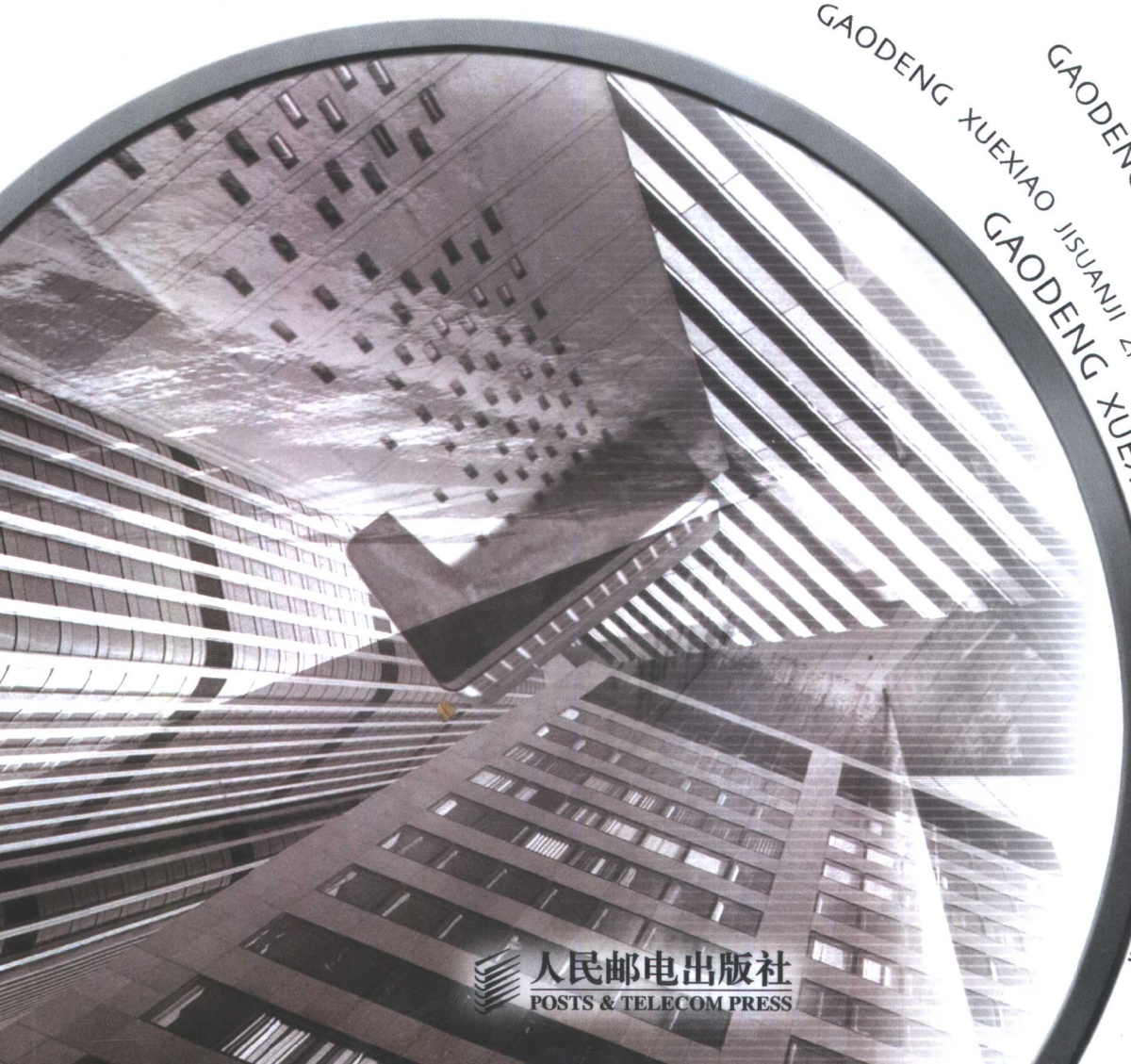
高等学校计算机专业教材

GAODENG XUEXIAO JISUANJI ZHUANYE JIAOCAI

计算机网络安全

◉ 邓亚平 编著



GAODENG XUEXIAO JISUANJI ZHUANYE JIAOCAI
GAODENG XUEXIAO JISUANJI ZHUANYE JIAOCAI
GAODENG XUEXIAO JISUANJI ZHUANYE JIAOCAI

