21世纪

21世纪高等院校规划教材

Internet

网络安全原理与应用

（第二版）

主　编　戚文静　刘　学

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

（第二版）

主　编　戚文静　刘　学

中国水利水电出版社
www.waterpub.com.cn

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：网络安全概述、网络体系结构及协议基础、密码学基础、密码学应用、防火墙技术、网络攻击和防范、入侵检测技术、病毒与防范、WWW安全、电子邮件安全、无线网络安全等。

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

本书可作为高等院校计算机、信息安全、网络工程、信息工程等专业信息安全课程的教材，也可作为成人高校、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，还可作为信息安全的培训教材及信息技术人员的参考书。

本书配有免费的电子教案，读者可以从中国水利水电出版社网站和万水书苑上下载，网址为：http://www.waterpub.com.cn/softdown/和http://www.wsbookshow.com。

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. -- 2版
. -- 北京 : 中国水利水电出版社，2013.2
21世纪高等院校规划教材
ISBN 978-7-5170-0607-7

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

中国版本图书馆CIP数据核字(2013)第014440号

策划编辑：雷顺加　　责任编辑：宋俊娥　　加工编辑：宋　杨　　封面设计：李　佳

书　名	21世纪高等院校规划教材 **网络安全原理与应用（第二版）**
作　者	主　编　戚文静　刘　学
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 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	三河市铭浩彩色印装有限公司
规　格	184mm×260mm　16开本　21印张　518千字
版　次	2005年9月第1版　2005年9月第1次印刷 2013年2月第2版　2013年2月第1次印刷
印　数	0001—4000册
定　价	36.00元

第二版前言

随着网络技术的成熟和不断发展，计算机网络已经成为人类生活中不可或缺的组成部分。越来越多的信息和重要数据利用网络存储和交换，电子商务、网络银行等网络业务的飞速发展，给人类的生产和生活带来了快捷与方便。但与此同时，攻击、入侵和病毒等问题也严重威胁着网络中各类资源和应用的安全性，极大地损害了网络使用者的利益，给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”是一门综合计算机、网络、通信、密码等技术的综合性学科，涉及硬件平台、软件系统、基础协议各方面的问题，内容复杂，形式多变。本书从网络安全的基本原理和技术基础出发，力求以浅显易懂、循序渐进的方式讲述网络安全的基本原理、技术应用及配置方法。全书分为 11 章，内容涉及：网络安全概述、网络体系结构及协议基础、密码学基础、密码学应用、防火墙技术、网络攻击和防范、入侵检测技术、病毒与防范、WWW 安全、电子邮件安全、无线网络安全等。

本书在第一版的基础上，结合一线教师和学生的反馈意见，对内容进行了适当的调整和补充，主要包括：对内容的系统性进行调整，使之在体系上更科学，在逻辑上更合理；针对网络安全对内容实效性要求高的特点，对内容的时效性进行检查和更新，去掉过时的内容，增加当前最新的技术和发展动态，保持资料的新鲜性；增加习题的数量，便于读者复习和加强对学习内容的理解；更加突出实践能力的培养，拓展课后实践题目的题材和方式，使读者能够更好地结合实际进行学习，做到学有所用、学以致用。

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，学会在开放的网络环境中保护信息和数据。本书注重理论与实践相结合，每章都配有应用实例，一方面有助于读者对理论知识的理解和掌握；另一方面，学以致用可以提高读者的学习兴趣、增加学习动力，也有助于提高读者的实践能力。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、刘学担任主编，并执笔编写了第 1、3、4、5、6、8、10、11 等章节的主要内容，孙鹏、李国文、张艳、袁卫华、杜向华、许丽娜、徐功文、柳楠等老师参与了第 2、6、7、8、9 章部分内容的编写及教学资源建设工作，赵秀梅、秦松、赵敬、赵莉、魏代森等老师参加了本书大纲讨论、内容校对工作。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 地址为：qiwj@hotmail.edu.cn。

编　者

2012 年 12 月

第一版前言

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，一方面可以帮助读者对理论知识进行理解和掌握；另一方面，学以致用可以提高读者的学习兴趣、增加学习动力，也有助于提高读者的实践能力。
- 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、刘学担任主编，并执笔编写了第 1、2、3、4、5、6、8、10 等章节内容，孙鹏、赵秀梅、秦松、杜向华等老师参与了第 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 地址为：wenjing_qi@21cn.com。

