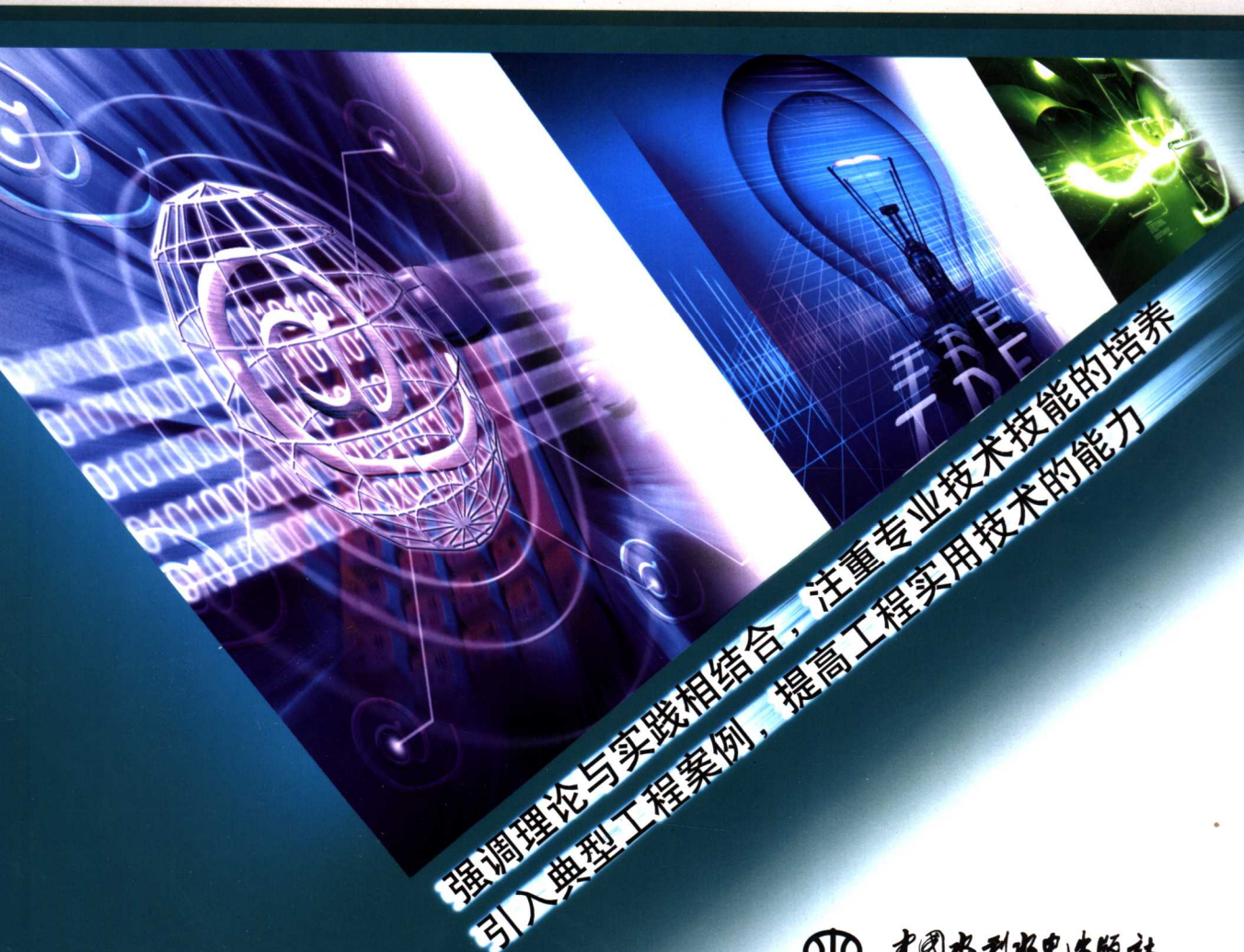
21世纪

高等院校规划教材

戚文静　刘学　主编

网络安全原理与应用



中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校规划教材

网络安全原理与应用

戚文静　刘　学　主　编

中国水利水电出版社

内 容 提 要

本书从网络安全的基本理论和技术出发，深入浅出、循序渐进的讲述了网络安全的基本原理、技术应用及配置方法。内容全面，通俗易懂，理论与实践相得益彰。全书分为11章，内容涉及：网络安全体系结构、密码学基础、密码学应用、防火墙、攻击技术、病毒与防范、入侵检测、WWW安全、E-mail安全、操作系统安全等等。

本书概念准确，选材适当，结构清晰，注重理论与实践的结合。每章都配有1～2个应用实例，并详细讲解使用了配置，既有助于帮助读者对理论的理解和掌握，也可作为实验指导资料。

本书可作为高等学校计算机、信息安全、网络工程、信息工程等专业信息安全课程的教材，也可供成人高校、高职高专和民办院校计算机等相关专业的网络安全课程教材，还可作为信息安全培训教材及信息技术人员的参考书。

本书配有免费电子教案，读者可以从中国水利水电出版社网站上下载，网址为：http://www.waterpub. com.cn/softdown/。

图书在版编目（CIP）数据

网络安全原理与应用 / 戚文静，刘学主编. —北京：中国水利水电出版社，2005

（21世纪高等院校规划教材）

ISBN 7-5084-3197-9

Ⅰ. 网… Ⅱ. ①戚…②刘… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2005）第093012号

书　　名	**网络安全原理与应用**
作　　者	戚文静 刘　学　主编
出版　发行	中国水利水电出版社（北京市三里河路6号　100044）
	网址：www.waterpub.com.cn
	E-mail：mchannel@263.net（万水）
	sales@waterpub.com.cn