人民邮电出版社
POSTS & TELECOM PRESS

高等学校计算机专业教材

计算机网络安全

邓亚平 编著

人民邮电出版社

图书在版编目（CIP）数据

计算机网络安全/邓亚平编著. —北京：人民邮电出版社，2004.9
高等学校计算机专业教材
ISBN 7-115-12498-1

Ⅰ. 计… Ⅱ. 邓… 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（2004）第 088776 号

内 容 提 要

本书详细地介绍计算机网络安全的基础理论、原理及其实现方法。主要内容包括网络安全概论、数据加密、计算机病毒的防治、操作系统的安全、数据库系统的安全、黑客入侵技术、网站的安全、网络协议的安全、防火墙技术、入侵检测技术、安全评估和安全法规等。

本书可作为高等院校本科计算机专业、通信工程专业和信息安全专业等相关专业的教材，也可作为计算机网络安全或信息安全课程的研究生教材，还可作为网络工程技术人员、网络管理员和信息安全管理人员的技术参考书。

高等学校计算机专业教材

计算机网络安全

◆ 编　　著　邓亚平
责任编辑　邹文波
执行编辑　王亚娜

◆ 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
读者热线：010-67129259
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：24.25
字数：588 千字　　2004 年 9 月第 1 版
印数：1－5 000 册　　2004 年 9 月北京第 1 次印刷

ISBN 7-115-12498-1/TP·4118

定价：31.00 元

前　言

计算机网络技术的飞速发展以及计算机网络应用的日益普及，给人们的生产方式、生活方式和思维方式带来了巨大的变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入了信息化时代。通过计算机网络，人们可以非常方便地存储、交换以及搜索信息，人们在工作、生活以及娱乐中都享受到了极大的便利。然而，人们在享受计算机网络所带来的巨大利益的同时，也受到计算机网络所暴露出的各种安全问题的困扰。这些安全问题不仅影响到信息社会的个人生活，而且也影响到金融业、证券业、电子政务、电子商务等政治和经济活动。

计算机网络安全问题已成为一个世界性的现实问题。可以说没有网络安全，就没有完全意义上的国家安全，也没有真正的政治安全、军事安全和经济安全。因此，加速计算机网络安全的研究和发展，加强计算机网络的安全保障能力，提高全民的网络安全意识已成为我国网络化和信息化发展的当务之急。

作者根据多年从事计算机网络安全科研和教学工作的实践编写了此书。在编写过程中，力求使本书具有以下特点。

（1）在内容安排上，尽量适合学生学习的特点，循序渐进，深入浅出，注重计算机网络安全的应用方法和技能的传授。

（2）注重教材的先进性。力求反映当前计算机网络安全技术发展的最新成果。

（3）兼顾教材的系统性与科学性，既要考虑知识和技能的科学体系，又要遵循教育规律，注意内容的取舍和与相关课程的衔接，尽量避免内容重复。

（4）力求文字精炼，语言流畅，并注重向学生传授灵活的学习方法。

（5）习题具有思考性和启发性，注重培养学生的创新能力。

通过对本教材的学习，读者可以系统地掌握计算机网络安全的基础知识和技能。

在本书的编写过程中，马传龙、张伟、殷科、刘强、徐震和董世容参加了部分录入及插图工作，在此一并表示感谢。

由于作者水平有限，编写时间仓促，本书难免有错误或不当之处，殷切希望广大读者批评指正。

编　者

目　录

第 1 章　网络安全概论

本章主要介绍计算机网络所面临的各种安全威胁，分析产生这些威胁的根源，并推荐从体系结构上加强网络系统安全的 PDRR 网络安全模型，最后讲述实施网络安全策略的一些基本原则。

通过本章的学习，读者应该掌握以下内容：

（1）了解计算机网络所面临的安全威胁；

（2）理解 PDRR 网络安全模型；

（3）掌握网络安全策略的基本原则。

1.1　网络安全面临的威胁

随着计算机网络技术的发展和社会信息化进程的加快，现在人们的生活、工作、学习、娱乐和交往都已离不开计算机网络。尽管计算机网络为人们提供了巨大的方便，但是受技术和社会因素的各种影响，计算机网络一直存在着多种安全缺陷。攻击者经常利用这些缺陷，实施攻击和入侵，给计算机网络造成了极大的损害。

