河南省高职高专计算机规划教材

计算机安全技术

主　编　杜庆灵
副主编　刘会霞　陈树平　李　健
编　者　（以姓氏笔画为序）
王文莉　王　硕　刘会霞
齐兰英　张天伍　李　飞
李　健　杜庆灵　杨成卫
陈树平　武书彦

西北大学出版社

图书在版编目(CIP)数据

计算机安全技术／杜庆灵主编.—西安:西北大学出版社,2006.2
高职高专计算机规划教材
ISBN 7-5604-2085-0

Ⅰ.计… Ⅱ.杜… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2005)第 139374 号

计算机安全技术

主　　编　杜庆灵
出版发行　西北大学出版社
通讯地址　西安市太白北路 229 号　　邮编　710069
经　　销　新华书店经销
印　　刷　河南新华印务有限公司
开　　本　787mm × 1092mm　1/16
印　　张　17.125
字　　数　388 千字
版　　次　2006 年 2 月第 1 版　2006 年 2 月第 1 次印刷
书　　号　ISBN 7-5604-2085-0/TP · 35
定　　价　26.00 元

出版说明

当前，我国正在走新型工业化道路，坚持以信息化带动工业化，以工业化促进信息化，加快发展现代服务业，全面建设小康社会。走新型工业化道路，既需要一大批拔尖创新人才，也需要数以千万计的专门人才和数以亿计的高素质劳动者。根据劳动力市场技能型人才短缺的状况，国家决定实施技能型紧缺人才培养培训工程，其中计算机人才的培养培训是其重要的组成部分。

为适应高职高专计算机教育发展的需要，促进教育教学改革和教材建设，满足经济和社会发展对计算机人才的需求，根据教育部等六部门印发的《关于实施职业院校制造业和现代服务业技能型紧缺人才培养培训工程的通知》精神，按照教育部《关于制定＜2004～2007年职业教育教材开发编写计划＞的通知》要求，在教育部有关部门的支持和指导下，经河南省教育厅批准，我们组织有关专家，对计算机高职高专教育的培养目标和模式、课程体系、教学内容、教学方法和手段、教学实践等方面，进行了广泛而深入的调研。

在充分调研的基础上，在教育部有关部门和河南省教育厅的大力支持下，我们组织有关专家召开了计算机高职高专教育教学研讨会、教学大纲审定会和主编人会议，确定了教材编写的指导思想、原则和要求，组织全省近40所院校的一线教师，吸取了最新的计算机高职高专教育教学经验和成果，编写了这套教材。本套教材充分体现了以就业为导向，以职业技能培养为根本的编写指导思想，突出了思想性、科学性、先进性、可读性和适用性的编写原则，较好地处理了“三基”（基本理论、基本知识、基本技能）关系，学历教育与职业认证、职业准入的关系。

这套教材虽经广泛调研与精心编撰，但一定还会存在这样或那样的不足，我们诚挚欢迎广大读者，尤其是选用该教材的教师和学生地其中的不足之处给予批评指正，以便我们在重印和修订时采纳有益的建议和意见，使之不断完善。

河南省高等学校计算机教育研究会

2006年1月

河南省高职高专计算机规划教材
参加编写学校
（以汉语拼音排序）

安阳师范学院
华北水利水电学院水利职业学院
黄河水利职业技术学院
河南财政税务高等专科学校
河南纺织高等专科学校
河南公安高等专科学校
河南工业大学
河南工业大学化学职业学院
河南经贸职业学院
河南农业职业学院
河南司法警官职业学院
河南商业高等专科学校
河南质量工程职业学院
济源职业技术学院
焦作大学
开封教育学院
开封人民警察学校
漯河职业技术学院
洛阳师范学院
平顶山工业职业技术学院
商丘师范学院
铁道警官高等专科学校
许昌职业技术学院
信阳农业高等专科学校
中原工学院广播影视职业学院
中州大学
郑州航空工业管理学院信息统计职业学院
郑州经济管理干部学院
郑州交通职业学院
郑州牧业工程高等专科学校
郑州轻工业学院
郑州轻工业学院轻工职业学院
郑州师范高等专科学校
郑州铁路职业技术学院

