XINXI YU WANGLUO ANQUAN JISHU JICHU

# 信息与网络安全技术基础

主编 王述洋 黎粤华 胡艳英


东北林業大學出版社

# 信息与网络安全技术基础

主　编　王述洋　黎粤华　胡艳英

东北林业大学出版社

**图书在版编目（CIP）数据**

信息与网络安全技术基础/王述洋，黎粤华，胡艳英主编．—哈尔滨：东北林业大学出版社，2005.11

ISBN 7-81076-819-0

Ⅰ．信…　Ⅱ．①王…②黎…③胡…　Ⅲ．信息网络-安全技术　Ⅳ．TP 393.08

中国版本图书馆 CIP 数据核字（2005）第 130935 号

**责任编辑：杨秋华**

**封面设计：彭　宇**

NEFUP

**信息与网络安全技术基础**

Xinxi yu Wangluo Anquan Jishu Jichu

主编　王述洋　徐粤华　胡艳英

东北林业大学出版社出版发行

（哈尔滨市和兴路 26 号）

东北林业大学印刷厂印装

开本 787×960　1/16　印张 15　字数 280 千字

2005 年 11 月第 1 版　2005 年 11 月第 1 次印刷

印数 1—2000 册

ISBN 7-81076-819-0

TP·67　定价：25.50 元

# 内 容 简 介

本教材较全面地介绍了信息与网络安全技术的基础知识，主要内容包括信息与网络安全技术的主要研究领域与关键技术、网络威胁与安全策略、网络安全协议、信息安全的数学基础、安全网络体系结构与模型、信息安全解决方案、数据加密技术、网络加密技术、密码算法、密钥管理与分发、操作系统安全、数据库安全、电子商务安全、计算机病毒理论、“防火墙”技术、实现安全服务的方法以及常用网上可利用的安全信息资源与工具等。

本书可作为信息安全工程、计算机、电子信息、通信工程、信息管理、电子商务等本科专业的教材和博士生、硕士生的教学参考书，也可供从事相关专业教学、科研和工程技术人员参考。

# 前 言

当代社会信息无所不在，没有人能摆脱信息的影响，信息是赢得竞争的前提，信息就是金钱和财富。因此，安全、及时、可靠、有效的信息，不论是对一个国家、一个企业，还是对个人，都是至关重要的。

计算机与网络技术的日益普及，以及现代网络技术的开放性、共享性，对人们进行信息的生产、加工、处理、储存、传输和使用都带来了巨大的方便，但与许多其他科学技术一样，在给人们带来方便的同时也带来了一些严重的问题。例如，网上欺骗、黑客攻击、网上洗钱、网上冒充、网上抢劫、网上病毒等无所不在，以至于使人们对来自于网上的任何一则信息都不能够相信它是真实的。可以说，信息安全已成为影响当代人类社会生活乃至一个国家安全和生死存亡的关键因素之一。因此，每一个生存在当今信息时代的公民和集团，信息与网络安全知识是其保护个人或集团机密信息、自身利益和财产安全的必备知识。

信息安全的问题主要集中在信息系统中，是一个涉及面宽广而又错综复杂的问题。威胁信息安全的因素很多，有自然灾害、各种故障以及各种有意或无意的破坏等。为了确保信息系统的安全，需要从多方面着手，采取各种措施，比如物理措施、管理措施、技术措施、教育措施等。基于计算机与通信技术相结合的现代信息网络系统，是一种有着广泛应用的信息传输系统，其安全性非常重要，特别是以 Internet 为代表的计算机通信网络正在成为未来全球信息系统的最重要的基础设施，如果它的安全性解决不好，将会直接影响国家安全和社会稳定。