	电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm　16开本　19.25印张　466千字
版　　次	2005年9月第1版　2005年9月第1次印刷
印　　数	0001—5000册
定　　价	28.00元

序

随着计算机科学与技术的飞速发展，计算机的应用已经渗透到国民经济与人们生活的各个角落，正在日益改变着传统的人类工作方式和生活方式。在我国高等教育逐步实现大众化后，越来越多的高等院校会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为了大力推广计算机应用技术，更好地适应当前我国高等教育的跨跃式发展，满足我国高等院校从精英教育向大众化教育的转变，符合社会对高等院校应用型人才培养的各类要求，我们成立了“21 世纪高等院校规划教材编委会”，在明确了高等院校应用型人才培养模式、培养目标、教学内容和课程体系的框架下，组织编写了本套“21 世纪高等院校规划教材”。

众所周知，教材建设作为保证和提高教学质量的重要支柱及基础，作为体现教学内容和教学方法的知识载体，在当前培养应用型人才中的作用是显而易见的。探索和建设适应新世纪我国高等院校应用型人才培养体系需要的配套教材已经成为当前我国高等院校教学改革和教材建设工作面临的紧迫任务。因此，编委会经过大量的前期调研和策划，在广泛了解各高等院校的教学现状、市场需求，探讨课程设置、研究课程体系的基础上，组织一批具备较高的学术水平、丰富的教学经验、较强的工程实践能力的学术带头人、科研人员和主要从事该课程教学的骨干教师编写出一批有特色、适用性强的计算机类公共基础课、技术基础课、专业及应用技术课的教材以及相应的教学辅导书，以满足目前高等院校应用型人才培养的需要。本套教材消化和吸收了多年来已有的应用型人才培养的探索与实践成果，紧密结合经济全球化时代高等院校应用型人才培养工作的实际需要，努力实践，大胆创新。教材编写采用整体规划、分步实施、滚动立项的方式，分期分批地启动编写计划，编写大纲的确定以及教材风格的定位均经过编委会多次认真讨论，以确保该套教材的高质量和实用性。

