普通高等教育“十一五”国家级规划教材

高等职业院校计算机教育规划教材

Gaodeng Zhiye Yuanxiao Jisuanji Jiaoyu Guihua Jiaocai

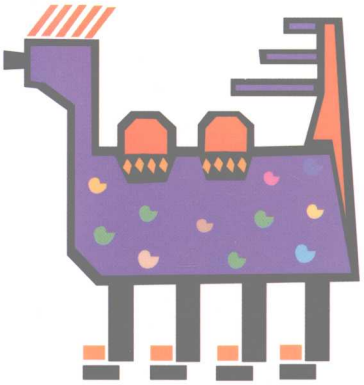
计算机网络安全技术

（第2版）

JISUANJI WANGLUO ANQUAN JISHU

石淑华 池瑞楠 编著

- 结合国际认证的先进课程体系
- 以工作过程为导向的学习过程
- 注重培养学生的实际应用能力



人民邮电出版社
POSTS & TELECOM PRESS

精品系列

普通高等教育“十一五”国家级规划教材

高等职业院校计算机教育规划教材

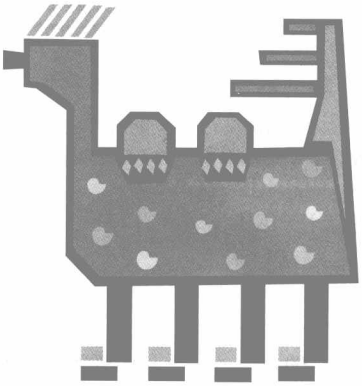
Gaodeng Zhiye Yuanxiao Jisuanji Jiaoyu Guihua Jiaocai

计算机网络安全技术

（第2版）

JISUANJI WANGLUO ANQUAN JISHU

石淑华 池瑞楠 编著



人 民 邮 电 出 版 社

北 京

精品系列

图书在版编目（CIP）数据

计算机网络安全技术 / 石淑华，池瑞楠编著. —2版.
北京：人民邮电出版社，2008.12（2009.2 重印）
高等职业院校计算机教育规划教材
ISBN 978-7-115-18832-8

Ⅰ. 计… Ⅱ. ①石…②池… Ⅲ. 计算机网络－安全技术－高等学校：技术学校－教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2008）第149174号

内 容 提 要

本书根据高职院校的教学特点和培养目标，全面介绍计算机网络安全的基本框架、基本理论，以及计算机网络安全方面的管理、配置和维护。全书共 8 章，主要内容包括计算机网络安全概述、黑客常用的系统攻击方法、计算机病毒、数据加密技术、防火墙技术、Windows Server 2003 的安全、Web 的安全性以及网络安全工程。本书注重实用，以实验为依托，将实验内容融合在课程内容中，使理论紧密联系实际。

本书可作为高职高专计算机及相关专业的教材，也可作为相关技术人员的参考书或培训教材。

普通高等教育“十一五”国家级规划教材
高等职业院校计算机教育规划教材
计算机网络安全技术（第 2 版）

◆ 编　　著　石淑华　池瑞楠
责任编辑　李　凯

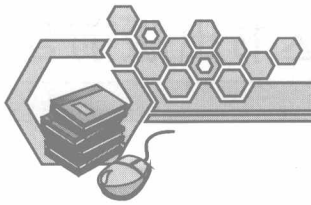
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
中国铁道出版社印刷厂印刷

◆ 开本：787×1092　1/16
印张：18.75
字数：480 千字　　2008 年 12 月第 2 版
印数：30 001-33 000 册　　2009 年 2 月北京第 2 次印刷

ISBN 978-7-115-18832-8/TP

定价：29.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154



第 2 版前言

本书的第 1 版自 2005 年 5 月出版以来，受到广大师生的欢迎，被许多高职院校选用，累计重印 10 多次，发行数万册。我们结合近年来的技术发展和教学改革情况，在保留第 1 版教材特色的基础上，对教材进行了全面修订，力争使本书体现以下特点。

