DVD 附赠光盘

大容量语音教学视频
直观引导配置操作

网管天下

网络安全

陈忠平 李旎 刘青凤 等编著

理论深刻透彻
配置直观明了

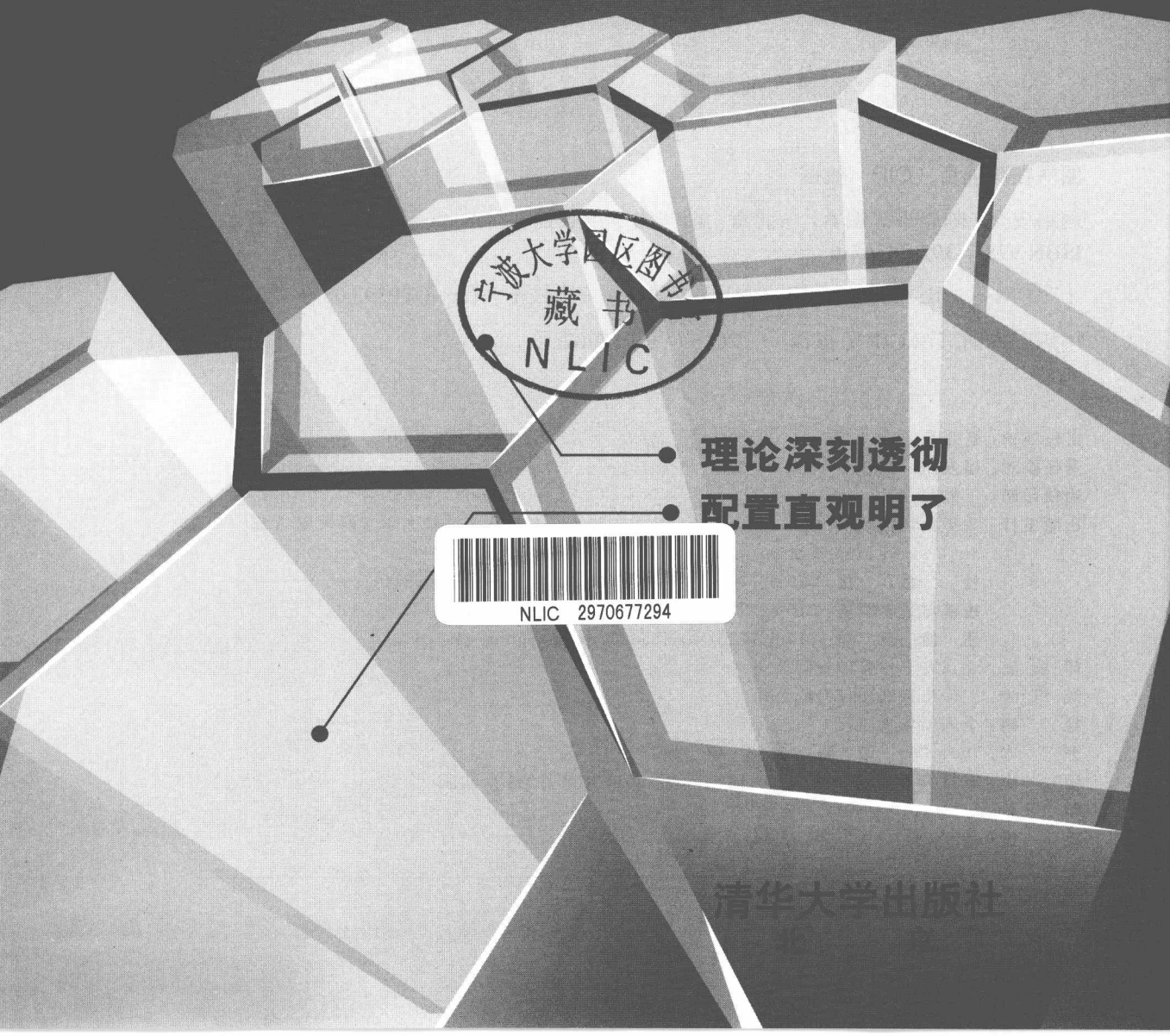
清华大学出版社

DVD 附赠光盘 | 大容量语音教学视频 直观引导配置操作

网管天下

网络安全

陈忠平 李旎 刘青凤 等编著



理论深刻透彻

配置直观明了

清华大学出版社

内 容 简 介

本书介绍网络安全方面的知识，具体包括认识网络安全、网络操作系统安全、网络设备安全、防火墙安全体系、加密技术及备份技术等。本书还插入大量的网络工具列表内容，让用户充分了解用于保证网络安全所需的各种关键技术和工具的应用等。