教材编委会分析研究了应用型人才与研究型人才在培养目标、课程体系和内容编排上的区别，分别提出了 3 个层面上的要求：在专业基础类课程层面上，既要保持学科体系的完整性，使学生打下较为扎实的专业基础，为后续课程的学习做好铺垫，更要突出应用特色，理论联系实际，并与工程实践相结合，适当压缩过多过深的公式推导与原理性分析，兼顾考研学生的需要，以原理和公式结论的应用为突破口，注重它们的应用环境和方法；在程序设计类课程层面上，把握程序设计方法和思路，注重程序设计实践训练，引入典型的程序设计案例，将程序设计类课程的学习融入案例的研究和解决过程中，以学生实际编程解决问题的能力为突破口，注重程序设计算法的实现；在专业技术应用层面上，积极引入工程案例，以培养学生解决工程实际问题的能力为突破口，加大实践教学内容的比重，增加新技术、新知识、新工艺的内容。

本套规划教材的编写原则是：

在编写中重视基础，循序渐进，内容精炼，重点突出，融入学科方法论内容和科学理念，反映计算机技术发展要求，倡导理论联系实际和科学的思想方法，体现一级学科知识组织的层次结构。主要表现在：以计算机学科的科学体系为依托，明确目标定位，分类组织实施，兼容互补；理论与实践并重，强调理论与实践相结合，突出学科发展特点，体现

学科发展的内在规律；教材内容循序渐进，保证学术深度，减少知识重复，前后相互呼应，内容编排合理，整体结构完整；采取自顶向下设计方法，内涵发展优先，突出学科方法论，强调知识体系可扩展的原则。

本套规划教材的主要特点是：

（1）面向应用型高等院校，在保证学科体系完整的基础上不过度强调理论的深度和难度，注重应用型人才的专业技能和工程实用技术的培养。在课程体系方面打破传统的研究型人才培养体系，根据社会经济发展对行业、企业的工程技术需要，建立新的课程体系，并在教材中反映出来。

（2）教材的理论知识包括了高等院校学生必须具备的科学、工程、技术等方面的要求，知识点不要求大而全，但一定要讲透，使学生真正掌握。同时注重理论知识与实践相结合，使学生通过实践深化对理论的理解，学会并掌握理论方法的实际运用。

（3）在教材中加大能力训练部分的比重，使学生比较熟练地应用计算机知识和技术解决实际问题，既注重培养学生分析问题的能力，也注重培养学生思考问题、解决问题的能力。

（4）教材采用“任务驱动”的编写方式，以实际问题引出相关原理和概念，在讲述实例的过程中将本章的知识点融入，通过分析归纳，介绍解决工程实际问题的思想和方法，然后进行概括总结，使教材内容层次清晰，脉络分明，可读性、可操作性强。同时，引入案例教学和启发式教学方法，便于激发学习兴趣。

（5）教材在内容编排上，力求由浅入深，循序渐进，举一反三，突出重点，通俗易懂。采用模块化结构，兼顾不同层次的需求，在具体授课时可根据各校的教学计划在内容上适当加以取舍。此外还注重了配套教材的编写，如课程学习辅导、实验指导、综合实训、课程设计指导等，注重多媒体的教学方式以及配套课件的制作。

（6）大部分教材配有电子教案，以使教材向多元化、多媒体化发展，满足广大教师进行多媒体教学的需要。电子教案用 PowerPoint 制作，教师可根据授课情况任意修改。相关教案的具体情况请到中国水利水电出版社网站 www.waterpub.com.cn 下载。此外还提供相关教材中所有程序的源代码，方便教师直接切换到系统环境中教学，提高教学效果。

总之，本套规划教材凝聚了众多长期在教学、科研一线工作的教师及科研人员的教学科研经验和智慧，内容新颖，结构完整，概念清晰，深入浅出，通俗易懂，可读性、可操作性和实用性强。本套规划教材适用于应用型高等院校各专业，也可作为本科院校举办的应用技术专业的课程教材，此外还可作为职业技术学院和民办高校、成人教育的教材以及从事工程应用的技术人员的自学参考资料。