从 Internet 的发展来看，从最初是为预防战争对军事指挥系统的毁灭性打击提出的课题，到后来发展到在科研教育的校园环境中解决互联、互通、互操作的技术问题。由于初期片面地追求网络开放性和信息共享性的缘故，使 Internet 的发展忽略了信息安全的问题。20 世纪 90 年代后，Internet 走上了社会应用和商业应用，商业应用的需要使人们很快就意识到忽视安全的严重性。尤其是在网上拥有利益的时代，一些不良行为从另一方面向人们揭示了信息系统的脆弱性，导致人们对信息与网络安全的空前重视。

首先人们意识到的是信息保密，这是古今中外战争的情报军事手段和政府专用技术，几乎人人皆知。可是到了当代信息社会，以 0、1 比特串编码，

信息在网上传输，连个“信封”都没有，电子邮件都是“明信片”，没有什么秘密可讲。而有些信息是需要保密的，这就是信息安全中的机密性需求。

在传统社会中，不相识的人们相互建立信任需要介绍信，并且在上面签名盖章。但是在电子信息环境中如何签名盖章，如何知道信息真实的发送者和接收者是谁，怎么知道信息是真实的，并且在法律意义上做到责任的不可抵赖，这就成为人们归纳的信息安全中的完整性和非否认性需求。

人们还认识到信息和信息系统都是它的所有者花费巨额代价建设起来的。但是，也存在着由于计算机病毒或者其他人为的原因可能造成的对主人的拒绝服务，被他人滥用。这就是信息安全中的可用性问题。

由于在社会中存在着不法分子和不法行为，各国之间也时有由于意识形态和利益冲突造成的敌对行为，政府对社会的监控行为（如搭线监听犯罪分子的通信）在社会广泛使用信息安全设施和装置时可能受到严重影响，于是出现了信息安全中的可控性问题。

本书着重从信息与网络安全基础知识角度出发，针对信息与网络的安全需求，较系统地阐述了解决信息与网络安全的一些关键技术和实现方法，同时也介绍了一些实用的信息安全标准和安全协议。本教材由王述洋、黎粤华、胡艳英任主编，梁颖红、谷志新、宋佳音任副主编。其中，第一章、第二章由王述洋编写；第三章、第七章、第九章由黎粤华编写；第四章由宋佳音编写；第五章由谷志新编写；第六章、第八章由胡艳英编写；第十章由梁颖红编写。全书由王述洋统稿。

本教材的特点是将信息安全理论和技术，特别是密码理论与技术融于信息网络实际应用之中，旨在让从事信息安全理论研究的学者对信息与网络安全知识有一个基本的了解和掌握，使其为进一步从事信息与网络安全工作或深入研究信息与网络安全技术奠定基础；同时让从事信息安全系统和产品开发的人员了解信息安全中的关键理论和技术，以设计和开发出更好、更安全的系统和产品。如能达到这一目标，笔者将无比欣慰。

由于时间仓促，加之笔者专业水平有限，本教材中的疏漏和谬误在所难免，敬请读者批评指正。

作　者

2005 年 8 月于哈尔滨

# 目 录

# 1 信息与网络安全概论

## 1.1 信息安全问题的由来及其严重性

### 1.1.1 信息和网络已成为现代社会的重要基础

当今世界正步入信息化、数字化时代，信息无所不在、无处不有。国与国之间变得“近在咫尺”。计算机通信网络在政治、军事、金融、商业、交通、电信、文教等各行各业中的作用日益增大。在 Internet 上，除了电子邮件、新闻论坛等文本信息的交流与传播之外，网上电话、网上传真、电子商务和视频等通信技术也在不断地发展与完善，正在为用户提供丰富多彩的网络与信息服务，用以网络为基础和手段来获取信息、交流信息正成为现代社会的一个新特征。在某种意义上讲，信息就是时间、财富、生命，就是生产力。