本书适用于中小企业网络管理人员、企业 IT 经理和网络管理员以及网络安全工程师自学选用，也可作为高校的选用教材和参考手册。

图书在版编目（CIP）数据

网络安全 / 陈忠平等编著. —北京：清华大学出版社，2011.2
ISBN 978-7-302-24365-6

Ⅰ. ①网…　Ⅱ. ①陈…　Ⅲ. ①计算机网络－安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 257902 号

责任编辑：夏兆彦
责任校对：徐俊伟
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编：**100084
社　总　机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：190×260　**印　张：**27.25　**字　数：**677 千字
版　　次：2011 年 2 月第 1 版　　**印　　次：**2011 年 2 月第1 次印刷
印　　数：1～4000
定　　价：49.80 元

产品编号：031003-01

FOREWORD

前言

网络已成为主要的数据传输和信息交换平台，许多部门和企业在网上构建了关键的业务流程。网络安全和信息安全是保障网上业务正常运行的关键，并已日益成为网络用户普遍关注的焦点问题。

本书介绍网络安全方面的知识，具体包括认识网络安全、网络操作系统安全、网络设备安全、防火墙安全体系、加密技术及备份技术等。本书还插入大量的网络工具列表内容，让用户充分了解用于保证网络安全所需的各种关键技术和工具的应用等。

1. 本书内容

本书分篇介绍与网络安全相关的重点内容，语言简单易懂、内容深入浅出，并插入大量的实例案例图形，使用户能更好地掌握该方面的技术。

本书共分 5 篇 13 章。

第一篇为认识网络安全（包含第 1～3 章），介绍网络安全的基础内容，使用户拥有扎实的理论知识。

第 1 章为网络安全基础，详细介绍网络安全概念、网络安全评价标准、常见的安全威胁与攻击、网络安全的现状和发展趋势等。

第 2 章为计算病毒，详细介绍计算机病毒概述、计算机病毒的危害、常见的计算机病毒类型、网络工具列表等。

第 3 章为网络攻击与防范，详细介绍黑客概述、常见的网络攻击、木马攻击与分析、木马的攻击防护技术等。

第二篇为网络操作系统安全(包含第 4～6 章)，介绍 Windows Server 2008 服务器操作系统中的安全应用等。

第 4 章为操作系统加固，详细介绍操作系统安装与更新、Internet 连接防火墙、安全配置向导、默认共享等。

第 5 章为系统安全策略，详细介绍账户策略、审核策略、限制用户登录、安全配置和分析、IPSec 安全策略等。

第 6 章为系统漏洞修补，详细介绍漏洞概述、漏洞预警、漏洞更新等。

第三篇为网络设备安全（包含第 7～8 章），典型介绍网络中交换机和路由器的安全配置技术。

第 7 章为交换机安全配置，详细介绍基于端口的传输控制、PVLAN 安全、基于端口的认证安全、配置 RMON 等。

第 8 章为路由器安全配置，详细介绍访问列表安全、网络地址转换、网络攻击安全防范、使用 SDM 配置路由器等。

第四篇为防火墙安全体系（包含第 9～11 章），介绍防火墙基础及

安全设置、Cisco PIX 防火墙的应用、入侵检测系统等。

第 9 章为防火墙基础，则详细介绍防火墙概述、防火墙的分类、防火墙的体系结构、防火墙的主要应用等。

第 10 章为 Cisco PIX 防火墙，详细介绍 PIX 防火墙的概述、PIX 防火墙的基本使用、PIX 防火墙的高级配置、PIX 防火墙系统日志、PIX 防火墙攻击防护等。