编 者

2005 年 7 月

目　　录

第 1 章　网络安全概述

本章介绍网络安全的基本概念和术语，分析网络安全现状及影响网络安全的因素；阐述网络安全对于政治、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 年美国国防部高级研究计划署（ARPA）建立的 ARPANET。这个网络最初用于军方的各种计算机之间的相互通信，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 ARPANET 的发展，它逐渐成为目前通常所说的国际互联网 Internet。Internet 早已不再局限于美国本土，也不再局限于军事用途，它已发展成为全球性的、高速互联的一个庞大系统，并对人类的生产和生活方式产生了巨大的影响。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，在不同的层面有不同的内涵。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，分别为：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（Availability）。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；另一方面可以通过访问控制机制，阻止非法访问进入网络。

（2）机密性（Confidentiality）。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。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。其中，密码技术是用于保障网络信息机密性的主要技术。

（3）完整性（Integrity）。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删除、修改、伪造、插入等，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。一般通过消息认证码（Message Authentication Code，MAC）的方式来进行完整性的认证，消息认证码是由原始消息经过一定的变换得到的，如通过 Hash 算法来生成消息认证码。

（4）可靠性（Reliability）。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、提高硬件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。在一些关键的应用领域，如航空、航天、电力、通信等，软件可靠性显得尤为重要，在银行、证券等金融服务性行业，其软件系统的可靠性也直接关系到自身的声誉和生存发展竞争力。随着软件系统的规模越来越大、结构越来越复杂，软件的可靠性越来越难以保证。若在软件项目的开发过程中，对可靠性没有提出明确的要求，只注重运行速度、结果的正确性和用户界面的友好性等直接效益因素，而在投入使用后才发现大量可靠性问题，会大大增加软件系统维护的困难和工作量，甚至造成无法投入实际使用的情况。

（5）不可抵赖性（Non-repudiation）。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消息内容。通过身份认证和数字签名技术来实现网络上信息交换或电子商务交易的不可抵赖性。

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，而不对其进行修改和破坏。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。对信息通信的主要威胁如图 1-1 所示。

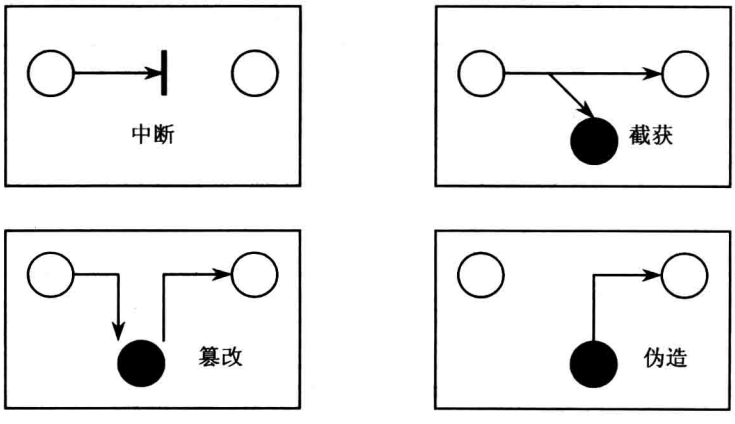

图 1-1　通信过程中的四种攻击方式

- 中断：是指攻击者使系统的资源受损或无法使用，从而使系统无法进行正常的通信和服务，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：是指攻击者未经许可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。

对通信的保护主要借助密码学的方法，通过对信息的加密来保证只有授权的用户才能看到信息的真实内容，通过消息认证及数据签名等技术来防止信息被篡改和伪造。

（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。另外，物理的不安全因素也是信息存储的主要潜在威胁之一，如由于自然灾害和环境因素引发的存储数据损坏。因此，对于重要信息和服务要有必要的备份机制来保障信息或服务被损坏时能够及时得到替代，把损失降到最低。

（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，使信息的安全性和完整性遭到损害。

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、硬件技术的发展不断地进化，这里简单地总结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	从设备发出的电磁辐射中泄露信息
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完整性损害
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

续表

威胁	描述
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（有、无、数量、方向、频率）进行观察，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	授权人员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

影响信息系统安全的因素很多，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。归结起来，针对信息系统的威胁主要有以下 3 类因素：

