21世纪高等院校计算机网络与通信教材

# 计算机网络安全与控制技术

北京希望电子出版社　总策划
卢　昱　王　宇　主　编
吴忠望　卢　鋆　张练达　编　著

科学出版社
www.sciencep.com

21世纪高等院校计算机网络与通信教材

# 计算机网络安全与控制技术

北京希望电子出版社　总策划
卢　昱　王　宇　主　编
吴忠望　卢　鋆　张练达　编　著

科学出版社
www.sciencep.com

## 内容简介

为了适应计算机科学与技术学科的发展和现代计算机教学的需要，作者在多年研究生、本科生和大专生的计算机网络教学、实践的基础上，介绍了计算机网络安全的现状及发展、网络安全体系结构、网络安全基本技术、网络防御技术、网络攻击技术、网络控制、受控网络系统、网络安全控制技术和网络安全工程并介绍了两个网络安全应用实例。

本书注重网络安全技术的实际应用，层次清晰，概念准确，内容丰富，图文并茂，适合学生系统地学习计算机网络技术各方面知识，每章都有习题以帮助学生巩固所学知识。本书可作为计算机专业的研究生、本科生和大专生以及电子信息类专业的研究生或本科生的教材，也可供计算机网络应用与信息技术的工程人员学习参考。

需要本书或需要得到技术支持的读者，请与北京中关村 083 信箱（邮编 100080）发行部联系，电话：010-82702660　010-82702658　010-62978181 转 103 或 238　传真：010-82702698　E-mail：tbd@bhp.com.cn

**图书在版编目（CIP）数据**

计算机网络安全与控制技术/卢昱，王宇主编. —北京：科学出版社，2005.6

21 世纪高等院校计算机网络与通信教材

ISBN 7-03-015297-2

Ⅰ. 计…　Ⅱ. ①卢…②王…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 026900 号

责任编辑：曾　华　／责任校对：马　君

责任印刷：媛　明　／封面设计：梁运丽

科学出版社　出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市媛明印刷厂印刷

科学出版社发行　各地新华书店经销

*

2005 年 6 月第　一　版　开本：787×1092 1/16

2005 年 6 月第一次印刷　印张：19 1/8

印数：1-3 000 册　字数：436 千字

**定价：27.00 元**

# 21世纪高等院校计算机网络与通信教材

## 编委会

# 序

目前，中国固定和移动两大网络的规模都已位居世界第 2 位，上网用户 2004 年总数达 9400 万，中国的信息通信制造业也得到很大的发展。今后 5 年中国信息产业预计将仍会以高于 20％的速度增长。中国将加快建设新一代信息通信网络，全面振兴信息通信产品制造业和软件业，建立能够支撑信息通信业发展的技术、生产体系。在向数字化、集成化、网络化转变的过程中，简单服务要向个性化服务发展，低带宽要向高带宽发展，电路交换要向分组交换发展。无线网络、网络多媒体、多媒体计算、人机自然语音通信是网络与通信专业重点建设的四大方向。

面对潜力巨大的中国市场，我国大学的相关专业需要培养具有知识创新能力的高素质人才，在通信高新技术的研究上争创国际先进水平，为我国在信息领域达到国际一流的目标作出贡献。

科技的发展使得教育要跟上时代发展的步伐，但是目前市面上还没有一套系统、完整的关于计算机网络与通信方面的教材。现有的教材有些偏重理论，有些则偏重实用，不太适合于课堂教学。而对于学习网络与通信的学生来说，不仅要懂得原理，还必须学会技术，这样才能符合“培养人才、创造知识、转化成果、服务社会”的教学宗旨，在人才培养、科学研究和技术应用等方面有所成就，为我国通信与信息领域的发展做出贡献。

为了获得与国际接轨的教学内容，达到提高整体教学水平的目的，北京希望电子出版社组织国内各大高校相关专业的教授、专家、学者，共同编选本套丛书。本套丛书强化学生实践能力和创新意识的培养，定位准确、内容创新、结构合理。在选材上主要采用了成熟的理论，并通过对目前研究现状的跟踪，补充了最新的研究成果；充分考虑了内容组织的系统性和完整性，从学生的认知规律出发，力求做到简明和便于教学的特色；以培养学生分析问题和解决问题的能力为目标，着重基本概念、基本原理和基本分析方法的论述。本套丛书特别突出了各项技术的实用性，可作为计算机网络和通信专业或相近专业本科生、研究生的教科书，同时，还可以作为从事网络系统开发的科研人员和相关行业技术人员、管理人员有用的参考资料。