- 按照新的思路组织内容。参考德国先进的职业教育模式，按照实际工作过程，提出教学内容；突出实际操作，注重培养学生的综合能力。本书以真实的校园网为背景，按照“攻击、防范、系统、管理”的顺序设计 4 个学习情境，使学生的学习建立在实际的工作环境中。
- 注重培养学生的动手能力。本书理论“以必需、够用为度”，特别注重实践环节，主要体现在两个方面：一方面是每章中都增加了大量的实验案例，这些案例遵循“源于实际、自主练习、层层递进、提高能力”的设计思路；另一方面是在第 8 章中安排了课程设计的内容，让学生自主学习，提高自身的综合能力。
- 注重知识的更新。计算机网络安全技术领域的一个典型特点就是技术更新速度较快。本书对第 1 版教材中的许多技术内容都进行了更新，并增加了很多新的知识，同时适当兼顾 CIW（Certified Internet Webmaster）的课程内容。
- 习题更加丰富。本书每章均配有精选的习题，以方便学生练习。

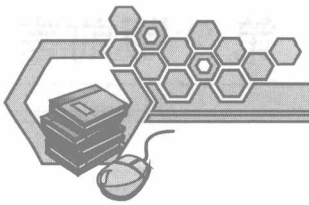
对于书中提到的一些工具软件，读者可以在 Internet 上自行下载。本书还配有 PPT 课件、教学大纲、习题答案等教学资源，任课教师可登录人民邮电出版社教学服务与资源网（www.ptpedu.com.cn）免费下载。

本书第 1 章、第 2 章、第 3 章、第 5 章、第 6 章由石淑华编写，第 4 章、第 7 章、第 8 章由池瑞楠编写，全书由石淑华统稿并审定。在本书的编写过程中，深圳职业技术学院网络技术专业教研室的蔡学军、刘平、王隆杰、张立涓、梁广民、杨名川、邹润生等老师在实验和绘图方面做了很多工作，并提出了许多宝贵意见，在此一并表示衷心的感谢！

由于编写水平有限，时间仓促，书中难免有不妥和错误之处，恳请广大读者批评指正。编者邮箱为 sshua@oa.szpt.net。

编　者

2008 年 9 月



丛书出版前言

目前，高职高专教育已经成为我国普通高等教育的重要组成部分。在高职高专教育如火如荼的发展形势下，高职高专教材也百花齐放。根据教育部发布的《关于全面提高高等职业教育教学质量的若干意见》（简称16号文）的文件精神，本着为进一步提高高等教育的教学质量服务的根本目的，同时针对高职高专院校计算机教学思路和方法的不断改革与创新，人民邮电出版社精心策划了这套高质量、实用型的系列教材——“高等职业院校计算机教育规划教材”。

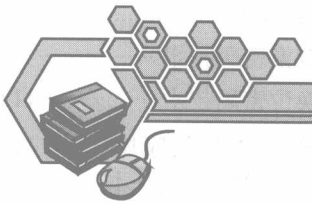
本套教材中的绝大多数品种是我社多年来高职计算机精品教材的积淀，经过了广泛的市场检验，赢得了广大师生的认可。为了适应新的教学要求，紧跟新的技术发展，我社再一次进行了广泛深入的调研，组织上百名教师、专家对原有教材做了认真的分析和研讨，在此基础上重新修订出版。

本套教材中虽然还有一部分品种是首次出版，但其原稿作为讲义也经过教学实践的检验。因此，本套教材集中反映了高职院校近几年来的教学改革成果，是教师们多年来教学经验的总结。本套教材中的每一部作品都特色鲜明，集高质量与实用性为一体。

本套教材的作者都具有丰富的教学和写作经验，思路清晰，文笔流畅；教材内容充分体现了高职高专教学的特点，深入浅出，言简意赅；理论知识以“够用”为度，突出工作过程导向，突出实际技能的培养。