（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。这类不安全因素对信息的完整性和可用性威胁最大，而对信息的保密性影响较小。如 1999 年 8 月吉林省某电信业务部门的通信设备被雷击中，造成惊人的损失；还有某铁路计算机系统遭受雷击，造成设备损坏、铁路运输中断等。解决这类安全威胁的主要方法是采取有效的物理安全保障措施，完善管理制度，对设备、服务及信息都要有良好的备份和恢复机制。

（2）人为因素。在网络安全问题中，人为的因素是不可忽视的。多数的安全事件是由于人员的疏忽、恶意程序、黑客的主动攻击造成的。人为因素对网络安全的危害性更大，也更难于防御。人为因素可分为有意和无意两种。有意是指人为的恶意攻击、违纪、违法和犯罪。例如，计算机病毒是一种人为编写的恶意代码，具有自我繁殖、相互感染、激活再生等特征。计算机一旦感染病毒，轻者影响系统性能，重者破坏系统资源，甚至造成死机和系统瘫痪。网络为病毒的传播提供了捷径，其危害也更大。黑客攻击是指利用通信软件，通过网络非法进入他人系统，截获或篡改数据，危害信息安全。对于这些有意的安全威胁行为，主要的防范措施包括建立适当的安全监控机制、及时检测和识别威胁、进行报警和响应等。无意是指网络管理员或使用者因工作的疏忽造成失误，没有主观的故意，但同样会对系统造成严重的不良后果。如由于操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享，文件的误删除，输入错误的数据等。人员无意造成的安全问题主要源自 3 个方面，一是网络及系统管理员方面，对系统配置及安全缺乏清醒的认识或整体的考虑，造成系统安全性差，影响网络安全及服务质量；二是程序员方面的问题，程序员开发的软件有安全缺陷，比如常见的缓冲区溢出问题；三是用户方面，用户有责任保护好自己的口令及密钥。以上这些人为的因素威胁到网络信息的机密性、完整性和可用性，防范此类威胁的方法包括防止电磁泄露、完善安全管理制度、制定合适的安全保护策略等，并加强对用户安全意识的教育。

（3）系统自身因素。计算机网络安全保障体系应尽量避免天灾造成的计算机危害，控制、

预防、减少人祸以及系统本身原因造成的计算机危害。尽管近年来计算机网络安全技术取得了巨大的进步，但计算机网络系统的安全性却比以往都更加脆弱。主要表现在它极易受到攻击和侵害、抗打击力和防护力很弱。其脆弱性主要表现在以下几个方面：

1）计算机硬件系统的故障。由于生产工艺或制造商的原因，计算机硬件系统本身有故障而引起系统的不稳定、受电压波动干扰等。硬件系统在工作时会向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件时，应尽可能减少或消除这类安全隐患。

2）软件组件。软件组件的安全隐患是来源于程序设计和软件工程中的问题。包括：软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及代码过长，不可避免地导致软件存在安全脆弱性；不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱。

软件组件可分为 3 类，即操作平台软件、应用平台软件和应用业务软件。这 3 类软件以层次结构构成软件组件体系。操作平台软件处于基础层，维系着系统组件运行的平台，因此操作平台软件的任何风险都可能直接危及或被转移、延伸到应用平台软件。所以，操作平台软件的安全等级应不低于系统安全等级要求。应用平台软件处于中间层，是在操作平台支持下运行的、支持和管理应用业务软件的软件。一方面，应用平台软件可能受到来自操作平台软件风险的影响；另一方面，应用平台软件的任何风险可直接危及或传递给应用业务软件。因此，应用平台软件的安全特性也至关重要。在提供自身安全保障的同时，应用平台软件还必须为应用业务软件提供必要的安全服务功能。应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险都直接表现为信息系统的风险，因此其安全功能的完整性及自身的安全等级必须大于系统安全的最小需求。

3）网络和通信协议。安全问题最多的网络和通信协议是基于 TCP/IP 协议的 Internet 及其通信协议。因为任何接入 Internet 的计算机网络，在理论上和技术实现上已无真正的物理界限，同时在地域上也没有真正的边界。国与国之间、组织与组织之间，以及个人与个人之间的网络界限是依靠协议、约定和管理关系进行逻辑划分的，因而是一种虚拟的网络现实。TCP/IP 协议最初设计的应用环境是美国国防系统的内部网络，这一网络环境是相互信任的，因此，TCP/IP 协议只考虑了互联互通和资源共享的问题，并未考虑来自网络中的大量安全问题。当其推广到全社会的应用环境之后，信任问题发生了，因此 Internet 充满安全隐患就不难理解了。