前　言

随着计算机技术的发展，计算机通信和数据处理已进入人们的日常生活。计算机网络由局域向广域发展，国家网络及全球网络遍及各个角落，时时刻刻都有各种形式的数据传输。它们可能是普通信函、商务信息，也可能是公司重要机密文件或国家机密。无论是从个人隐私、商务利益，还是国家安全角度考虑，都需要保证这些计算机信息的安全。网络与信息安全已成为一个重要的新兴交叉学科专业，许多大学开设了本科信息安全及相关专业，也编写出了很好的适应本科教学的教材，但对于高职高专的信息安全及相关专业，还没有比较适合的教材，为此我们组织有关专家及教学一线骨干的教师编写了本书。

本书由杜庆灵任主编，刘会霞、陈树平、李健任副主编。具体撰写分工如下：杜庆灵（河南公安高等专科学校）撰写第1章；李飞（济源职业技术学院）撰写第2章；王硕（河南商业高等专科学校）撰写第3章；武书彦（郑州牧业工程高等专科学校）撰写第4章；齐兰英（郑州轻工业学院轻工职业学院）撰写第5章；李健（河南司法警官职业学院）撰写第6章；刘会霞（河南公安高等专科学校）撰写第7章；陈树平（商丘师范学院）撰写第8章；杨成卫（郑州铁道警官高等专科学校）撰写第9章；张天伍、王文莉（郑州经济干部管理学院、郑州铁路职业技术学院铁道分院）撰写第10章。

由于我们水平有限，时间仓促，谬误之处在所难免，竭诚欢迎读者批评、指正，我们将不断修订、完善。

编　者

2005年7月

目　录

第 1 章　计算机安全技术概述

本章主要介绍计算机网络的基本知识，计算机网络安全的基本概念和主要技术等内容，是后面各章节的基础。

1.1　计算机网络概述

计算机应用的发展主要经历了三个阶段：主机计算机（mainframe computing）、分布式客户机/服务器计算（distributed client/server computing）、网络计算（network computıng ），其中网络计算模式是目前最有发展前景的模式。

1.1.1　网络协议

计算机网络是现代数字通信技术和计算机技术相结合的产物，是现代科学技术的一项重要成果。它是将处于不同地理位置、具有独立功能的多台计算机、终端以及外部设备，通过一定的方式连接起来并配备相应的网络系统软件，最终实现硬件、软件资源的共享和信息的处理与传递。一般情况下，在同类型的计算机、终端之间实现通信比较容易，而对不同类型计算机、终端的通信就相当困难。要解决这个问题，就需要网络协议及相应的网络体系结构。

在网络中，为使各计算机之间能正确地传递信息，必须在信息内容、信息格式、信息传输顺序等方面有一组事先约定好的规则，这组约定或规则就称为网络协议。网络协议由 3 个要素组成：

1. 语义

协议的语义由通信过程的说明构成，它规定了需要发出何种控制信息完成何种动作以及做出何种应答，对发布请求、执行动作以及返回应答予以解释，并确定用于协调和差错处理的控制信息。

2. 语法

语法是用于规定将若干个协议元素和数据组合在一起来表达一个更完整的内容时所应遵循的格式，即对通信时采用的数据结构形式的一种规定。

3. 时序

时序是对事件实现顺序的详细说明，指出事件的顺序以及速度匹配、排序。

由此可见，网络协议实质上是实体间通信时所使用的一种语言，是计算机网络不可缺少的组成部分。

目前，对于复杂的计算机网络协议，通常采用高度结构化的方式设计。结构化设计便于将一个复杂的系统设计问题分割成若干容易处理的子问题，各子问题相对独立，相互联系，用分层或协议分层来组织。在设计和选择协议时，不仅要考虑网络系统的拓扑结构、信息的传输量、所采用的传输技术、数据存取方式，还要考虑其效率、价格和适应性等问题。