本节分别讲述物理安全威胁、操作系统的安全缺陷、网络协议的安全缺陷、应用软件的实现缺陷、用户使用的缺陷和恶意程序等 6 个方面的安全威胁。

1.1.1　物理安全威胁

1. 物理安全问题的重要性

信息安全首先要保障信息的物理安全。物理安全是指在物理介质层次上对存储和传输的信息的安全保护。物理安全是信息安全的最基本保障，是不可缺少和忽视的组成部分。

对于运行在任何操作系统下的计算机系统，物理安全都是一个必须要考虑的重要问题。但这个问题中的大部分内容与网络安全无关，例如，服务器被盗窃了，其里面的硬盘就可能被窃贼使用物理读取的方式进行分析读取。这是一个极端的例子，更一般的情况可能是非法使用者接触了系统的控制台，重新启动计算机系统并获得控制权，或者通过物理连接的方式窃听网络信息。

在物理安全方面，与网络相关的问题主要在于传输数据的安全性。由于 TCP/IP 是一种分组交换协议，各个分组在网络上都是透明传输的，并经过不同的网络，由那些网络上的路由器转发，最后才能到达目的计算机。由于分组都是直接经过这些网络，所以这些网络上的计算机都有可能将其捕获，从而窃听到正在传输的数据。物理上的传输安全问题对网络安全

非常重要。

由于物理网络的传输限制，并不是在网络上的任何位置都能捕获分组信息。对于最常用的以太网，较老的共享式以太网能在任何一个位置窃听所有流经网络的分组信息，而新式的交换式以太网能够在交换机上隔离流向不同计算机的数据，因此安全性更高。然而，无论何种类型的网络，路由器总是一个非常关键的设备，所有流入和流出网络的数据都经过它，如果攻击者在路由器上进行窃听就会造成非常严重的安全问题。

2. 主要的物理安全威胁

物理安全威胁，即直接威胁网络设备。目前主要的物理安全威胁包括以下 3 大类。

- 自然灾害（例如，地震、水灾和火灾等）、物理损坏（例如，硬盘损坏、设备使用寿命到期和外力破损等）和设备故障（例如，停电或电源故障造成设备断电和电磁干扰等）。特点是突发性、自然因素性、非针对性。这种安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。
- 电磁辐射（例如，监听微机操作过程）、乘虚而入（例如，进入安全进程后半途离开）和痕迹泄漏（例如，口令、密钥等保管不善，易于被人发现）。特点是难以察觉性、人为实施的故意性和信息的无意泄漏性。这种安全威胁只破坏信息的秘密性，无损信息的完整性和可用性。
- 操作失误（例如，删除文件、格式化硬盘和线路拆除等）和意外疏忽（例如，系统掉电、操作系统死机等系统崩溃）。特点是人为实施的无意性和非针对性。这种安全威胁只破坏信息的完整性和可用性，无损信息的秘密性。

（1）外部终端的物理安全

如果所有的系统都锁在屋里，并且所有连接系统的网络和接到系统上的终端都在上锁的同一间屋内，则通信与系统一样安全（假如没有调制解调器）。但是系统的通信线在上锁的室外时，就会有安全问题。尽管从网络通信线路上提取信息所需要的技术，比从终端通信线获取数据的技术高几个数量级，同样的问题也会发生在网络连接上。

用一种简单的（但很昂贵）高技术加压电缆，可以获得通信的物理安全。这种技术是若干年前，为美国国家电话系统而研发的。通信电缆密封在塑料中；埋藏于地下，并在线的两端加压，线上连接了带有报警器的监视器，用来测量压力。如果压力下降，则意味着电缆可能破损，维修人员将被派出寻找并修复出问题的电缆。

电缆加压技术同时也提供了安全的通信线路。通信线路不是将电缆埋藏于地下，而是架设于整座楼中，每寸电缆都将暴露在外。如果有人企图割电缆，监视器会启动报警器，通知安全保卫人员电缆已被破坏。如果有人成功地在电缆上接上了自己的通信线，安全人员定期检查电缆的总长度，就可以发现电缆拼接处。加压电缆是屏蔽在波纹铝钢包皮中的，因此几乎没有电磁辐射，如果要用电磁感应窃听，势必需用大量可见的设备。这样终端就不必锁在办公室，而只需要将安全电缆的端头锁在办公室的一个盒子里。

另一个增加外部终端物理安全的方法是，在每天下班后就断开终端的连接。这样若有人想非法进入系统，将不得不试图在白天人们上班时间里获取终端的访问权，或不得不在下班后试图潜入计算机房。

（2）通信线路的物理安全

光纤通信线曾被认为是不可搭线窃听的，其断破处可被立即检测到，拼接处的传输会非常缓慢。光纤没有电磁辐射，所以也不能用电磁感应窃听。不幸的是光纤的最大长度有限，大于这一长度的光纤通信系统必须放大信号，这就需要将光信号转换成电脉冲，然后再恢复成光脉冲，继续通过线路传送。完成这一操作的设备（放大器）是光纤通信系统的安全薄弱环节，因为信号可能在这一环节被搭线窃听。