第 11 章为入侵检测系统，详细介绍 IDS 的概述、IDS 系统分类、IDS 的检测方式、IDS 的应用、IDS 的发展方向等。

第五篇为加密技术及备份技术（包含第 12、13 章），介绍网络安全中的公钥、数据加密技术和数据备份等。

第 12 章为公钥基础设施，详细介绍 PKI 基础、PKI 服务和实现、PKI 的体系结构、权限管理基础设施 PMI 概况、属性权威和权限管理、基于 PMI 建立安全应用等。

第 13 章为数据加密及备份，详细介绍密钥密码学、数据加密技术、EFS 文件的加密与解密、数据的备份与恢复、数据库的备份与恢复等。

2. 本书特色

- 面向职业角度和网管考试安排图书内容，增强了本书的实用性。内容全面，结构完善，形成系统而完备的网管知识体系。
- 通过相关企业征集 30 多个有代表性的、工作中经常应用的一些实例，在书中穿插介绍。将理论知识落实到日常的网络应用实践中，提高读者网络管理的实际应用能力。
- 由具有专业的企业服务器安全管理和网络维护经验的人员编写，对企业环境中面临的安全问题以及解决措施有独特的见解，并能用通俗易懂的语言，深入浅出地表达出来。
- 增加“网管心得”，介绍网管的实际工作环境和职业要求，便于没有工作经验的网管与相关职业接轨，掌握工作中必备技能或者相关知识。

3. 读者定位

本书由浅入深，通俗易懂，注重实践，适用于中小企业网络管理人员、企业 IT 经理和网络管理员，以及网络安全工程师自学选用，也可作为高校的选用教材和参考手册。

参与本书编写的除了封面署名人员外，还有胡家宏、王海峰、王健、张勇、冯冠、刘好增、赵俊昌、祁凯、孙江玮、田成军、刘俊杰、王泽波、张银鹤、阎迎利、何方、李海庆、王树兴、朱俊成、康显丽、崔群法、孙岩、秦长海、宋素萍、倪宝童、王立新、温玲娟、于会芳、赵喜来、杨宁宁、郭晓俊、方宁、牛丽萍、郭新志、王黎、安征、亢凤林、李海峰等。由于时间仓促，加之编者水平有限，书中疏漏之处在所难免，欢迎读者朋友登录清华大学出版社的网站 www.tup.com.cn 与我们联系，帮助我们改进提高。

编　者

2010 年 7 月

CONTENTS

目录

第一篇　认识网络安全

第二篇 网络操作系统安全

第三篇 网络设备安全

第四篇 防火墙安全体系

第五篇 加密技术及备份技术

第一篇　认识网络安全

第1章 网络安全基础

目前，计算机网络的普及度越来越大，不仅是人们工作、学习和生活的便捷工具，同时也为人们提供了各种各样的资源。但是，不得不注意到，网络虽然功能强大，但它有脆弱、易受到攻击的一面。

据美国联绑调查局（FBI）统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。在我国，每年因黑客入侵、计算机病毒对网络的破坏也造成了巨大的经济损失。因此，无论何时网络安全问题不容忽视。

本章从网络安全定义、网络安全概念、常见的安全威胁与攻击、网络安全的现状和发展趋势等方面进行学习，使读者对网络安全有清晰的认识。

本章学习要点：

- 了解网络安全的定义、安全模型及其研究的主要内容
- 熟悉安全的攻防体系结构和层次体系结构
- 了解网络安全评价标准及网络安全自身的脆弱性
- 掌握对网络安全提出的防范建议以及网络所面临的安全威胁种类
- 熟悉网络安全策略设计原则

1.1 网络安全基本概念

随着网络威胁的增加，人们逐渐建立了网络安全研究的相关技术和理论，提出了网络安全的模型、体系结构和目标等。本节从各个方面详细介绍有关网络安全的基础知识。

1.1.1 网络安全概述

网络安全从其本质上来讲就是网络上的信息安全，涉及的领域相当广泛，这是因为在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。凡是涉及网络上的信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全所要研究的领域。

严格地说，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，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断，这包括如下含义。