我们感谢该套规划教材的各位作者为教材的出版所做出的贡献，也感谢中国水利水电出版社为选题、立项、编审所做出的努力。我们相信，随着我国高等教育的不断发展和高校教学改革的不断深入，具有示范性并适应应用型人才培养的精品课程教材必将进一步促进我国高等院校教学质量的提高。

我们期待广大读者对本套规划教材提出宝贵意见，以便进一步修订，使该套规划教材不断完善。

21 世纪高等院校规划教材编委会

2004 年 8 月

前　言

在信息化社会中，人们对计算机网络的依赖日益增强。越来越多的信息和重要数据资源存储和传输于网络中，通过网络获取和交换信息的方式已成为当前主要的信息沟通方式之一。与此同时，由于网络安全事件频繁发生，使得网络安全成为倍受关注的问题。尤其是网络上各种新业务（如电子商务、网络银行等）的兴起以及各种专用网络（如金融网）的建设，对网络的安全性提出了更高的要求。攻击、入侵行为和病毒的传播严重威胁着网络中各类资源的安全性，极大地损害了网络使用者的利益，也为网络应用的健康发展带来巨大的障碍。因此，网络安全问题已成为各国政府普遍关注的问题，网络安全技术也成为信息技术领域的重要研究课题。

网络安全涉及硬件平台、软件系统、基础协议等方方面面的问题，复杂而多变。只有经过系统的学习和训练，才能对网络安全知识有全面的理解和掌握。本书从网络安全的基本理论和技术出发，深入浅出、循序渐进地讲述了网络安全的基本原理、技术应用及配置方法，内容全面，通俗易懂，理论与实践相得益彰。全书分为 11 章，内容涉及：网络安全体系结构、密码学基础、密码学应用、防火墙、攻击技术、病毒与防范、入侵检测、WWW 安全、E-mail 安全、操作系统安全。

本书的写作目的是帮助读者了解网络所面临的各种安全威胁，掌握网络安全的基本原理，掌握保障网络安全的主要技术和方法，学会如何在开放的网络环境中保护信息和数据，防止黑客和病毒的侵害。在学习本教材之前，读者应具备编程语言、计算机网络、操作系统等方面的基础知识。本书适合作为计算机及相关专业的学生教材或参考书，也可作为对网络安全感兴趣的初学者的自学教材。

本书的主要特点是：

- ✧ **注重理论与实践相结合**：每章都配有应用实例，一方面可以帮助学生对理论知识的理解和掌握；另一方面，学以致用可以提高学生的学习兴趣、增加学习动力，也有助于提高学生的实践能力。
- ✧ **内容丰富、科学合理**：本书在选材时充分考虑学生的基础和能力，在协调内容的深度、广度、难度的关系以及理论和应用的比例方面，都做了深入的考虑，在保证科学性和实用性的同时，尽量做到深入浅出、通俗易懂。

本书由戚文静、刘学主编，并执笔编写了 1、2、3、4、5、6、8、10 等章节内容，孙鹏、赵秀梅、秦松、杜向华等老师参加了第 7、9、11 章部分内容的编写工作，参加本书编写工作的还有赵敬、杨云、刘倩、杨艳春、董艳丽、王红、张磊等。本书在编写过程中参阅了大量的中外文献及安全网站，从中获得了很多启示和帮助，在此一并感谢。

由于网络安全是一门内容广博、不断发展的学科，加之作者水平有限，书中的疏漏和不足在所难免，敬请读者批评指正。作者的 E-mail：wenjing_qi@21cn.com。

编　者

2005 年 7 月

目　　录

第 1 章　网络安全概述

本章学习目标

本章介绍了网络安全的基本概念和术语，分析了网络安全现状及影响网络安全的因素；阐述了网络安全对于政治、经济、军事等方面的重要作用；最后分析了国内外对信息安全的重视和立法情况。通过本章的学习，应达到以下目标：

