目标之一。

(3) 可用性

信息的可用性是指当被授权用户需要时，能访问到所需要的信息资源，防止由于人为或非人为因素造成系统的拒绝服务。诸如，暂时降低系统性能、系统崩溃而需人工重新启动、数据永久性的丢失，在网络环境下破坏网络和有关系统的正常运行等，均可造成信息资源不能按照需要供用户使用。

(4) 可控性

可控性是指可以在授权范围内控制信息的流向及行为方式，对信息的传播及内容具有控制的能力。为保证可控性，首先需要对用户进行身份验证，其次要控制谁能访问系统中的数据以及以什么方式访问，最后要将用户的活动记录下来，便于查询审计。

(5) 抗抵赖性

抗抵赖性是指信息的行为人要对自己的行为负责，不能抵赖自己曾有过的行为，如不能否认自己发出过或收到过对方的信息，这在商业和金融系统中是十分重要的。

(6) 可靠性

可靠性是指系统在运行过程中，抗干扰(包括人为、机器及网络故障)和保持正常工作的能力，即保持工作的连续性和正确性的能力。

总之，信息安全的宗旨是，不论信息处于动态还是静态，均应该向合法的服务对象提供准确、及时、可靠的信息服务，而对其他任何人员或组织，包括内部、外部以至于敌方，都要保持最大限度的信息的不可接触性、不可获取性、不可干扰性和不可破坏性。

1.3 信息安全的主要技术

信息系统是为用户提供信息服务的，信息系统安全的最终的目的就是为用户提供安全的信息服务，因此，信息安全是整个信息系统安全的核心。

信息系统中信息的安全，依赖于系统本身的安全，或者说首先构成信息系统的各种计算机硬件、通信设备必须安全，没有丢失和被破坏。在此基础上，如何保证系统中信息的安全，使其具有保密性、完整性、可用性、可控性和抗抵赖性，除了在管理上和法律上可以给予保护