为方便教师授课，本套教材将提供完善的教学服务。读者可通过访问人民邮电教学服务与资源网 http://www.ptpedu.com.cn 下载相关资料。

欢迎广大读者对本套教材的不足之处提出批评和建议！



目 录

第1章 计算机网络安全概述

职业能力要求

- 专业能力：掌握网络安全行业的基本情况，了解网络安全行业的新技术；培养良好的职业道德。
- 社会能力：具有认真负责、严谨细致的工作态度和工作作风，具备良好的团队协作和沟通交流能力。
- 方法能力：良好的自学能力，对新技术有学习、研究精神，较强的动手操作能力。

学习目标

- 了解网络安全的重要性；
- 掌握网络安全的定义；
- 了解信息安全的发展历程；
- 了解网络安全所涉及的知识领域；
- 了解网络安全常见的防护技术。

本章概要地介绍了网络安全领域中的问题：网络安全的重要性以及网络安全的定义（1.1 节）、信息安全的发展历程（1.2 节）和网络安全的防护体系（1.4 节）。在本章的学习过程中，除了掌握网络安全领域中的基本概念外，还应该掌握信息安全领域的新技术。本章的重点是注重培养读者的兴趣，使读者的学习有一个良好的开端。

1.1 网络安全简介

1.1.1 网络安全的重要性

随着信息科技的迅速发展以及计算机网络的普及，计算机网络深入到国家的政府、军事、文教、金融、商业等诸多领域，可以说网络无处不在。资源共享和计算机网络安全一直作为一对矛盾体而存在着，计算机网络资源共享进一步加强，信息安全问题日益突出。

中国互联网协会旗下的DCCI（互联网数据中心）于2008年1月9日发布的《中国互联网调查报告》显示，2007年中国Internet用户规模达1.82亿人。预计2008年中国Internet用户规模将达2.44亿人。我国Internet继续快速发展，各种Internet新业务如雨后春笋般涌现，电子政务、电子商务得到进一步推广，Internet的社会基础设施功能表现得越来越明显。国家计算机网络应急技术处理协调中心（简称CNCERT/CC）在《2006年网络安全工作报告》显示：2003～2006年接收非扫描类事件报告数量比较如图1-1所示。

除了具体的网络安全攻击事件，病毒对网络安全的影响也越来越大，金山毒霸为近几年来的新增病毒/木马数量进行了对比，如图1-2所示。2007年，计算机病毒/木马仍处于一种高速“出新”的状态。2007年病毒/木马增长速度与2006年相比有所放缓，但仍处于大幅增长状态，总数量还是非常庞大的。

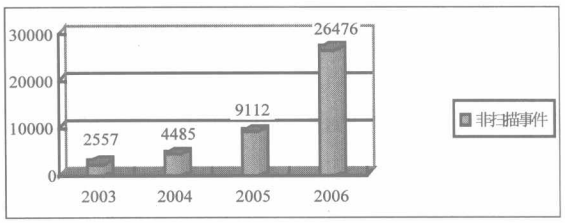


图1-1 接收非扫描类事件年度统计（2003～2006年）

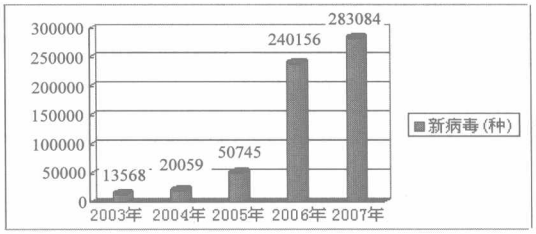


图1-2 新增加病毒统计（2003～2007年）

各种计算机病毒和网上黑客对Internet的攻击越来越猛烈，网站遭受破坏的事例不胜枚举。

2006年第38个世界电信日暨首个世界信息社会日的主题是“Promoting Global Cyber Security”（推进全球网络安全）。这充分体现出网络安全不再是一个潜在的问题，已经成为当前信息社会现实存在的重大问题，与国家安全息息相关，涉及国家政治和军事命脉，影响国家的安全和主权。一些发达国家如英国、美国、日本、俄罗斯等把国家网络安全纳入了国家安全体系。因此，网络安全不仅成为商家关注的焦点，还是技术研究的热门领域，同时也是国家和政府关注的焦点。