1.1.2 网络的层次结构

网络设计中采用的结构化设计法，就是将网络按照功能分成一系列的层次，每一层完成一个特定的服务来实现本层的功能，同时又向它的上一层提供服务，服务的提供和使用都是通过相邻间的接口来进行的。这就是人们通常所说的网络的层次结构，如图 1.1 所示。

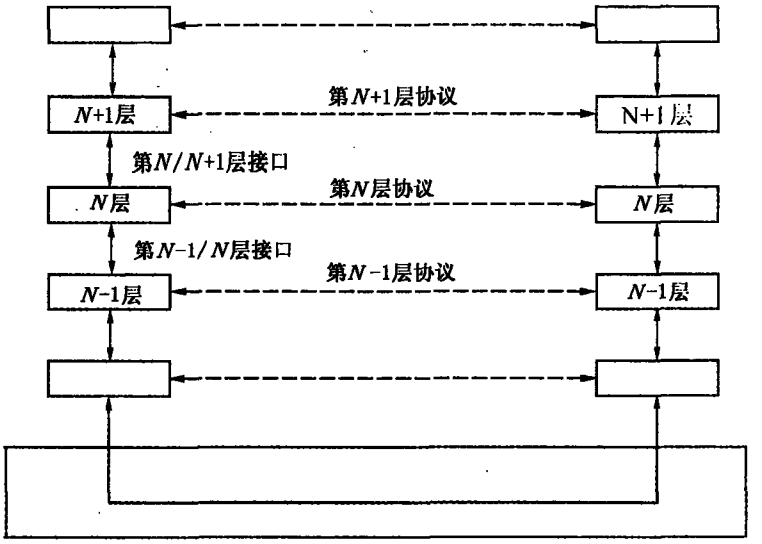

图 1.1 网络的层次结构模型

图 1.1 描述了一个通用的网络层次模型，其中有以下常用的术语：

1. 实体与对等实体

每一层中的活动元素称为实体，实体可以是软件实体（如进程），也可以是硬件实体（如智能 I/O 芯片）。位于不同系统上同一层中的实体称为对等实体，不同系统间进行通信实际上是各对等实体间在通信。

2. 通信与虚通信

事实上，除了在最底层的物理媒体上进行的是实通信（图中用实线表示实通信，用虚线表示虚通信）之外，其余各对等实体间进行的都是虚通信，即并没有数据流从一个系统的第 N 层直接流到另一个系统的第 N 层。每个实体只能和同一系统中上下相邻的实体进行直接的通信，不同系统必须通过其下各层的通信间接完成。

3. (N)服务与(N)服务数据单元

第 N 层实体向第($N+1$)层实体提供的在第 N 层上的通信能力称为第 N 层服务。由此可见，第($N+1$)层实体通过请求第 N 层的服务完成第($N+1$)层上的通信，而第 N 层实体通

过请求第(N－1)的服务完成第 N 层上的通信，以此类推直到最底层，最底层上的对等实体通过连接它们的物理媒体直接通信。

服务是在服务接入点(Service Access Point—SAP)提供给上层使用的。(N)SAP 就是(N+1)层可以访问 N 层服务的地方。每个 SAP 都有一个惟一标识它的地址。

接受(N)服务的(N+1)实体叫做(N)服务用户。在 OSI 模型中(后边将介绍)，把(N)层要跨过网络传递给对等实体，然后向上交给(N+1)层的信息称为第 N 层服务数据单元(Service Data Unit—SDU)。

4. (N)协议与(N)协议数据单元，两个第 N 层实体进行通信的规则的集成为第 N 层的协议(图 1.1 中的水平虚线)