总之，系统自身的脆弱和不足，是造成信息系统安全问题的内部根源，各种人为因素正是利用系统的脆弱性使各种威胁变成现实。所以，保障网络的安全需要从几个方面考虑。首先，从根源出发，设计高可靠性的硬件和软件；其次就是要加强管理，设置有效的安全防范和管理措施；还有很重要的一点就是应当加强宣传和培训，增强用户的安全意识。

1.1.3 网络安全策略

安全策略是指在某个安全区域内，所有与安全活动相关的一套规则，这些规则由此安全区域内所设立的一个权威建立。如果说网络安全的目标是一座大厦的话，那么相应的安全策略就是施工的蓝图，它使网络建设和管理过程中的安全工作避免盲目性。但是，它并没有得到足够的重视。国际调查显示，目前 55%的企业网没有自己的安全策略，仅靠一些简单的安全措

施来保障网络安全，这些安全措施可能存在互相分立、互相矛盾、互相重复、各自为战等问题，既无法保障网络的安全可靠，又影响网络的服务性能，并且随着网络运行而对安全措施进行不断的修补，使整个安全系统愈加臃肿不堪，难于使用和维护。

网络安全策略包括对企业的各种网络服务的安全层次和用户的权限进行分类、确定管理员的安全职责、如何实施安全故障处理、网络拓扑结构、入侵和攻击的防御和检测、备份和灾难恢复等内容。本书中所说的安全策略主要指系统安全策略，主要涉及四个大的方面，分别为：物理安全策略、访问控制策略、信息加密策略、安全管理策略。

1. 物理安全策略

制定物理安全策略的目的是保护路由器、交换机、工作站、各种网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击；验证用户的身份和使用权限，防止用户越权操作；确保网络设备有一个良好的电磁兼容工作环境；建立完备的机房安全管理制度，妥善保管备份磁带和文档资料；防止非法人员进入机房进行偷窃和破坏活动。

2. 访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。下面分述各种访问控制策略。

（1）入网访问控制。入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为 3 个步骤，分别为：用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查。三道关卡中只要任何一关未通过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令，否则，用户将被拒在网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密。经过加密的口令，即使是系统管理员也难以得到它。用户还可采用一次性用户口令，也可用便携式验证器（如智能卡）来验证用户的身份。

网络管理员应该可以控制和限制普通用户的账号使用、访问网络的时间和方式。用户名或用户账号是所有计算机系统中最基本的安全形式。用户账号应只有系统管理员才能建立。用户口令应是每个用户访问网络所必须提交的“证件”，用户可以修改自己的口令，但系统管理员应该可以控制口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后，再进一步履行用户账号的默认限制检查。网络应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应能对用户的账号加以限制。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

（2）网络的权限控制。网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。可以根据访问权限将用

户分为以下几类：特殊用户（即系统管理员）；一般用户，系统管理员根据他们的实际需要为他们分配操作权限；审计用户，负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用一个访问控制表来描述。

（3）目录级安全控制。网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可以进一步指定对目录下的子目录和文件的访问权限。对目录和文件的访问权限一般有 8 种，分别为：系统管理员（Supervisor）权限、读（Read）权限、写（Write）权限、创建（Create）权限、删除（Erase）权限、修改（Modify）权限、文件查找（File Scan）权限、存取控制（Access Control）权限。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8 种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

（4）属性安全控制。当使用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

（5）网络服务器安全控制。网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，执行安装和删除软件等操作。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

（6）网络监测和锁定控制。网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形、文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

（7）网络端口和结点的安全控制。网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护，并以加密的形式来识别结点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用于防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

（8）防火墙控制。防火墙是一种保护计算机网络安全的技术性措施，它是一个用于阻止黑客访问某个机构网络的屏障，是控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

3. 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网络会话的完整性。网络加密可以在链路层、网络层、应用层等进行，分别对应网络体系结构中的不同层次形成加密通信通道。用户可以根据不同的需要，选择适当的加密方式。

加密过程由加密算法来具体实施。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方使用的密钥是否相同来分类，可以将这些加密算法分为