1.1.2 网络脆弱性的原因

1. 开放性的网络环境

正如一句非常经典的语句所说：“Internet的美妙之处在于你和每个人都能互相连接，Internet的可怕之处在于每个人都能和你互相连接。”

Internet是跨国界的，这意味着网络的攻击不仅仅来自本地网络的用户，也可以来自Internet

上的任何一台机器。Internet 是一个虚拟的世界，所以无法得知连机的另一端是谁。图 1-3 所示为网上非常出名的一幅图片。在这个虚拟的世界里，已经超越了国界，某些法律也受到了挑战，因此网络安全面临的是一个国际化的挑战。

图 1-3　网上图片

网络建立初期只考虑方便性、开放性，并没有考虑总体安全构想，因此任何一个人、团体都可以接入，网络所面临的破坏和攻击可能是多方面的。例如，可能是对物理传输线路的攻击，也可能是对网络通信协议及应用的攻击；可能是对软件的攻击，也可能是对硬件的攻击。

我国有些专家从 2002 年提出了“网络实名制”，但是社会趋于多元化以及网络的开放性，不同的国家情况有所不同，而且“网络实名制”本身难以同网络时代相适应，可操作性差。在现实中，很难做到真正的“网络实名制”。

2. 协议本身的缺陷

网络传输离不开通信协议，而这些协议也有不同层次、不同方面的漏洞，针对 TCP/IP 等协议的攻击非常多，在以下几个方面都有攻击的案例。

（1）网络应用层服务的安全隐患。例如，攻击者可以利用 FTP、Login、Finger、Whois、WWW 等服务来获取信息或取得权限。

（2）IP 层通信的易欺骗性。由于 TCP/IP 本身的缺陷，IP 层数据包是不需要认证的，攻击者可以假冒其他用户进行通信，即 IP 欺骗。

（3）针对 ARP 的欺骗性。ARP 是网络通信中非常重要的协议，基于 ARP 的工作原理，攻击者可以假冒网关，阻止用户上网，即 ARP 欺骗。近一年来 ARP 攻击更与病毒结合在一起，破坏网络的连通性。

（4）局域网中以太网协议的数据传输机制是广播发送，使系统和网络具有易被监视性。在网络上，黑客能用嗅探软件监听到口令和其他敏感信息。

3. 操作系统的漏洞

网络离不开操作系统，操作系统的安全性对网络安全同样有非常重要的影响，有很多网络攻击方法都是从寻找操作系统的缺陷入手的。操作系统的缺陷有以下几个方面。

（1）系统模型本身的缺陷。这是系统设计初期就存在的，无法通过修改操作系统程序的源代码来弥补。

（2）操作系统程序的源代码存在 Bug。操作系统也是一个计算机程序，任何程序都会有 Bug，操作系统也不会例外。例如，冲击波病毒针对的就是 Windows 操作系统的 RPC 缓冲区溢出漏洞。那些公布了源代码的操作系统所受到的威胁更大，黑客会分析其源代码，找到漏洞进行攻击。

（3）操作系统程序的配置不正确。许多操作系统的默认配置的安全性很差，进行安全配置比较复杂并且需要一定的安全知识，许多用户并没有这方面的能力，如果没有正确地配置这些功能，

也会造成一些系统的安全缺陷。

Microsoft 公司在 2005 年正式公布了 55 个具有编号的操作系统安全漏洞，2006 年则公布了 78 个，同比增长 41.8%。漏洞的大量出现和不断快速增加是网络安全总体形势趋于严峻的重要原因之一。不仅仅操作系统存在这样的问题，其他应用系统也一样。