随着全球信息基础设施和各个国家的信息基础的逐渐形成，社会对计算机网络的依赖日益增强。为此，人们不得不建立各种各样的信息系统来管理各种机密信息和各种有形、无形财富。但是这些信息系统都是基于计算机网络来传输和处理信息，实现其相互间的联系、管理和控制的。如各种电子商务（Electronic Commerce）、电子现金（Electronic Cash）、数字货币（Digital Cash）、网络银行（Network Bank），乃至国家的经济、文化、军事和社会生活等方方面面，都日趋强烈地依赖网络这个载体。可见，信息和网络已成为现代社会的重要基础，以开放性、共享性和无限互联为特征的网络技术正在改变着人们传统的工作方式和生活方式，也正在成为当今社会发展的一个新的主题和标志。

### 1.1.2 信息安全与网络犯罪危害日趋严重

事物总是辩证统一的。信息与网络科技进步在造福人类的同时，也给人们带来了新的问题和潜在危害。计算机网络的产生就像一个打开了的潘多拉魔盒，使得新的邪恶——计算机与网络犯罪相伴而来。

第一，计算机联网是与开放系统同时发展起来的。开放系统的标志是开

放系统互连（Open System Interconnection，OSI）模型的提出。自从20世纪70年代以来，OSI模型得到了不断发展和完善，从而成为全球公认的计算机通信协议标准。除了OSI标准外，另一些标准化组织也相继建立了一些开放系统网络协议，其中最有影响力的是Internet协会提出的TCP/IP协议。通过围绕开放系统互连所开展的标准化活动，使得不同厂家所生产的设备进行互联成为现实。然而，在网络开发之初，由于人们考虑的是系统的开放性和资源共享的问题，忽视了信息与网络技术对安全的需要，结果导致网络技术先天不足——本质安全性非常脆弱，极易受到黑客的攻击或有组织的群体的入侵。可以说，开放性和资源共享性是网络安全问题的主要根源。与此同时，系统内部人员的不规范使用或恶意行为，也是导致网络系统和信息资源遭到破坏的重要因素。以下是一些有关网络攻击和信息破坏的一些案例报道，从中可见现实中的信息与网络安全问题是多么严重。

1988年11月2日，美国有6 000多台计算机被病毒感染，致使Internet不能正常运行。这是一次非常典型的病毒入侵计算机信息网络事件。在这次事件中有5个计算机中心和12个地区节点，链接着政府、大学、研究所和拥有政府合同的约25万台计算机遭受了攻击，直接经济损失达9 600万美元。这个病毒程序设计者是康奈尔（Cornell）大学的年仅23岁的研究生罗伯特·莫里斯（Robert T. Morris）。罗伯特·莫里斯设计的病毒程序利用了系统本身存在的缺陷。由于罗伯特·莫里斯成了当时入侵ARPANET的最大的电子入侵者，因而被批准参加康奈尔大学的毕业设计，并获得哈佛大学Aiken中心超级用户的特权。他也因此被判3年缓刑，同时罚款1万美元并强制其进行了400小时的社区服务，以示惩罚。

1996年8月17日，美国司法部的网络服务器遭到黑客入侵，“美国司法部”的主页被改为“美国不公正部”，司法部部长的照片被换成了希特勒的照片，司法部的徽章被换成了纳粹党徽，并下载了一幅色情女郎的图片作为司法部部长的助手，最后还留下了很多攻击美国司法政策的言论。

1993年6月，美国一家医院链接到网络上的一些体检数据被黑客恶意篡改成癌检阳性，结果导致许多被测者误认为自己患上了癌症，造成一片混乱和恐慌。

1996年12月29日，一黑客入侵到美国空军的全球网网址并对其主页进行肆意篡改，其中空军介绍、新闻发布等内容被替换成一段简短的黄色录像，并宣称美国政府所说的一切都是谎言。这次黑客入侵迫使美国国防部不得不关闭了80多个军方网址。

1998年4月25日下午，一神秘黑客非法侵入中国公众多媒体信息网

(CHINANET) 贵州站点的 www 主机，将“贵州省情”的 Web 页面改换成一幅不堪入目的淫秽画面。同年 8 月 22 日，一黑客攻击了江西省中国公用多媒体信息网（169 台），结果导致整个系统瘫痪。