对于任何可在不上锁的地方存取的系统，是通信特别严重的安全薄弱环节。当允许用户通过挂到本地电信公司的拨号调制解调器存取系统时，系统的安全程度就将大大地削弱，有电话和调制解调器的人就有可能非法进入该系统。

总之，好的安全系统就是控制对系统和它所连接网络的物理接近。

1.1.2　操作系统的安全缺陷

操作系统是用户和硬件设备的中间层，是任何计算机在使用前都必须安装的。任何操作系统都自带一系列的系统应用程序，为用户使用计算机提供有效和方便的操作。实际上，这些应用程序也是一种软件。不同于用户应用程序的是，操作系统的应用程序在用户安装操作系统的时候都是缺省安装的。如果这些应用程序有安全缺陷，那么就会使系统处于不安全的状态。因此，了解操作系统经常出现的安全缺陷是很有必要的。

目前，人们使用的操作系统分为两大类：UNIX/Linux 系列和 Windows 系列。下面分别举例说明这两大类操作系统中存在的安全缺陷。

1. 公共缺陷检索（Common Vulnerabilities and Exposures，CVE）

大多数信息安全工具都包含一个信息安全缺陷的数据库，例如，CERT 安全公告和 Bugtraq ID 等。但是，这些数据库对信息安全缺陷的描述格式各不相同。有时，很难确定在不同数据库中所描述的缺陷是否是同一个缺陷。每一个数据库都使用自己的编号以及描述格式，这样会给使用者带来很多不便。

CVE 是信息安全确认的一个列表或者词典。它对不同信息安全缺陷的数据库之间提供一种公共的索引，是信息共享的关键。有了 CVE 检索之后，一个缺陷就有了一个公共的名字，从而可以通过 CVE 的条款检索到包含该缺陷的所有数据库。

CVE 有如下几个特点：

① 每一种缺陷都有惟一的命名；

② 每一种缺陷都有惟一的标准描述；

③ CVE 不是一个数据库而是一种检索词典；

④ CVE 为多个不同的数据库提供一种交流的共同语言；

⑤ CVE 是评价信息安全数据库的一个基础；

⑥ CVE 可以通过因特网阅读和下载；

⑦ CVE 的会员可以给 CVE 提供自己数据库的索引信息及其修改信息。

2. UNIX 操作系统的安全缺陷

（1）远程过程调用（Remote Procedure Calls，RPC）

远程过程调用允许一台机器上的程序执行另一台机器上的程序。它们被广泛地用于提供

网络服务，如 NFS 文件共享和 NIS。很多 UNIX 操作系统的 RPC 软件包中包含具有缓冲区溢出缺陷的程序。以下的程序具有缓冲区溢出的缺陷。

① rpc.yppasswdd：服务端守护进程，用来控制来自 yppasswd 的修改密码请求以及修改 NIS 密码文件。rpc.yppasswdd 以超级用户的权限运行。

② rpc.espd：IRIX 操作系统的一个嵌入支持部分（Embedded Support Partner，ESP）。rpc.espd 以超级用户的权限运行。

③ rpc.cmsd：日历管理服务守护进程（Calendar Manager Service，CMS）。rpc.cmsd 以超级用户的权限运行。

④ rpc.ttdbserver：ToolTalk 数据库服务器（ToolTalk Database Server）。

⑤ rpc.bind：把 RPC 程序号转换为通用地址的服务器。

如果系统运行上述程序之一，那么系统就很可能受到 RPC 服务缓冲区溢出的攻击。值得注意的是，UNIX 的绝大部分版本都具有这个缺陷。解决这个问题的最好方案是全部删除这些服务。在必须运行该服务的地方，安装最新的补丁。定期检查供应商的补丁库查找最新的补丁并立刻安装。在路由器或防火墙中对 RPC 端口 111，以及 RPC loopback 端口 32770～32789（TCP/UDP）加以适当的控制。