- 理解网络安全的基本概念和术语
- 了解目前主要的网络安全问题和安全威胁
- 理解基本的网络安全模型及功能
- 了解网络和信息安全的重要性
- 了解国内外的信息安全保障体系

自 20 世纪 90 年代以来，互联网在全球呈爆炸式增长，这是最初的互联网的发明者们始料未及的。Internet 的历史可以追溯到 1969 年美国国防部高级发展研究署（ARPA）建立的 APARNET 网。这个网络最初用于使军方的各种计算机能够相互通信，通过一组叫做 TCP/IP 的通信协议将军方的各种不同的计算机互相连接起来。随着 APARNET 的发展，它逐渐成为目前我们通常所说的国际互联网 Internet。Internet 已经不再局限于美国本土，也不再局限于军事用途。目前，通过网络获取和交换信息的方式已成为主要的信息沟通方式，并且这种趋势还在不断地发展。网络上各种新业务（如电子商务、网络银行等）的兴起以及各种专用网络（如金融网）的建设，对网络的安全性提出了更高的要求，而如何保障网络安全成为目前一个亟待解决的问题。

1.1　网络安全的基本概念

1.1.1　网络安全的定义及相关术语

1. 网络安全的定义

在解释网络安全这个术语之前，首先要明确计算机网络的定义。计算机网络是地理上分散的多台自主计算机互联的集合，这些计算机遵循约定的通信协议，与通信设备、通信链路及网络软件共同实现信息交互、资源共享、协同工作及在线处理等功能。

所以，从广义上说，网络安全包括网络硬件资源及信息资源的安全性。硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等。要实现信息快速、安全的交换，一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件以及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性、真实性等是网络安全

研究的重要课题，也是本书涉及的重点内容。

从用户角度看，网络安全主要是保障个人数据或企业的信息在网络中的保密性、完整性、不可否认性，防止信息的泄露和破坏，防止信息资源的非授权访问。对于网络管理者来说，网络安全的主要任务是保障合法用户正常使用网络资源，避免病毒、拒绝服务、远程控制、非授权访问等安全威胁，及时发现安全漏洞，制止攻击行为等。从教育和意识形态方面，网络安全主要是保障信息内容的合法与健康，控制含不良内容的信息在网络中的传播。例如英国实施的“安全网络 R-3 号”计划，其目的就是打击网络上的犯罪行为，防止 Internet 上不健康内容的泛滥。

可见网络安全的内容是十分广泛的，不同的人群对其有不同的理解。我们在此对网络安全下一个通用的定义：网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，保证网络系统正常运行、网络服务不中断。

2. 网络安全的属性

在美国国家信息基础设施（NII）的文献中，给出了安全的 5 个属性：可用性、机密性、完整性、可靠性和不可抵赖性。这 5 个属性适用于国家信息基础设施的各个领域，如：教育、娱乐、医疗、运输、国家安全、通信等。

（1）可用性。可用性是指得到授权的实体在需要时可以得到所需要的网络资源和服务。由于网络最基本的功能就是为用户提供信息和通信服务，而用户对信息和通信需求是随机的（内容的随机性和时间的随机性）、多方面的（文字、语音、图像等），有的用户还对服务的实时性有较高的要求。网络必须能够保证所有用户的通信需要，一个授权用户无论何时提出要求，网络必须是可用的，不能拒绝用户要求。攻击者常会采用一些手段来占用或破坏系统的资源，以阻止合法用户使用网络资源，这就是对网络可用性的攻击。对于针对网络可用性的攻击，一方面要采取物理加固技术，保障物理设备安全、可靠地工作；另一方面通过访问控制机制，阻止非法访问进入网络。