1998 年 6 月 16 日，上海某信息网的 8 台服务器被黑客攻击，黑客破译了该网络大部分工作人员的口令和 500 多个合法用户的账号和密码，其中包括两台服务器上超级用户的账号和密码。

1998 年 10 月 27 日，刚刚开通的“中国人权研究会”网页，被“黑客”严重篡改。

2004 年的“冲击波”病毒，先后使全球 50 多万台电脑瘫痪，并且遭受感染的电脑会自动注册到该病毒制造者杰弗里·李·帕森的网站（t33kid.com），帕森可以方便地跟踪和监视遭受感染电脑的“一举一动”，令遭受感染的电脑无任何安全可言。

第二，随着信息时代和网络社会的到来，基于网络的各种新业务不断兴起。为此，人们建立了各种各样的信息系统，结果导致人类社会的一些机密和财富高度集中于计算机和网络中，保密和财富安全与信息安全息息相关。于是，信息安全的问题变得越来越重要，已成为网络经济和网络社会能否安全健康发展的关键之所在。

实际上，在信息密集的金融业电子化后，不但使国际贸易的资金流动和清算速度大大加快，而且同时也使巨额资金操纵、洗钱等非法金融行为变得非常便利，这就极有可能爆发国家甚至世界级的金融危机；同时，若网上传输的军事、国家机密信息一旦被敌方截获，其后果就更不堪设想。可见，如何解决信息与网络安全问题，如何解决由于信息网络化、商务电子化后给人类社会带来的新的不安全、不稳定因素非常重要，甚至直接影响到国家的安全和生死存亡。1998 年发生的亚洲金融危机在很大程度上就是由于金融电子化管理失控所致；1994 年年底，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，对美国 CITYBANK 银行的计算机主机进行了一连串攻击，并通过电子转账的方式窃走了 1 100 万美元。据美国 ABA（American Bar Association）组织调查估计，仅美国每年因计算机和网络犯罪所造成的经济损失就超过 150 亿美元，全世界每年因计算机和网络犯罪所造成的直接经济损失更是无法估计。

在 Internet 上，每天都有数十起的计算机犯罪发生。然而事实上，我们知道的有关网络入侵等计算机犯罪只是实际所发生的事例中很小的一部分，大多数网络入侵或攻击并没有被发现，即使被发现了，也常常由于这样或那样的原因，人们并不愿意公开它，以免引起公众的惊慌和混乱。据统计，商

业信息被窃取的事件正在以每月 280%的速率在增加。据有关专家估计，每公开报道一次网络入侵，就同时有近 550 例是不被公众所知晓的。可见，人们知道的计算机犯罪和黑客攻击事件仅仅是浮出水面之“冰山”的一小角。

第三，由于信息本身就是时间、财富，就是生产力，因此，世界各国无不千方百计地利用电子空间的无国界性和信息战的制胜性来实现其以前军事、文化、经济侵略所达不到的战略目的。例如，美国在两次海湾战争中均巧妙地利用其信息战的优势有效地使伊拉克的各种信息系统和军事指挥信息中枢瘫痪，使敌方成为“聋子”和“瞎子”，掌控了战争的主动权，最后推翻了伊拉克萨达姆政权。可见，从某种意义上讲，对任何国家，信息安全问题都已成为一个正在严重影响社会发展和关系国家安全、国家主权和社会稳定的重大现实问题。有关专家预计，未来的信息与网络安全问题远比核威胁要严重得多。

今天，信息安全的重要性已引起世界各国政府、企业、集团和组织的高度关注，确保信息与网络安全是一件刻不容缓的大事，已成为世界各国共同关注的焦点。因此，研究和掌握信息与网络安全技术，预防和控制信息与网络安全突发事件，确保信息与网络的安全，具有十分重要的战略意义和现实意义。