在撰写过程中参阅了大量的参考书、论文和资料，这里谨向所有的作者致以崇高的敬意！

我们欢迎更多的优秀教师参与到教材建设中来，真诚希望广大教师、学生与读者朋友在使用本丛书过程中提出宝贵的意见和建议。若有投稿或建议，请发至本丛书出版者电子邮件：textbook@bhp.com.cn

21 世纪高等院校计算机网络与通信教材编委会

# 前　言

信息化成为当前国民经济和军事发展的重要推动力。国家基础设施、国防基础设施以及与人民生活息息相关的各行各业的建设与发展，对计算机和网络的依赖程度不断增大，使计算机网络成为国家发展和人民生活的不可或缺的重要组成部分。Internet 将全世界各种各样的计算机设备和网络互连起来，并通过各种便利的接入方式为人们提供随时随地的网络服务。网络的开放性和潜藏的商业、经济、军事利益给网络黑客、计算机犯罪人员、国外敌对势力和恐怖分子等创造了大量可乘之机，使计算机网络安全受到了前所未有的关注和重视。

计算机网络安全与控制技术是不断发展的技术，它是以密码学为基础，以网络安全体系结构为框架，以安全服务和安全机制为基石，以安全需求为牵引，以各种网络安全技术为保障，以网络安全控制为手段，目的是尽可能地降低网络的安全风险，提高网络的安全性，确保网络信息的机密性、完整性、可用性、可控性、真实性和抗否认性。实现计算机网络安全是一个工程性和实践性很强的学科，它需要系统化的工程解决方法，标准化的分析、设计和实施过程。研究和实现计算机网络安全，必须掌握基本的安全理论和安全工程知识，树立安全防范的意识，熟悉各种安全实施原则与方法，对计算机网络攻击与防御技术有深入的了解，并且具备发现和解决相关领域安全问题的能力。

本书重点讲述了计算机网络领域中的安全技术问题，涵盖了网络安全体系结构、网络安全基本技术、网络攻击技术、网络防御技术、网络控制、网络安全控制技术和网络安全工程等方面的知识，力求从简洁、全面、新颖、深刻的视角分析网络应用领域中存在的有关安全的问题、技术和方法，并着重从网络控制的角度诠释系统解决网络安全的新理论和新思维。本书共分 10 章，第 1 章介绍了网络安全的基本概念，概述了网络安全的现状、演进目标和发展历史。第 2 章讲解了网络安全的基本参考模型，OSI 网络安全体系结构，经典的网络安全模型和网络安全保障体系。第 3 章论述了密码技术、数字签名技术、消息认证技术、访问控制技术、身份鉴别技术和 PKI 技术等基本的安全知识。第 4 章介绍了防火墙、虚拟专用网、入侵检测、信息隐藏、病毒防范、密罐和安全管理等常用的网络防御技术。第 5 章叙述了网络攻击的一般过程、常用的攻击手段和攻击技术。第 6 章从控制的角度论述了网络控制的相关概念、控制方式和控制结构。第 7 章提出了受控网络的基本概念和设计原则，然后介绍了受控网络系统安全结构的组成、安全模型以及受控网络的安全控制功能，并对受控网络系统的控制结构进行了设计和分析。第 8 章专门针对安全领域，介绍了网络安全控制的各种技术，包括加密控制技术、鉴别的安全控制技术、协议的安全控制技术和代码的安全控制技术等。第 9 章论述了网络安全工程的一般过程，安全风险评估和效能评估的原则与方法以及安全风险管理的策略与过程。第 10 章从工程实践的角度，介绍如何运用网络安全技术和安全工程的实施原则，实现数据库应用系统的安全和数字地球系统的安全。