（2）机密性。机密性是指网络中的信息不被非授权实体（包括用户和进程等）获取与使用。这些信息不仅指国家机密，也包括企业和社会团体的商业秘密和工作秘密，还包括个人的秘密（如银行账号）和个人隐私（如邮件、浏览习惯）等。网络在人们生活中的广泛使用，使人们对网络机密性的要求提高。用于保障网络机密性的主要技术是密码技术。在网络的不同层次上有不同的机制来保障机密性。在物理层上，主要是采取电磁屏蔽技术、干扰及跳频技术来防止电磁辐射造成的信息外泄；在网络层、传输层及应用层主要采用加密、路由控制、访问控制、审计等方法来保证信息的机密性。

（3）完整性。完整性是指网络信息的真实可信性，即网络中的信息不会被偶然或者蓄意地进行删除、修改、伪造、插入等破坏，保证授权用户得到的信息是真实的。只有具有修改权限的实体才能修改信息，如果信息被未经授权的实体修改了或在传输过程中出现了错误，信息的使用者应能够通过一定的方式判断出信息是否真实可靠。

（4）可靠性。可靠性是指系统在规定的条件下和规定的时间内，完成规定功能的概率。可靠性是网络安全最基本的要求之一。目前对于网络可靠性的研究主要偏重于硬件可靠性的研究，主要采用硬件冗余、提高研究质量和精确度等方法。实际上，软件的可靠性、人员的可靠性和环境的可靠性在保证系统可靠性方面也是非常重要的。

（5）不可抵赖性。不可抵赖性也称为不可否认性。是指通信的双方在通信过程中，对于

自己所发送或接收的消息不可抵赖。即发送者不能抵赖他发送过消息的事实和消息内容，而接收者也不能抵赖其接收到消息的事实和内容。

1.1.2　主要的网络安全威胁

1. 网络安全威胁的定义及分类

所谓的网络安全威胁是指某个实体（人、事件、程序等）对某一网络资源的机密性、完整性、可用性及可靠性等可能造成的危害。安全威胁可分成故意的（如系统入侵）和偶然的（如信息被发到错误地址）两类。故意威胁又可进一步分成被动威胁和主动威胁两类。被动威胁只对信息进行监听，而不对其修改和破坏。主动威胁则是对信息进行故意篡改和破坏，使合法用户得不到可用信息。实际上，目前没有统一、明确的方法对安全威胁进行分类和界定，但为了理解安全服务的作用，人们总结了计算机网络及通信中常遇到的一些威胁。

（1）对信息通信的威胁。用户在网络通信过程中，通常遇到的威胁可分为两类，一类为主动攻击，攻击者通过网络将虚假信息或计算机病毒传入信息系统内部，破坏信息的真实性、完整性及可用性，即造成通信中断、通信内容破坏甚至系统无法正常运行等较严重后果的攻击行为。另一类为被动攻击，攻击者截获、窃取通信信息，损害信息的机密性。被动攻击不易被用户发现，具有较大的欺骗性。对信息通信的威胁主要方式如图 1-1 所示。

- 中断：是指攻击者使系统的资源受损或不可用，从而使系统的通信服务不能进行，属于主动威胁。
- 截获：是指攻击者非法获得了对一个资源的访问，并从中窃取了有用的信息或服务，属于被动威胁。
- 篡改：是指攻击者未经授权访问并改动了资源，从而使合法用户得到虚假的信息或错误的服务等，属于主动攻击。
- 伪造：是个攻击者未经许可而在系统中制造出假的信息源、信息或服务，欺骗接收者，属于主动攻击。