在(N)协议控制下两个对等(N)实体间的通信，使(N)层能够向上一层(即 N+1 层)提供服务。在第 N 层协议中所传送的每一信息被称作第 N 层协议数据单元(Protocol Data Unit－PDU)。

5. 接口与服务原语

相邻实体间的通信是通过它们的边界进行的，该边界称为相邻间的接口。在模型的接口上，(N+1)层实体通过 SAP 把一个接口数据单元(Interface Data Unit，IDU)传递给 N 层实体。IDU 由服务数据单元 SDU 和一些接口控制信息(Interface Control Information，ICI)。控制信息用于帮助下一层完成任务(如 SDU 中的字节数)，它本身不是数据的一部分。

图 1.2 说明处于接口两边的两层之间的关系。

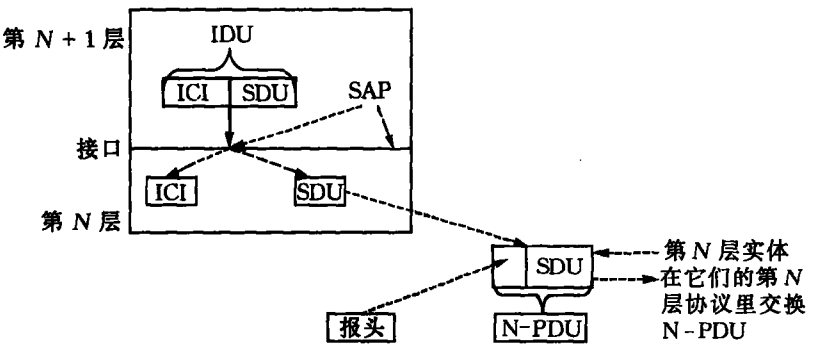

图 1.2　处于接口两边的两层之间的关系

在接口处规定了下层向上层提供服务，以及上下层实体请求(提供)服务所使用的形式规范语句，这些形式规范语句称为服务原语。因此可以说，相邻实体通过发送或接收服务语言进行交互作用。

通常人们将网络的层次结构、协议栈和相邻层的接口以及服务统称为网络体系结构。

1.2　网络参考模型

目前最主要和流行的网络参考模型是 ISO/OSI 参考模型和 TCP/IP 参考模型。本小节主要介绍这两个参考模型，并简要分析当前高速信息网络的体系结构。

1.2.1 ISO/OSI 参考模型

开放系统互联参考模型(Open System Interconnection Reference Model,OSI/RM)是国际标准化组织(International Standardization Organization,ISO)为解决异种互联而制定的开放式计算机网络层次结构模型。它的最大特点是将服务、接口、协议这三个概念明确地区别开来。服务说明某一层提供什么服务,接口说明上层如何使用下层的服务,而协议涉及如何实现该层的服务。各层采用什么样的协议是没有限制的,只要向上提供相同的服务并且不改变相邻的接口即可。这种思想同现代的面向对象的编程思想是完全一致的,一层就是一个对象,服务实现的细节完全封装在层内。因此,各层之间具有很强的独立性。

OSI 参考模型只是规定了网络的层次划分,以及每一层上所实现的功能。尽管 ISO 已为每一层都制定了标准,但它没有规定每一层所实现的服务和协议。因此,它本身并不是一个网络体系结构。

1. OSI 参考模型的分层结构

OSI 参考模型是设计和描述网络通信的基本框架,采用的层次结构由 7 层组成,从高层到低层依次是应用层、表示层、会话层、传输层、网络层、数据链路层和物理层,如图 1.3 所示。