- 网络运行系统安全，即保证信息处理和传输系统的安全。
- 网络上系统信息的安全。

❑ 网络上信息传播的安全，即信息传播后果的安全。

❑ 网络上信息内容的安全，即狭义的“信息安全”。

计算机网络安全的主要内容不仅包括硬件设备、管理控制网络的软件方面，同时也包括共享的资源，快捷的网络服务等方面。具体来讲包括如下内容。

❑ 网络实体安全

计算机机房的物理条件、物理环境及设施的安全，计算机硬件、附属设备及网络传输线路的安装及配置等。

❑ 软件安全

保护网络系统不被非法入侵，系统软件与应用软件不被非法复制、篡改、不受病毒的侵害等。

❑ 数据安全

保护数据不被非法存取，确保其完整性、一致性、机密性等。

❑ 安全管理

在运行期间对突发事件的安全处理，包括采取计算机安全技术，建立安全管理制度，开展安全审计，进行风险分析等内容。

❑ 数据保密性

信息不泄露给非授权的用户、实体或过程，或供其利用的特性。在网络系统的各个层次上有不同的机密性及相应的防范措施。例如，在物理层，要保证系统实体不以电磁的方式（电磁辐射、电磁泄露等）向外泄露信息，在数据处理、传输层面，要保证数据在传输、存储过程中不被非法获取、解析，主要的防范措施是采用密码技术。

❑ 数据完整性

数据完整性指数据在未经授权时不能改变其特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性，完整性要求信息的原样，即信息的正确生成、正确存储和正确传输。影响网络信息完整性的主要因素包括设备故障、传输、处理或存储过程中产生的误码、网络攻击、计算机病毒等，其主要防范措施是校验与认证技术。

❑ 可用性

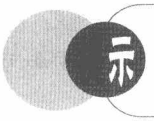
网络信息系统最基本的功能是向用户提供服务，而用户所要求的服务是多层次的、随机的，可用性是指可被授权实体访问，并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

❑ 可控性

可控性指对信息的传播及内容具有控制能力，保障系统依据授权提供服务，使系统任何时候不被非授权用户使用，对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取防范措施。

❑ 可审查性

提供历史事件的记录，对出现的网络安全问题提供调查的依据和手段。



完整性与保密性不同，保密性要求信息不被泄露给未授权用户，而完整性则是要求信息不受各种原因的破坏。

1.1.2　安全模型

随着信息化社会的网络化，各国的政治、外交、国防等领域越来越依赖于计算机网络，因此，计算机网络安全的地位日趋重要。

从宏观上讲，目前国家、政府部门正在不断制定和完善网络安全的法律、网络安全标准等；而从具体角度讲，针对企业、集团、高校等网络用户而言，拥有经济合理的网络安全设备是保障网络安全的硬件技术，能够协调进行有效的安全管理工作是能够保障网络长期安全、相对稳定运作的动力。而两者所围绕的核心问题是针对预防的主要网络攻击手段及当前运作实体的经济技术能力建立一个可实施的、合理的、长期有效的网络安全模型。

围绕安全模型设计与实施，将相关的网络安全技术与安全机制方面的工作有机结合起来，才能够有效地保证网络安全。所以，建立合理有效的网络安全模型，无论是对硬件设备的选择，还是对后期网络安全管理工作的开展，都是一个关键技术问题。从而也决定了它在实现网络安全方面不可忽视的重要性。网络安全能否有效地担任职责，这对网络技术的发展，网络时代信息秩序的维护以及企业和单位用户的网络正常运行都奠定了坚实的基础。

目前，在网络安全领域存在较多的网络安全模型。这些安全模型都较好地描述了网络安全的部分特征，又都有各自的侧重点，在各自不同的专业和领域都有着一定程度的应用。

1. 基本模型

在网络信息传输中，为了保证信息传输的安全性，一般需要一个值得信任的第三方负责在源节点和目的节点间进行秘密信息分发，同时当双方发生争执时，起到仲裁的作用。

在基本模型中，通信的双方在进行信息传输前，首先建立起一条逻辑通道，并提供安全的机制和服务来实现在开放网络环境中信息的安全传输，图 1-1 为基本安全模型的示意图。