本书在选材上主要采用了成熟的理论，并通过对目前研究现状的跟踪，补充了最新的研究成果。全书充分考虑了内容组织的系统性和完整性，特别突出了各项技术的实用性，可以作为计算机网络和信息安全专业或相近专业本科生、研究生的教科书，同时还是从事网络安全、网络管理、信息系统开发的科研人员和相关行业技术人员、管理人员有用的参考资料。

由于网络安全涉及知识的范围较广，技术较新，编写时难免有错误和不足之处，望广大读者和专家批评指正。

编者

# 目　录

# 第1章 绪 论

在《千年警醒：信息化与知识经济》一书中，作者如此界定近代的历史阶段特征：19世纪是铁路的时代；20世纪是高速公路的时代；21世纪则将是信息网络的时代。在《未来之路》和《数字化生存》等书中，对于网络时代生活情趣也有大量描述。随着对网络日趋理性化的思考，人们也日益注意到网络带来的种种负面影响。网络存在的安全问题，实已酿成举世之忧。典型的证据，正好来自互联网的故乡。

据2000年美国进行的社会调查，有70%的美国网民对互联网的安全缺陷深感忧虑，这实际上给出了三七开的“不及格”打分。

美国白宫、美国国防部和美国联邦调查局这种重要网站，以及“微软”这类计算机行业的顶级网站，尽管采取了精心的防范措施，但都先后遭“黑”、遭病毒，甚至瘫痪。网络的脆弱性由此足见一斑。

当年积极倡导“信息高速公路”的克林顿总统，他本人竟一直不敢用E-mail与他在加州上大学的女儿通信，生怕有人窃看；他守着“信息高速公路”，却有悸于加以使用。

世纪之交，伴随着信息化发展而来的信息安全与互联网的安全问题已经成为全球性的重要问题。据统计，全世界由于信息系统的脆弱性而导致的经济损失，每年达数亿美元，并且逐年上升。网络安全问题日益严重。据美国《金融时报》报道，现在平均数秒钟就发生一次入侵计算机互联网的事件；互联网的防火墙，超过1/3被攻破。网络安全危机已经随着科技的发展成为信息化进程中的重要瓶颈。为了维护和加快信息产业的发展，各国政府、企业、科研人员也都在与当前肆虐的各种网络灾害进行着不懈的斗争，安全问题一日未得到彻底解决，企业、社会、国家就会随时有遭到攻击甚至毁灭的危险。如何把握网络安全技术体系，从而形成核心安全系统，已经是21世纪初期信息网络界急待解决的问题。

## 1.1 网络的现状和演进目标

查阅20世纪90年代文化史的关键词，“网络”肯定是一个发烫的词条。这个词犹如一阵旋风冲入90年代，俨然代表了某种强大的历史力量。因特网于1991年由美国国家科学基金会（NSF）解禁，至少在当时，没有多少人预见到这个揭幕仪式如同开启了潘多拉盒子。事实上，计算机网络已经默默地存在了20余年。第1个计算机网络——阿帕网络——于1969年秘密问世。然而，解禁之前的计算机网络不过是一项保密的军事技术隐藏于美国国防部高级研究计划署的办公大楼。如果没有突如其来的历史青睐，那么，如同许多有趣的发明那样，因特网的意义也只能封锁在技术范畴之内。

突如其来的历史青睐是如何发生的？这个问题涉及了众多方面。迄今为止，“网络”这个概念业已成为划时代的标志之一。谈论人们置身的时代，网络是一个不可回避的词汇——“信息时代”的主体部分离不开网络的组织。网络的意义远远地突破了技术范畴而介入了经济、文化乃至一个社会的民主政治。按照某些人的预计，网络会在相当程度上改造传统的社会制度。换言之，网络似乎正在赢得某种万众瞩目的特殊位置。

### 1.1.1 灰色网络

网络是 20 世纪最伟大的科技成就之一。人们运用现代通信技术将地理位置不同、功能独立的多个计算机系统相互链接起来，并以功能完善的网络软件实现网络资源共享和信息传递，实现了一种前所未有的“神奇链接”。正是因为这种神奇的链接，改变了人类传统的生产方式和生活模式，使人类社会告别了工业时代，进入了以互联网为主要特征的信息时代。