### 1.1.3 计算机与网络犯罪技术日趋复杂

在过去的十几年中，网络黑客们一直在通过计算机的漏洞来对计算机系统进行攻击，而且这种攻击的方法正在变得越来越复杂。

在 20 世纪 80 年代，大部分入侵者的方法仅仅是利用猜口令、系统的配置不当，以及系统上软件本身的漏洞。到了 1994 年，这些方法虽然仍被使用，但又增加了新的方法，有些入侵者甚至通过读取操作系统源代码的方法来获取系统的漏洞，并以此研究攻击系统的方法。另外，近年来一些网络黑客编写的入侵软件和攻击工具，可通过 Internet 很容易地下载得到，这就给网络安全提出了更严峻的挑战。

2004 年公安部公布的全国信息网络安全状况调查结果显示，在被调查的 7 072 家政府、金融证券、教育科研、电信、广电、能源交通、国防和商贸企业等部门和行业的重要信息网络、信息系统使用单位中，发生网络安全事件的比例为 58%，其中发生 1 次的占总数的 22%，发生两次的占 13%，发生 3 次的占 23%。在已发生的网络安全事件中，计算机病毒、蠕虫和木马程序造成的安全事件占发生安全事件单位总数的 79%，拒绝服务、端口扫描和篡改网页等网络攻击事件占 43%，大规模垃圾邮件传播造成的安全

事件占36%。54%的被调查单位网络安全事件造成的损失比较轻微，损失严重和非常严重的占发生安全事件单位总数的10%。公安部公共信息网络安全监察局有关负责人表示，造成网络安全事件的主要原因是安全管理制度不落实和安全防范意识薄弱，其中因未修补、防范软件漏洞等原因造成的安全事件占总数的66%。

面对如此严重的网络威胁和信息安全问题，人们必须研究和开发出科学有效的信息安全技术与信息安全系统管理措施，实施“标”、“本”兼治，才能实现信息安全的目标。但是现有的大多数计算机网络在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制层次上。因此，随着网络互联程度的日益扩大，这种安全机制对于庞大的网络环境来说形同虚设。另外，开放性和资源共享是计算机网络安全问题的主要根源，目前网络上使用的许多协议，比如TCP/IP协议，在制定之初根本就未考虑信息安全的需要，存在着很多“本质安全”先天不足的问题，其安全性只好依赖于加密、网络用户身份鉴别、存取控制策略等补救技术手段予以解决。因此，TCP/IP协议根本不能满足信息安全的要求。另外，我国在信息化基础建设中使用的许多硬件、软件产品的核心技术都掌握在外国人手中，在使用这些软件和硬件产品时缺乏对其进行有效管理和技术改造，同时由于标准不一、管理不严，使得信息与网络自身的防护能力很弱，许多应用系统处于不设防状态，具有极大的风险性和危险性。这种情况使得我国的信息安全形势尤为严峻。

为了解决上述问题，国内很多研究机构在这方面做了大量工作，主要从事数据加密技术、身份认证、数字签名、“防火墙”、安全审计、安全管理、安全内核、安全协议、IC卡（存储卡、加密存储卡、CPU卡）、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。当前，一个科学地研究和开发信息安全技术，系统地学习和掌握信息与网络安全知识的时代已经到来。

## 1.2 信息安全的概念与内涵

### 1.2.1 数字信息与信息安全

信息资源是国家的战略资源，围绕着信息资源的获取、使用和控制，世界各国之间早已展开了激烈的竞争。信息安全问题是伴随着信息管理和信息科技的普及应用而产生的。无论是何种形式的信息都存在着安全问题。如纸

质信息存在着泄密问题，也存在着由于信息载体不耐久或者由于保管不当而造成信息丢失的问题。近年来，随着全球信息化进程的日益加快，数字信息大量产生，已成为当代信息的主体，并从经济到文化，从工作到生活，从军事到政务等方面对社会生活和各行各业产生巨大影响。随之而来的信息安全问题日益突出，并成为各国社会和集团无法回避的一个重大现实问题。