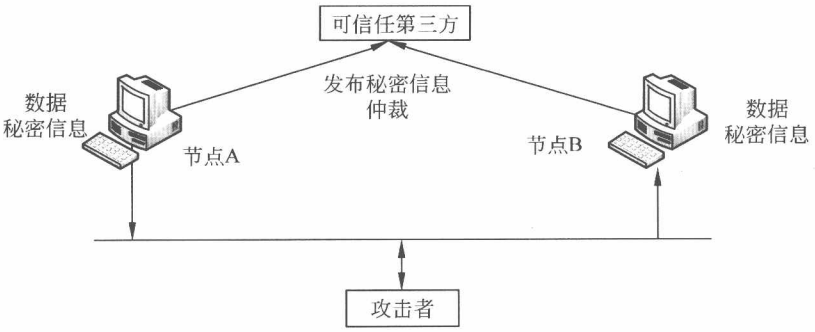


图 1-1　基本安全模型示意图

信息的安全传输主要包括以下两点。

- 从源节点发出的信息，使用信息加密等加密技术对其进行安全的转发，从而实现该信息的保密性，同时也可以在该信息中附加一些特征信息，作为源节点的身份验证。
- 源节点与目的节点应该共享如加密密钥这样的保密信息，这些信息除了发送双方和可信任的第三方之外，对其他用户都是保密的。

2. P2DR 模型

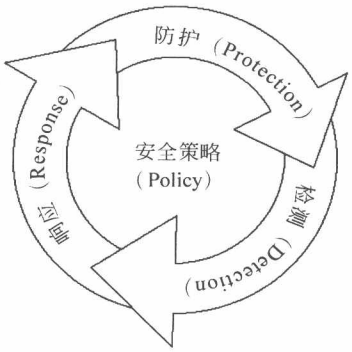


图 1-2　P2DR 模型结构示意图

P2DR 模型是由美国国际互联网安全系统公司（ISS）提出的动态网络安全理论或称为可适应网络安全理论的主要模型。该模型是美国可信计算机系统评价准则（TCSEC）的发展，也是目前被普遍采用的模型，主要由安全策略（Policy）、防护（Protection）、检测（Detection）和响应（Response）4 部分构成。其中，防护、检测和响应构成了一个所谓完整的、动态的安全循环，在安全策略的整体指导下保证信息系统的安全，图 1-2 为其构成示意图。

对于该模型的各组成部分有如下说明。

❑ **安全策略**

安全策略是模型的核心，所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略两个部分。

❑ **防护**

防护是根据系统可能出现的安全问题而采取的预防措施，这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网（VPN）技术、防火墙、安全扫描和数据备份等。

❑ **检测**

当攻击者穿透防护系统时，检测功能就会发挥作用，与防护系统形成互补。检测是动态响应的依据。

❑ **响应**

当系统检测到危及安全的事件、行为、过程时，响应系统就开始工作及对发生事件进行处理，杜绝危害的进一步蔓延扩大，力求系统尚能提供正常服务。响应包括紧急响应和恢复处理两部分，而恢复处理又包括系统恢复和信息恢复。

总之，P2DR 模型是在整体的安全策略的控制和指导下，在综合运用防护工具（如防火墙、操作系统身份认证、加密等）的同时，利用检测工具（如漏洞评估、入侵检测等）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态。防护、检测和响应组成了一个完整的、动态的安全循环，在安全策略的指导下保证信息系统的安全。