万物皆进化，网络也不例外。把握网络进化导向，是一种前瞻运筹，事关一个企业乃至一个国家的网络命运和前途。为此，对网络现实和网络未来，须有脱俗的审视，才能有出众的作为。

进入 20 世纪 90 年代后期，计算机网络特别是互联网呈现出爆炸性发展，并以惊人的速度在全球范围内扩张，其触角伸向社会的政治、经济、军事、文化、教育等各个领域。从美洲到欧洲，从亚洲到非洲，网络如燎原之火，迅速波及全球，渗透到人类生活的各个方面，掀起了一场席卷全球的网络风暴。一方面，网络的东风吹开了千树万花，以其独特的开放性、共享性为人类带来了无限欢乐与遐想；另一方面，由于网络信息安全问题，它又成了“带刺的玫瑰”，给国家、企业和个人带来了极大的安全隐患和信息灾难。网络，在虚拟与现实之间、正义与邪恶之间、有序与混乱之间、安全与威胁之间、开放与控制之间，交错徘徊，形成了一种复杂的灰色状态。

世上任何高新科技的应用，本应是可控的，若出现失控状态就应被定义为进入灰色状态。然而，现有网络平时就处在安全失控的灰色状态下运行，灰色成为网络的现实状态。

灰色网络并不是严格的概念，而是对现有网络一种形象的、比喻的描述，是对具有某些特征的一类网络的高度概括。一般可以从网络的状态特征上来刻画灰色网络。

**定义 1.1** 灰色网络是指不确知的、难测度的、结构多样多变、局部有序而整体无序，不安全的、非受控的网络系统。现有的网络大多数属于灰色网络的范畴，也就是说网络拓扑既有异构、病构特点，又具备一定的自组织、可生存能力；既遍布安全隐患、威胁和不良内容，又具有形式多样的安全和管理手段，网络整体上是无序的、不确知的、不安全的和不受控的。

灰色网络固有的开放性和不确定性带来的网络安全问题，一直备受关注而没有可信有效的解决方案。目前的网络安全技术大都缺乏统一的理论指导，都是针对某一方面或某个层次的安全问题提出的解决方案，很难从整体上和根本上解决网络安全问题。

灰色网络的存在，改变了世界，改变了社会，改变了人类生活，同时也从根本上改变了人类的安全观念，使网络安全成为国家安全的关键环节。种类繁多的病毒、动机叵测而又手段高超的黑客、网络恐怖主义者等，都对网络构成了严重的威胁，网络安全作为一个日益突出的全球性和战略性问题，现实地摆在人们面前。保障网络安全，改变灰色现状，构建绿色网络，成为信息时代必须解决的重大课题。

### 1.1.2 绿色网络

灰色网络的受害者涉及个人、企业、国家，乃至全人类，是人类必须要加以解决的历史难题。针对灰色网络的现状，人们提出了可信网络、主动网络和受控网络等概念。这些概念都是网络健康、理性发展过程中的典型代表。可信网络是相对内外网而言的，它认为

内部网络是安全可信的，外部网络则是充满威胁、不安全的，显然可信网络的这种观念已经不适应网络的发展了；受控网络是针对安全性、可控性要求较高的特种网络提出的，其适用范围有限，以牺牲部分开放性和效率来保证网络的安全可控，是当前的一个研究热点。随着未来网络安全、可信、受控的需求日益迫切，人们开始从控制的角度考虑网络问题，通过将网络的设备、人员、应用和环境纳入受控的体系，将网络上的各种进程、行为、状态都控制起来，减少整个网络的不确定性和无序性，从而达到增强网络安全性的效果。

国际社会，对网络安全问题及其引发的网络进化，一直保持关注。早在 20 世纪 90 年代，国内外学术界就开始有呼吁，认为互联网是一种“信不过”的网络（Untrustworthy Network），并开展了网络结构创新的探索。据此背景，由联合国科教文组织牵头召开的“世界科学大会”（1999 年 6 月 25 日～7 月 1 日），把解决网络缺陷和负面效应问题列为大会重点议题之一。此后不久，ITU-T 于 2000 年 2 月发布了 Y.130 文件，提出了未来网立足于 ICA（Information Communication Architecture，信息通信结构）的建议，把中间件层和基础层一起定义为 GII 基础设施。值得关注的是，在整篇 Y.130 中，没有出现“IP 统治未来网”之类的提法，被推荐的是 ICA 结构，而现在盛行的以 IP 网为典型的灰色网络恰恰不含有这种结构。ICA 的出台，表明国际上已建立起一种未来网络定位的新理念。不像“IP 统治未来网”方案具有鲜明的排他性那样，ICA 开发的策略是博纳众长，据以取得功能突破。