据美国 CERT/CC 统计，该组织 2006 年全年收到信息系统安全漏洞报告 8064 个，平均每天超过 22 个，与 2005 年同期相比增长了 34.6%。自 1995 年以来，漏洞报告总数达到 30780 个，具体统计结果如图 1-4 所示。

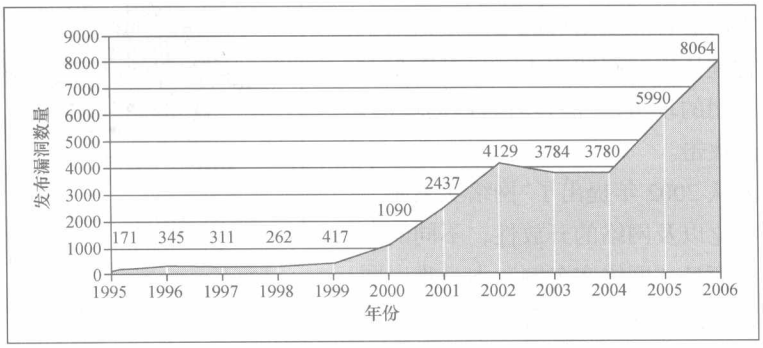


图 1-4　系统漏洞数量比较

4. 人为因素

许多公司和用户的网络安全意识薄弱、思想麻痹，这些管理上的人为因素也影响了安全。

1.1.3　网络安全的定义

国际标准化组织（ISO）引用 ISO 74982 文献中对安全的定义：安全就是最大程度地减少数据和资源被攻击的可能性。

《计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念："计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。"

从本质上讲，网络安全是指网络系统的硬件、软件和系统中的数据受到保护，不受偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域。

欧共体对信息安全给出如下定义："网络与信息安全可被理解为在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输数据，以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性。"

网络安全的具体含义会随着重视"角度"的变化而变化。例如，从用户（个人、企业等）的角度来说，希望涉及个人隐私或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、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说，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

后门、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。从安全保密部门的角度来说，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，避免机要信息泄露，避免对社会产生危害、对国家造成巨大损失。从社会教育和意识形态的角度来说，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。

1.1.4　网络安全的基本要素

网络安全的目的如图 1-5 所示：保障网络中的信息安全，防止非授权用户的进入以及事后的安全审记。

图 1-5　网络安全的目的

上述目的也就是网络安全的 5 个基本要素，即保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可控性（Controllability）与不可否认性（Non-Repudiation）。

1. 保密性

保密性是指保证信息不能被非授权访问，即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，还通过加密阻止非授权用户获知信息内容，确保信息不暴露给未授权的实体或者进程。

2. 完整性

完整性是指只有得到允许的人才能修改实体或者进程，并且能够判断实体或者进程是否已被修改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。

3. 可用性

可用性是信息资源服务功能和性能可靠性的度量，涉及物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。授权用户根据需要可以随时访问所需信息，攻击者不能占用所有的资源而阻碍授权者的工作。使用访问控制机制阻止非授权用户进入网络，使静态信息可见，动态信息可操作。

4. 可控性

可控性主要是指对危害国家信息（包括利用加密的非法通信活动）的监视审计。控制授权范围内的信息的流向及行为方式。使用授权机制，控制信息传播的范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控性。

5. 不可否认性

不可否认性是对出现的安全问题提供调查的依据和手段。使用审计、监控、防抵赖等安全机制，使攻击者、破坏者、抵赖者“逃不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性，一般通过数字签名等技术来实现不可否认性。