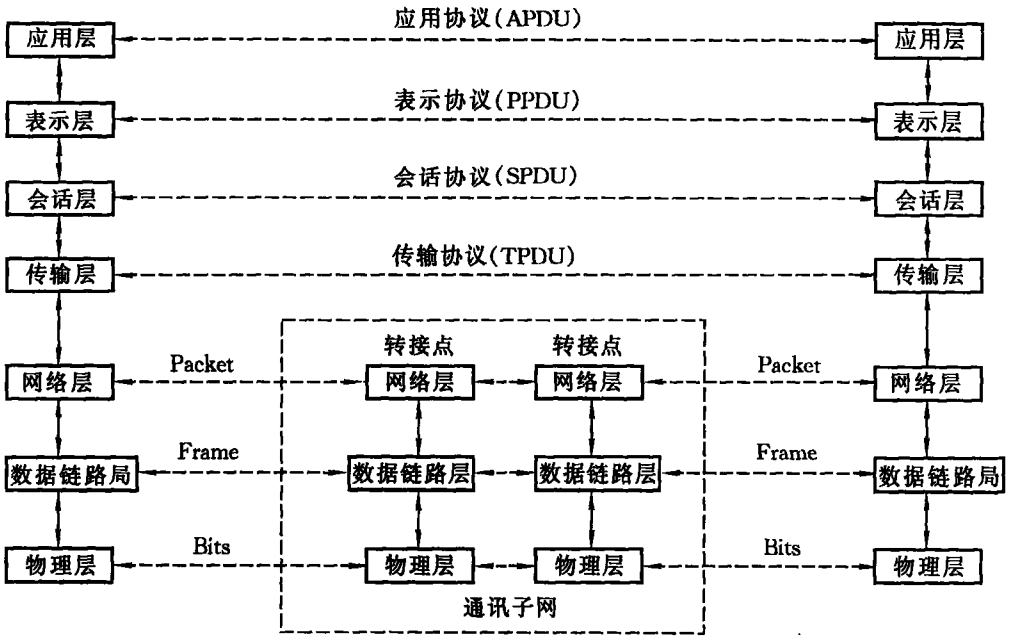

图 1.3 7 层 OSI 参考模型

2. 各层的主要功能(见图 1.4)

(1)物理层

物理层是开放系统互联参考模型的最底层,它的功能是实现系统与物理媒体的接口,并规定其机械、电气功能和规程方面的特性。它主要对其上层——数据链路层提供以下服务:数据电路标误用、物理连接及其端点、物理服务数据单元等。

7	应用层	处理网络应用
6	表示层	数据表示
5	会话层	互联主机通信
4	传输层	端到端连接
3	网络层	寻址和最短路径
2	数据链路层	介质访问
1	物理层	二进制传输

图 1.4 各层的主要功能

(2)数据链路层

数据链路层是在网络实体之间建立、保持和释放数据链路,为服务数据单元提供功能和规程方面的手段。它主要是使网络层能够透明地、可靠地进行数据的传输。它能纠正物理层内可能发生的错误。其主要功能是:信息的传输、差错控制、流量控制和异步处理。

(3)网络层

网络层在开放系统互联之间提供建立、保持和终止网络连接的手段,并为传送实体间通过网络连接交换网络服务数据单元提供功能和规程。网络层的主要功能是:路由选择和转接、服务选择与子网选择、流量控制、差错检测与恢复等。它提供给传输层的服务主要是:网络地址、网络服务数据单元和加速网络服务数据单元、服务质量参数。

(4)传输层

传输层是建立在网络层和会话层之间的一个层次,实质上它是网络体系结构中高低层之间衔接的一个接口层。传输层不仅是一个单独的结构层,还是整个分层体系协议的核心,没有传输层,整个分层协议就没有意义。

传输层获得下层提供的服务包括:发送和接收顺序正确的数据包分组序列,并用其构成传输层数据,获得网络层地址,包括虚拟信道号和逻辑信道号。传输层向上层提供的服务包括:无差错的有序的报文收发;提供传输连接;进行流量控制。