可见，以创建具有安全保障的网络作为一种时代责任，适时开发 IP 技术之后的网络技术，正是网络技术进步的必然。在这种背景和需求下，我们提出了绿色网络的概念，绿色网络作为网络进化的未来，是一种崭新的、理想的新概念网络。

**定义 1.2** 绿色网络一般是指具备了一定的符合可信、安全、有序和受控等要求的硬件设施，建立了较完善的网络控制体系和信息访问机制的网络。它包括硬件设施和软件建设两个方面。就硬件设施而言包括绿色计算机系统、绿色信道、绿色节点和各种网络绿化装置等，就软件建设而言包括安全控制策略、安全控制机制、控制体系和网络绿化软件系统等。绿色网络的主要标志是：有健全的网络监管控制体系，有完备有效的威胁防御措施，有健康优良的信息环境。

绿色网络是相对于目前的网络状态及其未来发展趋势提出的一种新概念网络体系。作为人们追求的一种理想网络空间，绿色网络在目前的理论和技术条件下还很难实现。构建安全、可信、受控的绿色网络的首要任务和必要步骤是绿化网络，就是在尽量不改变现有网络基础设施的基础上，按照网络安全控制体系架构，搭建网络绿化平台，在网络的各个层次分别安装安全控制部件，各部件协同工作，构成一体化的绿色网络系统，从而解决网络的安全问题。研究网络安全技术特别是安全控制技术，进行网络绿化改造并最终实现绿色网络，是网络安全领域内的魔道之战中立于不败的必由之路。

## 1.2　网络安全概述

“安危相易，祸福相生”，开放是信息革命的精神，是网络技术高速发展的根本原因，是信息经济一如既往的精神动力。同时，开放是一柄双刃剑，无可避免地带来了网络安全隐患。随着互联网的发展，网络安全问题日益凸现，网络安全技术也日新月异。老子曰：“为之于未有，治之于未乱”。网络安全作为一道技术防护屏障，不是附属，而是必需，否

则，带来的将是不可预见的损失。

有网络存在就会有安全问题。传统通信的安全问题是点到点之间的通信保密，是点到点之间的通信保密，现在则是网络安全问题。在新经济时代，网络在一定意义上说就是财富。第1，它是信息最集中的地方；第2，它是财富最集中的地方。随着互联网的发展，随着基于Internet平台的电子商务、电子政务等方式的出现，人们对网络的依赖性也越来越大。如果网上出现故障，不仅给人们带来不便，更可能造成巨大的经济损失。小到信息数据的丢失，大到系统遭受破坏。据有关资料显示，全球每20秒就受到一次攻击。在美国因网络攻击每年造成几十亿美元的经济损失，所以说它的危害是很大的。现在，网络安全已经上升到国家安全，有些国家的网络安全计划由总统亲自负责。网络安全涉及到政府和企业，如电信、金融、教育、大型企业等。

从远古结绳到仓颉造字，从烽火狼烟传讯到全球卫星直播，从面对面交谈到网上漫游，信息交流充斥着人类生活的方方面面。可以说，人类社会时刻也离不开信息。在信息的主要载体——互联网出现以前，由于受到信息交流工具的限制，使信息还没有被做为社会的重要生产要素来对待。从社会发展来看，物质、能量、信息是密不可分的基本资源。农业社会和工业社会，更强调的是有形的物质资源，物质和能量占据社会生活的主导地位，国家安全侧重于抵御外敌入侵的军事安全、政治安全和经济安全。进入21世纪的信息社会，信息、物质、能量演变成为“三足鼎立”，并且信息占据了支配地位，成为最宝贵的战略资源；互联网作为信息交流的主要工具得到了充分的开发和利用。国家经济和社会的发展越来越依赖于信息资源、信息技术和信息产业。