1.1.5 典型的网络安全事件

网络安全事件不计其数，典型的网络安全事件如表1-1所示。

表1-1　　典型安全事件

时　间	发生的主要事件
1983年	美国联邦调查局首次逮捕了6名少年黑客，因其所居住的地区密尔沃基电话区号是414而被称做“414黑客”。这6名少年黑客被控侵入60多台计算机，其中包括斯洛恩-凯特林癌症纪念中心和洛斯阿拉莫斯国家实验室
1988年	康奈尔大学研究生罗伯特·莫里斯（22岁）向Internet上传了一个“蠕虫”程序。这个程序是他为攻击UNIX系统的缺陷而设计的，能够进入网络中的其他计算机并自我繁衍。当时使得美国6000多个系统（几乎占当时Internet的1/10）陷入瘫痪，专家称这个“蠕虫”程序造成了1500万到1亿美元的经济损失
1995年	米特尼克被逮捕。他被指控闯入许多计算机网络，偷窃了2万个信用卡号和复制软件。他曾闯入“北美空中防务指挥系统”，破译了美国著名的“太平洋电话公司”在南加利福尼亚州通信网络的“改户密码”，入侵过美国DEC等5家大公司的网络。专家们测算，米特尼克一人就造成了美国一些公司8000万美元的巨额损失
1999年4月	台湾大同工学院资讯工程系学生陈盈豪所制造的“CIH”病毒，在26日发作，引起全球震撼。保守估计全球有6千万台计算机受害
2000年2月	以“雅虎”为首的美国一系列大型网站遭到了黑客有组织的攻击，他们攻击的目标包括雅虎、电子港湾、亚马孙、微软网络等美国大型网站。据统计，在2月7、8、9日这短短的3天里，这些受害公司的损失就超过了10亿美元，其中仅营销和广告收入一项便高达1亿美元
2001年9月	“9·11”事件促使人们更加重视网络安全以及灾后恢复能力，事件后，美国国务院在贝尔茨维尔建立了一个网络监视中心。美国加大了网络安全技术的研发力度，并积极采取措施，在网络防御实践中使用新的安全防护技术
2002年10月	黑客用DDoS攻击影响了13个根DNS（Domain Name Server）中的8个，作为整个Internet通信路标的关键系统遭到严重的破坏
2003年1月	出现“蠕虫王”病毒，利用Microsoft SQL Server的漏洞进行传播，由于Microsoft SQL Server在世界范围内都很普及，因此此次病毒攻击导致全球范围内的Internet瘫痪，全世界范围内损失额高达12亿美元
2004年10月	国内的腾讯QQ、神州数码、江民公司、一家著名电子商务网站陆续被黑客攻陷或入侵。其中一些网站还受到了黑客的巨额敲诈勒索，这是国内首起网络黑客勒索事件
2006年	防止恶意软件对内核的非授权修改，Microsoft通过Patch Guard技术能够封杀对64位版Windows Vista内核的访问，以赛门铁克、McAfee为代表的安全厂商声称，它们需要访问操作系统内核，探测rootkit等恶意软件。在受到来自欧盟委员会和韩国监管机构的压力后，Microsoft同意开放访问内核的API。但是，厂商需要等到Microsoft发布Vista SP1后才能够使用这些API
2007年	超过9400万名用户的Visa和MasterCard信用卡信息被黑客窃取

CA公司（美国Computing Associates公司，全球著名的软件公司之一）关于网络安全事件的预算计算公式如图1-6所示。

图 1-6　网络安全事件的预算计算公式

通过这个公式可以预想，系统平台将越来越多，应用更加多样化，网络安全设备也逐渐增多，将来面临的网络安全事件将会更多。

1.2　信息安全的发展历程

随着科学技术的发展，信息安全技术也进入了高速发展的时期。人们对信息安全的需求也从单一的通信保密发展到各种各样的信息安全产品、技术手段等多方面。总地来说，信息安全技术在发展过程中经历了以下 4 个阶段。

1.2.1　通信保密阶段

20 世纪 40 年代 ~ 70 年代，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，重点是通过密码技术解决通信保密问题，保证数据的保密性与完整性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单地称为通信安全，即 COMSEC（Communication Security）。