传输层的功能是从会话层接收数据,如果把数据切成较小的数据片,并把数据传送给网络层,确保数据片正确到达网络,从而实现两层间数据的透明传送。传输层只能存在于端系统(即主机)中,而在通信子网中是没有传输层的,传输层以上各层不再管信息传输的问题了。

(5)会话层

会话层用于建立、管理以及终止两个应用系统之间的会话。它是用户连接到网络的接口,负责两个主机间的原始报文的传输。会话层为表示层提供服务,同时接受传输层的服务。为了实现在表示层实体之间传输数据,会话连接必须被映射到传输连接上。

会话层的功能包括会话连接到传输的映射、会话连接的流量控制、会话连接恢复与释放、会话连接管理、差错控制。

会话层是面向处理的核心。

会话层为表示层提供的服务主要是:会话连接的建立和释放、常规和加速数据交换、交互管理、会话连接同步及异常报告等。

(6)表示层

表示层在应用过程中之间传送的信息，提供表示方法的服务。它关心的只是发出信息的语法与语义。表示层要完成某些特定的功能，主要有不同数据码格式的转换，提供数据压缩、解压缩服务，对数据进行加密、解密。

表示层为应用层提供的服务包括语法转换、语法选择等。语法转换涉及代码转换和字符的转换、数据格式的修正以及数据结构操作的适配。语法选择提供初始选择一种语法和以后修正这种选择手段。

(7)应用层

网络应用层是通信用户之间的窗口，为用户提供网络管理、文件传输、事务处理等服务。其中包含了若干独立的、用户通用的服务协议模块。作为 OSI 的最高层，应用层为网络用户之间的通信提供专用的程序。应用层的内容主要取决于用户的各自需要，这一层涉及的主要问题是：分布数据库、分布计算机技术、网络操作系统和分操作系统、远程文件传输、电子邮件、终端电话及远程作业登录与控制等。在 OSI 的 7 个层次中，应用层是最复杂的，所包含的应用层协议也最多，有些协议还在研究和开发之中。

总之，可以将上述各层的主要功能归纳如下：

物理层：将比特流送到物理媒体上传送，即相当于对上一层的每一步应怎样利用物理媒体；

数据链路层：在数据链路上无差错地传送帧，即相当于每一步应该怎样走；

网络层：分组转送、路由选择和流量控制，即相当于走哪条路可达到该处；

传输层：从端到端网络透明地传送报文，即相当于对方在何处；

会话层：会话的管理与数据传输的同步，即相当于轮到谁讲话和从何处讲；

表示层：数据格式的转换，即相当于对方看起来像什么；

应用层：与用户应用进程的接口，即相当于做了什么。

1.2.2 TCP/IP 参考模型

TCP/IP 是目前 Internet 所使用的一组基本协议集，狭义的 TCP/IP 包括传输控制协议(Transfer Control Protocol，TCP)和网际协议(Internet Protocol，IP)两个协议，而广义的 TCP/IP 已经成了 Internet 协议的代称，包括从物理接口直到用户应用层的一系列协议集。它实际上包括上百个各种功能的协议，如远程登录、文件传输和电子邮件等，其中 TCP 协议和 IP 协议是保证数据完整传输的两个基本的重要协议。

1. TCP/IP 的层次划分及功能

TCP/IP 协议 4 层结构如图 1.5 所示。

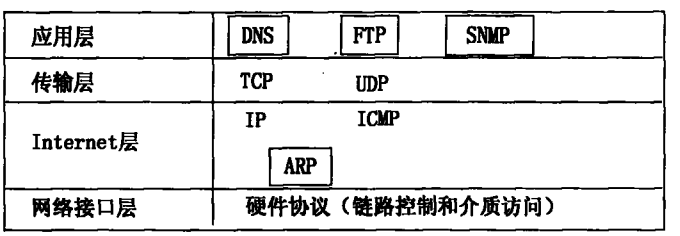

图 1.5 TCP/IP 参考模型