从用户（个人或企业）的角度来说，希望涉及个人隐私或商业利益的信息在网上传输时能够保障其机密性、完整性和真实性，避免其他人利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害；同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，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“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络“黑客”的攻击。

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，避免其通过网络泄露，避免由于这类信息的泄密对社会产生危害，对国家造成巨大的经济损失。

从社会教育和意识形态的角度来讲，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。

可见，当代信息安全主要是指基于计算机和网络的数字信息安全。

### 1.2.2 信息安全的概念和内涵

#### 1.2.2.1 信息安全的主要目标

综观国内外有关信息安全事件的危害和后果，信息安全的研究目标应主要集中在以下三个方面：

（1）保障各种有用信息（包括动态的、正在网络上传输的信息和静态的、存储在计算机、网络、工作场所和各种载体中的有用信息和各种资源）免遭毁坏、泄露、盗窃、监听、截获、丢失、修改或被非法访问、获取和使用；

（2）保障信息本身的完整性、真实性和可用性能够长久维护和不变；

（3）确保信息发出者不能抵赖所发信息，收到信息者不能否认收到了所要信息或篡改其内容。

#### 1.2.2.2 信息安全的概念和内涵

所谓信息安全，笼统地讲，是一门有关信息安全的全新的系统工程技术，是指在信息的生产、加工、转换、存储、传输、使用等一系列环节和过

程中，为确保实现上述信息安全目标所采用的一系列有效对策、知识方法和各种技术的总称。就总体而言，信息安全主要包括信息本身的安全、计算机系统的安全、网络安全、信息管理体系的安全四个层次的内容。

（1）信息本身的安全。信息本身的安全主要是指为了保证信息本身在产生、传输、使用、存储过程中免遭破坏、修改、窃取、非法截获和使用；为了使秘密信息不泄露，非密信息本身的完整性、真实性、可用性能够得到长久不变的维护所应采取的一切技术、方法和措施。常见的这类技术有身份认证技术、存取控制与数据加密技术、备份技术、紧急处理与系统恢复技术、存储介质防失效技术和异地存放、安全保管技术等。这里所论的信息包括存在于网络之中的动态信息，也包括存储在未联网的独立的计算机上的信息和脱机独立保存在特定存储介质中的静态信息。

（2）计算机系统的安全。计算机系统安全的主要目标是保护存放在计算机系统中的信息与资源免受毁坏、替换、盗窃和丢失。关注的重点主要包括：避免内部人员对计算机系统造成有意或无意的威胁；确保计算机的硬件、软件能够正常运转；提供正常的服务，所处理的数据能够保密、完整和可用。为了保证计算机系统的安全，防止非法入侵对系统的威胁和攻击，制定正确的政策、策略和对策非常重要。首先，应根据计算机系统的安全需要进行必要的系统安全及保密设计，然后在安全设计的基础上，再采取适当的技术组织策略和措施。计算机系统安全技术涉及的内容比较多，大体包括以下方面：硬件系统安全技术、软件系统安全技术、数据信息安全技术、运行服务安全技术、病毒防治技术、“防火墙”技术和计算机应用系统安全检测与评价技术等。

（3）信息管理体系的安全。信息管理体系的安全主要涉及信息管理体系建制安全、规章制度安全、人事人才安全、立法安全和信息安全管理标准等有关信息系统化、规范化和法制化管理等内容。

（4）网络安全。网络安全有广义和狭义之分。广义网络安全强调的是整个信息系统的安全，从其本质上讲就是网络上的信息安全，它涉及的领域相当广泛，强调的是对整个网络而不是网络中的某个或某些单元进行保护，需要研究的除了上述的信息安全内容外，还包括研究如何提高网络系统的软件与硬件的安全性能，防范用户（或罪犯）从外部对网络进行攻击，以保证系统的运行安全及传输安全。由于目前的公用通信网络中存在着各种各样的安全漏洞和威胁，因此，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广义网络安全的研究领域。狭义网络安全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，系统能够连续、可靠、正常地运行，网络服务不中断。