这个阶段的标志性事件是：1949 年 Shannon 发表的《保密通信的信息理论》，该理论将密码学纳入了科学的轨道；1976 年 Diffie 与 Hellman 在“New Directions in Cryptography”一文中提出了公钥密码体制；美国国家标准协会在 1977 年公布的《国家数据加密标准》（Data Encryption Standard，DES）。这时人们关心的只是通信安全，重点是通过密码技术解决通信保密问题，而且主要的关心对象是军方和政府。

当时，美国政府和一些大公司已经认识到了计算机系统的脆弱性。但是，由于计算机使用范围不广，再加上美国政府将其当作敏感问题而施加控制，因此，有关计算机安全的研究一直局限在比较小的范围。

1.2.2　计算机安全阶段

20 世纪 80 年代后，计算机的性能迅速提高，应用范围不断扩大，计算机和网络技术的应用进入了实用化和规模化阶段，人们利用通信网络把孤立的计算机系统连接起来，共享资源，信息安全问题也逐渐受到重视。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的计算机安全阶段，即 COMPSEC（Computer Security）。

这一时期的标志是美国国防部在 1983 年出版的《可信计算机系统评价准则》（Trusted

Computer System Evaluation Criteria，TCSEC），为计算机安全产品的评测提供了测试方法，指导信息安全产品的制造和应用。美国国防部1985年再版的《可信计算机系统评价准则》（又称橙皮书）使计算机系统的安全性评估有了一个权威性的标准。

这个阶段的重点是确保计算机系统中的软、硬件及信息在处理、存储、传输中的保密性、完整性和可用性。安全威胁已经扩展到非法访问、恶意代码、口令攻击等。

1.2.3 信息技术安全阶段

20世纪90年代，主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等，网络安全的重点放在确保信息在存储、处理、传输过程中及信息系统不被破坏，确保合法用户的服务和限制非授权用户的服务，以及必要的防御攻击的措施。强调信息的保密性、完整性、可控性、可用性的信息安全阶段，即ITSEC（Information Technology Security）。

这个阶段的主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN等措施。

这一时期的主要标志是在1993年至1996年美国国防部在TCSEC的基础上提出了新的安全评估准则《信息技术安全通用评估准则》，简称CC标准。1996年12月，ISO采纳CC，并作为国际标准ISO/IEC 15408发布。2001年，我国将ISO/IEC 15408等同转化为国家标准——GB/T 18336—2001《信息技术安全性评估准则》。

1.2.4 信息保障阶段

20世纪90年代后期，随着电子商务等的发展，由此衍生出了诸如可控性、抗抵赖性、真实性等其他原则和目标。对安全性有了新的需求：可控性，即对信息及信息系统实施安全监控管理；不可否认性，即保证行为人不能否认自己的行为。信息安全也转化为从整体角度考虑其体系建设的信息保障（Information Assurance）阶段，也称为网络信息系统安全阶段。

这一时期，在密码学方面，公开密钥密码技术得到了长足的发展，著名的RSA公开密钥密码算法获得了广泛的应用，用于完整性校验的散列函数的研究也越来越多。主要的保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测系统、PKI、VPN等。

信息安全受到空前的重视，各个国家分别提出自己的信息安全保障体系。1998年美国国家安全局（NSA）制定了《信息保障技术框架》（Information Assurance Technical Framework，IATF），提出了“深度防御策略”，确定了包括网络与基础设施防御、区域边界防御、计算环境防御和支撑性基础设施的深度防御目标。

1.3 网络安全所涉及的内容

在Internet中，网络安全的概念和日常生活中的安全一样常被提及，而“网络安全”到底包括什么，具体又涉及哪些技术，大家未必清楚，可能会认为“网络安全”只是防范黑客和病毒。其实网络安全是一门交叉学科，涉及多方面的理论和应用知识。除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学，是一个多领域的复杂系统。网络安全所涉及的知识领域如图1-7所示。

网络安全涉及上述多种学科的知识，而且随着网络应用的范围越来越广，以后涉及的学科领域有可能会更加广泛。一般地，把网络安全涉及的内容分为以下几个方面，如图1-8所示。