RPC 服务缓冲区溢出缺陷的 CVE 条款如下：

CVE-1999-0003、CVE-1999-0693、CVE-1999-0018、CVE-1999-0696、CVE-1999-0019、CVE-1999-0704、CVE-2001-0236 和 CVE-2000-0666。

（2）Sendmail

Sendmail 是在 UNIX 和 Linux 操作系统中用得最多的发送、接收和转发电子邮件的程序。Sendmail 在因特网上的广泛应用使它成为攻击者的主要目标，过去的几年里曾发现了若干个缺陷。事实上，第一个建议是 CERT/CC 在 1988 年提出的，指出了 Sendmail 中一个易受攻击的缺陷。其中最为常用的是攻击者可以发送一封特别的邮件消息给运行 Sendmail 的机器，Sendmail 会根据这条消息要求受劫持的机器把它的口令文件发送给攻击者的机器，这样口令就会被破解。UNIX 和 Linux 的大部分版本都会受到该漏洞的影响。Sendmail 有很多易受攻击的弱点，必须定期地更新和打补丁。检查 Sendmail 最新版本和补丁版本，如果没有更新版本或安装补丁文件，就可能受攻击。

Sendmail 缺陷的 CVE 条款如下：

CVE-1999-0047、CVE-1999-0130、CVE-1999-0131、CVE-1999-0203、CVE-1999-0204 和 CVE-1999-0206。

3. Windows 系列操作系统的安全缺陷

（1）Unicode

Unicode 是 ISO 发布的统一全球文字符号的国际标准编码。它是一种双字节的编码。不论何种平台、何种程序、何种语言，Unicode 为每一个字符提供了惟一的序号。Unicode 标准被包括 Microsoft 在内的很多软件开发商所采用。通过向 IIS（Internet Information Server）服务器发出一个包括非法 Unicode UTF-8 序列的 URL，攻击者可以迫使服务器逐字“进入或退出”目录并执行任意脚本，这种攻击称为目录转换（Directory Traversal）攻击。

Unicode 用“% 2f”和“% 5c”分别表示“/”和“\”，但也可以用所谓的“超长”序列

来代表这些字符。“超长”序列是非法的 Unicode 表示符，它们比实际代表这些字符的序列要长。“/”和“\”均可以用一个字节来表示。例如，“%c0%af”代表“/”用了两个字节，就是一个“超长”序列。IIS 服务器不对超长序列进行检查。这样在 URL 中加入一个超长的 Unicode 序列，就可以绕过 Microsoft 的安全检查。如果发出的请求来自一个可执行的目录，攻击者可以在服务器上运行可执行文件。安装了 IIS 5.0，而没有安装 Service Pack 2 的 Windows 2000 Server 都存在着这个漏洞。

最好的判断是否存在这个缺陷的方法是运行 Hfnetchk。Hfnetchk 是用来帮助网络管理员判断系统所打补丁情况的工具。为进一步确认，可以键入以下命令：

http://victim_iis_server/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

这个 URL 地址需要根据实际系统适当修改。如果已移走了 scripts 目录（建议这么做），这个命令就失效了。这时可以暂时建立一个有执行权限的目录，或使用一个已有的有执行权限的目录，来代替 scripts 目录。例如，如果已经删除了 scripts 目录，但另外有一个 cgi-bin 目录，可以使用 cgi-bin 目录代替 scripts 目录来测试系统。如果系统是易受攻击的，这个 URL 会送回一个目录，列出驱动器 C 下的所有内容。这时用户只是运行 DIR 命令，如果是一个攻击者的话，就有可能大肆破坏或在用户的系统上安装一个后门。

解决上述问题的方案是如果不需要使用 Web 服务器，就把 IIS 服务器关闭。一般来说，Windows 2000 Server 的缺省安装都是把 IIS 服务器打开的。如果实在需要 IIS 服务器，应下载 Microsoft 的最新补丁。另外，IIS Lockdown 和 URL Scan 都可以避免这类攻击。IIS Lockdown 可以帮助系统管理员锁住 IIS 服务器，URL Scan 是一个可以过滤很多 HTTP 请求的过滤器，它可以过滤包含 UTF-8 编码字符的请求。

Unicode 缺陷的 CVE 条款如下：

CVE-2000-0884。

（2）ISAPI 缓冲区溢出

Microsoft IIS（Internet Information Server）是在大多数 Microsoft Windows NT 和 Windows 2000 服务器上使用的服务器软件。在安装 IIS 的时候，多个 ISAPI（Internet Services Application Programming Interface）被自动安装。ISAPI 允许开发人员使用多种动态链接库 DLLs 来扩展 IIS 服务器的性能。一些动态链接库，例如 idq.dll，有编程错误，使得它们进行不正确的边界检查。特别是，它们不阻塞超长字符串。攻击者可以利用这一点向 DLL 发送数据，造成缓冲区溢出，进而控制 IIS 服务器。