然而，互联网在软硬件方面存在着“先天”的漏洞，这使得信息所具有的高无形价值、低复制成本、低传播成本和强时效性的特点造成了各种各样的安全隐患，安全成为了网络信息资产的核心属性。

### 1.2.1 网络安全的相关概念

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此，可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的机密性、完整性和可用性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。从广义上来说，凡是涉及到网络上信息的机密性、完整性、可用性、真实性、抗否认性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全从其本质上来讲就是网络上的信息安全。

1. 信息安全

信息安全已经历了漫长的发展过程。从某种意义上说，从人类有信息交流开始就涉及信息的安全问题。从古代烽火传信到今天的通信网，只要存在信息交流，就可能存在信息欺骗。信息安全的概念也是与时俱进的，过去是通信保密（COMSEC），昨天是信息安全（INFOSEC），而今天以至于今后是信息保障（IA- Information Assurance）。

（1）通信保密

信息安全的初级阶段，人们似乎更关注信息通信的机密性。通常采用一些简单的替代或置换来保护信息。这些变换是密码学的雏形。这一阶段发展了很多密码算法，但基本的方法都是将字母编号后进行平移、旋转、置换、扩展等变换。例如，将字母编号平移产生了凯撒密码。其他的算法还有单表置换算法、Vigenere 算法、Wernam 算法等、Hill 算法等。此外，还发展了密码分析和破译方法。

（2）信息安全

随着数学、计算机和通信技术的发展，信息的处理能力和传输能力大大提高，靠传统的密码变换已不能满足信息化的要求。因此，信息安全的发展速度也在加速，出现了现代密码理论、计算机安全和通信安全的新理论和新技术。这一阶段的信息安全包括在信息系统的物理层、运行层，以及对信息自身的保护（数据层）及攻击（内容层）的层面上，所反映出的对信息自身与信息系统在机密性、可用性与真实性方面的保护与攻击等内容。

（3）信息保障

目前，国际研究前沿已将信息安全上升到信息保障的高度，提出了计算环境安全、通信网安全、边界安全及安全支撑环境和条件的概念，并开始研究信息网络的生存性等课题。美国国家安全局（NSA）在 IATFV3.1 中提出了深度防御（Defense-in-Deepth）的概念，把信息安全上升到信息保障的高度，并提出了人（People）、技术（Technology）、操作（Operation）3 方面并举的核心策略，基于这个核心，IATF 定义了各种环境下的安全需求和技术方案的框架，对现有的信息安全技术提出了许多新的挑战。

总之，信息安全还没有形成完整的学科概念，但其发展速度正在加快，信息安全研究人员正在增加，信息安全作为独立产业的形态开始显现，主管部门的也在加大管理力度，并加紧制定信息安全法律法规。信息安全学科正应时代需要发展和完善。

2. 网络安全

过去的信息安全主要是通信保密，通信发展到今天的分布系统网络化的前提下，互联网的触角延伸到人们生产、生活的每个角落，由此引出了网络安全这一新课题。

网络安全在不同的环境和应用中会得到不同的解释。对于用户（个人、企业等）而言，网络安全意味着涉及个人隐私和商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的隐私和利益造成侵犯和损害；对于网络运行和管理者而言，网络安全意味着对本地网络信息的访问、读写等操作进行保护和控制，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；对安全保密部门而言，网络安全更侧重于对非法的、有害的或涉密的信息进行过滤和防堵，避免其通过网络泄漏，同时避免由于这类信息的泄密而对社会产生危害，对国家造成重大损失。