网络安全在不同的应用环境和学术流派中有不同的解释，可进一步分为运行系统安全、网络上系统信息安全、网络上信息传播安全、网络上信息内容的安全等。

运行系统安全，即保证信息处理和传输系统的安全。包括计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全性考虑，硬件系统的可靠性、安全性，计算机操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。它侧重于保证系统的正常运行，避免因为系统的崩溃和损坏而对系统内存储、处理和传输的信息造成破坏和损失；避免由于电磁泄漏产生信息泄露，干扰他人或受他人干扰。本质上是保护系统的合法操作和正常运行。

网络上系统信息安全，包括用户口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

网络上信息传播安全，即信息传播后果的安全。该部分包括信息过滤、不良信息的过滤等。它侧重于防止和控制非法、有害信息的传播，以防止在公用通信网络上大量自由传输的信息失控。本质上是维护道德、法则或国家利益。

网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

综合上述，网络安全就是要保证网络上存储和传输信息的安全性，是指通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。网络安全从结构层次上还可分为物理安全、安全测控和安全服务。

## 1.3 信息安全化的基本特征及其主要威胁

随着全球信息化及经济全球化的发展，信息资源共享应用日益广泛和深入。但是信息在公共通信网络上存储、共享和传输，会经常遭受非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管

理部门、政府或军事领域对公共通信网络中的存储与传输的数据安全问题更为关注。有时人们因为安全因素不敢使用 Internet 这样的公共网络来传输和存储重要的信息和数据。因此，如何不断地提高信息安全化的程度和水平是信息安全工程学研究的永恒主题。

### 1.3.1 信息安全化的基本特征

信息安全是新出现的一种非传统安全，是现代安全科学技术学科的新的组成部分。然而，同其他传统安全一样，虽然人们追求的目标是信息安全化，但是，相对于一定的社会、技术、经济水平和条件，没有绝对的安全，只能达到相对的安全。那么，相对于当代技术、经济条件的信息安全化有哪些基本特征？其面临的主要威胁类型是什么？搞清楚这些基本问题，对科学客观地进行信息安全化研究和建设，具有重要的指导意义。

信息安全是一门新兴学科，关于信息安全化的具体特征的标志尚无统一的界定标准。但在现阶段，对信息安全化至少应具有机密性保证、完整性保证、可用性保证和可控性保证四个基本特征，却具有广泛的认同。

（1）机密性保证。机密性保证是指保证信息不泄露给非授权的用户、实体的过程，或供其利用的特性。换言之，就是保证只有授权用户可以访问和使用数据，而限制其他人对数据进行访问或使用。

数据机密性在商业、军事领域具有特别重要的意义。如果一个公司的商业计划和财政机密被竞争者获得，那么该公司就会有极大麻烦。

数据的机密性分为网络传输机密性和数据存储机密性。如同通信电话能被窃听一样，网络传输也可能被窃听，其解决办法就是对传输数据进行加密处理。本教材第五章将详细介绍数据加密技术及其应用。数据存储机密性主要是通过访问控制来实现的。根据不同的安全要求和等级，一般将数据分成敏感型、机密型、私有型和公用型等几种类型，管理员常对这些数据的访问加以不同的访问控制。如经理可以访问所有数据，一些技术人员除了敏感型数据以外都能进行访问，一般职员只能访问私有型数据和公司型数据。在实践中这类访问控制的实现并不难，许多安全型操作系统（如 UNIX、Windows NT 等操作系统）都能做到。但值得注意的是，人们常用的 Windows 95 和 DOS 操作系统并不具有这种功能。

保证数据机密性的另一个易被人们忽视的环节是管理者的安全意识。一个有经验的黑客可能会通过收买或欺骗某个职员，而获得机密数据，这是一种常见的攻击方式，在信息安全领域称之为社会工程。

（2）完整性保证。完整性是指数据未经授权不能进行任何改变的特性。