安装了 Microsoft Index Server 2.0 的系统和 Windows 2000 中的 Indexing Service 都具有 idq.dll 缓冲区溢出缺陷。Windows 2000 Server、Advanced Server 和安装了 IIS 5.0 的 Server Data Center Edition 都有.printer 缓冲区溢出缺陷。Windows 2000 Professional 也具有 DLL 的缺陷，但不是缺省安装。如果可能，应使用 Group Policy，禁止基于网络的打印。Windows XP 没有这个缺陷。

如果安装了 IIS 服务器，并没有打过补丁（SP2），那么该系统很可能会受到这种攻击。可以用 Hfnetchk 工具检查系统打补丁的情况。

解决上述问题的方案是如果发现系统具有这种缺陷，则安装最新的 Microsoft 补丁。同时，应检查并取消所有不需要的 ISAPI 扩展。经常检查这些扩展是否被恢复。还要记住最小权限规则，系统应运行系统正常工作所需的最少服务。另外，IIS Lockdown 和 URL Scan 均可以

避免这类攻击。IIS Lockdown 可以帮助管理员锁住 IIS Server，URL Scan 是一个可以过滤很多 HTTP 请求的过滤器，它可以过滤包含 UTF8 编码字符的请求。

ISAPI 缓冲区溢出缺陷的 CVE 条款如下：

CVE-1999-0412、CVE-2001-0241、CVE-2000-1147 和 CVE-2001-0500。

1.1.3 网络协议的安全缺陷

TCP/IP 是目前 Internet 使用的协议。它之所以有今天如此广泛的使用，是因为它在设计原则上体现出很多优点，例如，简单性、可扩展性强和尽力而为等原则。这些原则给使用 TCP/IP 的用户带来非常方便的互连环境，使得 Internet 的用户迅速地增加。但是，TCP/IP 也存在着一系列的安全缺陷。有的缺陷是由于源地址的认证问题造成的，有的缺陷则来自网络控制机制和路由协议等。这些缺陷，是所有使用 TCP/IP 的系统所共有的，以下将讨论这些安全隐患。

1. TCP/IP 概述

（1）TCP/IP 基本结构

TCP/IP 是一组 Internet 协议，不但包括 TCP 和 IP 两个关键协议，还包括其他协议，如 UDP、ARP、ICMP、Telnet 和 FTP 等。TCP/IP 的设计目标是使不同的网络互相连接，即实现互联网。为了达到这个目标，TCP/IP 被设计成四层结构，从上到下分别为：应用层、传输层、网络层和物理链路层，如图 1.1 所示。

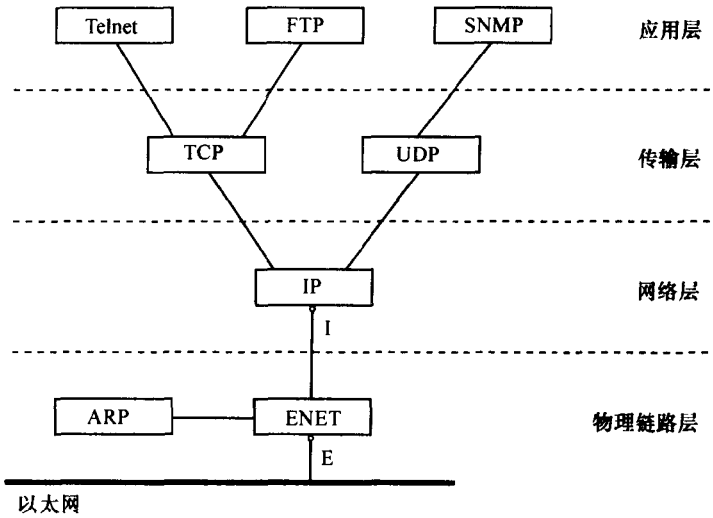


图 1.1 TCP/IP 基本逻辑结构

图 1.1 所示的是 TCP/IP 各层的逻辑结构。任何一台计算机想在 Internet 上与其他计算机互连，必须有这样的逻辑结构。每一层可以有一个或多个模块，每个模块实现一定的数据处理功能。应用程序（如 Telnet 和 FTP）运行在应用层。传输层给应用层提供端对端的数据传输，传输层有两种协议：TCP 和 UDP。网络层实现包转发功能，是网络之间互连的关键技术，网络层的协议为 IP。物理链路层包括网络物理线路、网络驱动和一些协议，如 ARP。目