一般可以认为网络安全包括物理安全、运行安全和数据安全 3 个层次，它们涵盖的范围如图 1-1 所示。

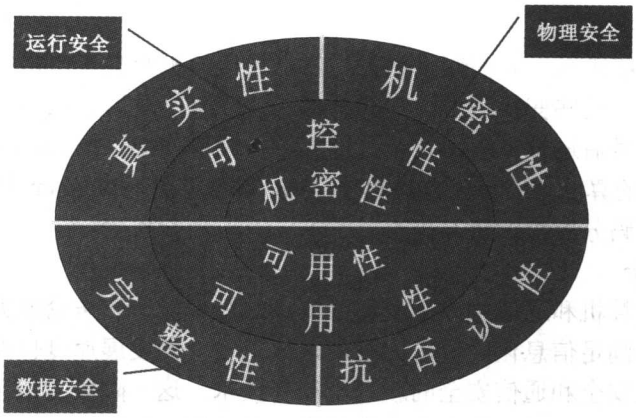


图 1-1 网络安全涵盖的范围

网络安全与其所保护的信息对象有关，本质是在信息的安全期内保证其在网络上流动时或静态存放时不被非授权用户非法访问，但授权用户却可以访问。显然，网络安全、信息安全和系统安全的研究领域是相互交叉和紧密联系的。下面给出本书所研究和讨论的网络安全的含义：

**定义 1.3** 网络安全是指通过各种计算机、网络、密码技术和信息安全技术、网络控制技术，保护网络中传输、交换、处理和存储的信息的机密性、完整性、可用性、真实性、抗否认性和可控性。

定义中所述的 6 大信息安全属性的详细定义请参见 1.2.2 节。

3. 网络安全观

网络安全的特性决定了网络安全本身是一个不断变化、快速更新的领域，也意味着人们对于网络安全领域的投资是长期的行为。但现在的问题是，到底该如何利用技术来保护计算机和网络不受安全的威胁。许多用户在应用计算机接入网络时，往往存在侥幸心理，不会将安全作为首要问题考虑，希望一步到位，并希望其安全措施能永保安全。

首先，网络安全是动态发展的问题。从发展趋势来看，信息网络的安全日益显示出了其重要性。不同国家、地区之间的政治、军事、文化等冲突也动辄引发一轮又一轮的网络攻击战争，如中美、中日、大陆和台湾之间都曾多次爆发大规模的有组织的网络攻击。这些有组织、有目的的网络攻击行为一方面提醒了网络建设者要始终把安全问题放在首位，另一方面也将大大促进网络攻击技术的发展。

其次，网络安全实施是一个系统工程。安全问题涉及身份鉴别、访问控制、数据机密性、数据完整性、抗抵赖、审计、可用性和可靠性等多种基本的安全服务，涉及 ISO/OSI 所有的 7 个协议层次（物理层、链路层、网络层、传输层、会话层、表示层和应用层），覆盖了信息网络中物理环境、通信平台、网络平台、主机平台和应用平台等多个系统单元。因此，这是一个立体的、多方位、多层次的系统问题，在规划、设计、实施信息网络的安全系统时也必须用系统工程的方法论来考虑。

最后，网络安全实施是一个社会工程。在信息网络中，用户接口是至关重要的。在采取了各种复杂的安全技术之后，如果系统的最终用户没有足够的安全意识和安全常识，不

能正确应用各项安全措施，那么其后果要么是安全系统不能工作，影响信息网络的正常运转，要么是安全系统演出空城计，不能起实际的作用（如在一个安全系统中使用简单的用户密码）。因此，在安全系统建设工程中，必须充分重视用户的安全，加强对用户安全意识的培训，加强安全常识的教育，加强安全系统的使用培训。

所以说，网络安全是一个动态发展的系统工程和社会工程，需要长期、持久的巨大的财力、物力、人力的投入，需要从组织、管理等方面采取强有力的措施，才能确保网络在信息的大洋中永远坚固、安全、可靠。

### 1.2.2 网络安全目标

在 ISO7498-2 开放系统安全架构中提出，要解决网络安全问题，主要是在 4 方面提供服务，而 IATF 则进一步演化为安全的 5 性。

1. 机密性

防止信息被非法获得，即防止信息泄漏给非授权的用户、实体或过程，或供其利用。机密性可以保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。

常用的保密技术包括：防侦收（使对手侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）。

2. 完整性

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储和传输。

完整性与机密性不同，机密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障、误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。

保障网络信息完整性的主要方法有：

协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段；

纠错编码方法：由此完成检错和纠错功能，最简单和常用的纠错编码方法是奇偶校验法；

密码校验和方法：它是抗撰改和传输失败的重要手段；

数字签名：保障信息的真实性；

公证：请求网络管理或中介机构证明信息的真实性。

3. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，