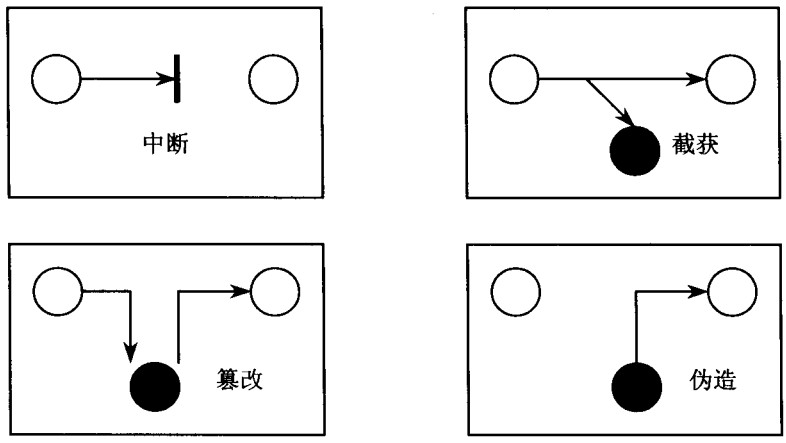


图 1-1　通信过程中的四种攻击方式

对通信的保护主要采用加密方法。

（2）对信息存储的威胁。对于存储在计算机存储设备中的数据，也存在着同样严重的威

胁。攻击者获得对系统的访问控制权后，就可以浏览存储设备中的数据、软件等信息，窃取有用信息，破坏数据的机密性。如果对存储设备中的数据进行删除和修改，则破坏信息的完整性、真实性和可用性。对信息存储的安全保护主要通过访问控制和数据加密方法来实现。

（3）对信息处理的威胁。信息在进行加工和处理的过程中，通常以明文形式出现，加密保护不能用于处理过程中的信息。因此，在处理过程中信息极易受到攻击和破坏，造成严重损失。另外，信息在处理过程中，也可能由于信息处理系统本身软、硬件的缺陷或脆弱性等原因，使信息的安全性遭到损害。

2. 网络安全威胁的主要表现形式

网络中的信息和设备所面临的安全威胁有着多种多样的具体表现形式，而且威胁的表现形式随着软硬件技术的不断发展不断地进化，这里简单地总结了一些典型的危害网络安全的行为，如表 1-1 所示。

表 1-1 威胁的主要表现形式

威胁	描述
授权侵犯	为某一特定目的被授权使用某个系统的人，将该系统用作其他未授权的目的
旁路控制	攻击者发掘系统的缺陷或安全弱点，从而渗入系统
拒绝服务	合法访问被无条件拒绝和推迟
窃听	在监视通信的过程中获得信息
电磁泄露	从设备发出的辐射中泄露信息
非法使用	资源被某个未授权的人或以未授权的方式使用
信息泄露	信息泄露给未授权实体
完整性破坏	对数据的未授权创建、修改或破坏造成数据一致性损害
假冒	一个实体假装成另外一个实体
物理侵入	入侵者绕过物理控制而获得对系统的访问权
重放	出于非法目的而重新发送截获的合法通信数据的拷贝
否认	参与通信的一方事后否认曾经发生过此次通信
资源耗尽	某一资源被故意超负荷使用，导致其他用户的服务被中断
业务流分析	通过对业务流模式进行观察（有，无，数量，方向，频率），而使信息泄露给未授权实体
特洛伊木马	含有觉察不出或无害程序段的软件，当它被运行时，会损害用户的安全
陷门	在某个系统或文件中预先设置的“机关”，使得当提供特定的输入时，允许违反安全策略
人员疏忽	一个授权的人出于某种动机或由于粗心将信息泄露给未授权的人

3. 构成威胁的因素

影响信息系统的因素很多，这些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；还可能是黑客对网络资源的非法使用。归结起来，针对信息系统的威胁主要有以下 3 个因素：

（1）环境和灾害因素。温度、湿度、供电、火灾、水灾、地震、静电、灰尘、雷电、强电磁场、电磁脉冲等，均会破坏数据和影响信息系统的正常工作。灾害轻则造成业务工作混乱，重则造成系统中断甚至造成无法估量的损失。如 1999 年 8 月吉林省某电信业务部门的通信设