1.1.3　网络安全攻防技术

“道高一尺，魔高一丈”，这是网络安全攻击与防御最好的写照。有矛就有盾，也是相互对立的两个方面。而在网络安全中，“攻”和“防”与“矛”和“盾”非常相似。

网络安全的攻防体系结构由网络安全物理基础、网络安全的实施及工具和防御技术三大方面构成，图 1-3 为其结构示意图。

对于用户来讲，如果不知道如何攻击，那么再好的防守也是经不住考验的，目前，常用的攻击技术主要包括 5 个方面。

❑ **网络监听**　自己不主动去攻击别人，在计算机上设置一个程序去监听目标计算机与其

他计算机通信的数据。

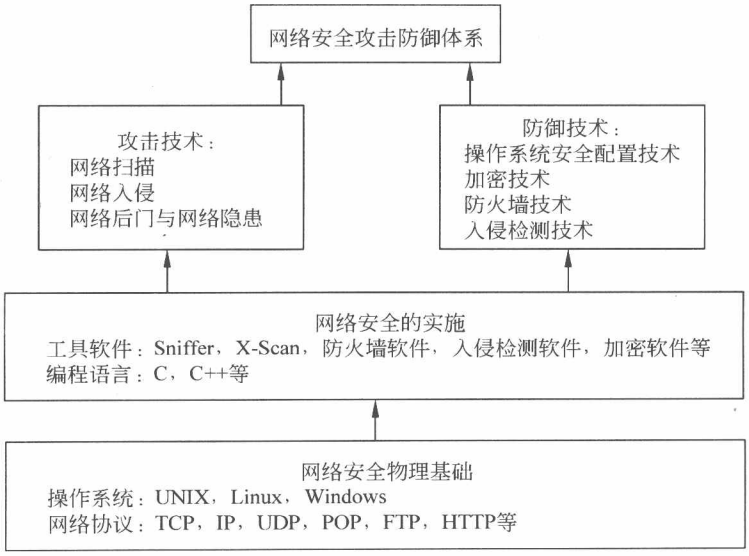


图 1-3 网络安全攻防体系结构

- **网络扫描** 利用程序去扫描目标计算机开放的端口等，目的是发现漏洞，为入侵该计算机作准备。
- **网络入侵** 当探测发现对方计算机存在漏洞以后，入侵到目标计算机以获取信息。
- **网络后门** 成功入侵目标计算机后，为了对“战利品”进行长期控制，在目标计算机中种植木马等。
- **网络隐身** 入侵完毕退出目标计算机后，将自己入侵该计算机的痕迹清除掉，从而防止被对方管理员发现。

对于防御技术通常包括以下 4 个方面。

- **操作系统的安全配置** 操作系统的安全是整个网络安全的关键。
- **加密技术** 为了防止被他人（非法分子）监听和盗取数据，通过加密技术将所有的数据进行加密。
- **防火墙技术** 利用防火墙，对传输的数据进行限制，从而防止系统被入侵或者是减小被入侵的成功率。
- **入侵检测** 如果网络防线最终被攻破了，需要及时发出被入侵的警报。

另外，为了保证网络的安全，用户在软件方面可以选择在技术上已经成熟的安全辅助工具，如抓数据包软件 Sniffer，网络扫描工具 X-Scan 等。另外，如果用户具有较高的编程能力，还可以选择自己编写程序。目前，有关网络安全编程常用的计算机语言有 C、C++或者 Perl 等。

1.1.4 层次体系结构

从层次体系结构上，通常将网络安全划分成物理安全、逻辑安全、操作系统安全和联网安全 4 个层次。

1. 物理安全

物理是指计算机硬件、网络硬件设备等。而物理安全是指整个计算机硬件、网络设备和传输介质等一些实物的安全。通常物理安全包括如下 5 个方面。

❑ 防盗

与其他的物体一样，物理设备（如计算机）也是偷窃者的目标之一，如盗走硬盘、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施以确保计算机设备不会丢失。

❑ 防火

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。

人为事故是指由于操作人员不慎如吸烟、乱扔烟头等，使存在易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火蔓延到机房而引起火灾。

❑ 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电放电火花，造成火灾。还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。

❑ 防雷击

利用传统的避雷针防雷，不但增加雷击概率，还会产生感应雷，而感应雷是电子信息设备被损坏的主要原因之一，也是易燃易爆品被引燃引爆的主要原因。

目前，对于雷击的主要防范措施是根据电气、微电子设备的不同功能及不同受保护程序和所属保护层来确定防护要点作分类保护；根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应作多层保护。

❑ 防电磁泄露

与其他电子设备一样，计算机在工作时也要产生电磁发射。电磁发射包括辐射发射和传导发射两种类型。而这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原，从而会造成计算机中信息的泄露。

目前，屏蔽是防电磁泄露的有效措施，屏蔽方式主要包括电屏蔽、磁屏蔽和电磁屏蔽 3 种类型。

2. 逻辑安全

计算机的逻辑安全需要用口令、文件许可等方法来实现。例如，可以限制用户登录的次数或对试探操作加上时间限制；可以用软件来保护存储在计算机文件中的信息。

限制存取的另一种方式是通过硬件完成的，在接收到存取要求后，先询问并校核口令，然后访问位于目录中的授权用户标志号。

另外，有一些安全软件包也可以跟踪可疑的、未授权的存取企图，例如，多次登录或请