普通高等教育“十五”国家级规划教材

网络安全

徐国爱　主编

北京邮电大学出版社
·北京·

信息安全专业系列教材

编　委　会

总　　序

办好信息安全本科专业的第一要素是拥有高质量的教材。由于各方面的原因,我国开办信息安全本科专业的历史很短,刚刚起步,但是,当前以各种形式开办信息安全本科专业的高等院校却非常多,学生总数也相当可观,而且其中大部分学生已经学完基础课程,即将进入专业课的学习阶段。

与信息安全本科专业招生的火爆场面形成鲜明对比的是,到目前为止,我国还没有一套自己的信息安全本科专业系列教材。为了保证信息安全本科专业学生的培养质量,2001 年,北京市教委以“精品教材立项”的形式委托我们北京邮电大学信息安全中心负责编写《现代密码学基础》、《信息安全概论》、《网络安全》、《信息隐藏与数字水印》、《入侵检测》、《计算机病毒原理及防治》等 6 本教材,随后,教育部又将此套系列教材列入了“普通高等教育‘十五’国家级教材规划”。由此可见,此套教材的编写确实受到了各级教育主管部门的高度重视。

北京邮电大学信息安全中心是一专门从事信息安全的教学、科研和成果转化的重点实验室。该实验室已经培养出了我国第一位密码学博士,而且在“信息安全”和“密码学”两个专业领域内健全了博士后、博士、硕士和本科的培养教育体系,已经培养出了数以百计的信息安全研究生。

在接受了北京市教委和教育部的编写信息安全本科系列教材的任务之后,我们立即组织了最强的师资队伍投入到教材的编写工作之中。经过两年多的不懈努力,数易其稿,反复研讨,按照教育目标和大学生基本素质培养的要求,本着推进理工融合及学科交叉的思想,经过优化课程体系和精选课程内容,我们终于完成了信息安全本科专业系列教材的第一批教材(共 6 本)。现在我们正在着手规划信息安全本科专业的第二批教材,它们的暂定名分别是《安全操作系统》、《安全数据库》、《安全访问控制》、《安全检测与监控》、《数字证书与管理》、《安全备份与灾难恢复》、《安全隔离技术》、《安全服务技术》、《安

全系统工程》、《安全规范与标准》等。我们诚意邀请国内所有高等院校的权威安全专家加入第二批教材的编写工作(有意者请与我们直接联系。地址:100876,北京邮电大学信息安全中心126信箱)。我们希望这套信息安全本科专业系列教材最终完成之后能够基本满足国内各类高校信息安全本科专业的普遍需求。

虽然我们的目标是编写一套适合信息安全专业本科生使用的精品教材,但是,由于水平有限,时间仓促,且信息安全本科专业刚刚开始,我们还没有足够的实践机会,不足之处和错误在所难免,恳请读者和同行专家多提意见,以便我们再版时充分修改,不断完善。

衷心感谢北京邮电大学胡正名教授对本套教材的大力支持,感谢北京邮电大学信息安全中心二百余位成员的支持与配合。本套教材也是国家自然科学基金项目(90204017, 60372094, 60373059)和国家“973”项目(G1999035804)资助的成果,在此一并表示感谢。

杨义先 教授、博士生导师、全国政协委员
2004年1月于北京邮电大学信息安全中心

内 容 简 介

本书作为信息安全系列教材之一,全面系统地介绍了作为信息安全主要内容之一的网络安全的核心技术和其在电子商务中的应用。全书内容分为 3 个部分,第一部分(第 1～2 章)在对互联网系统简要介绍的基础上,对网络系统进行了细致的安全性分析;第二部分(第 3～7 章)是对网络安全主流技术的集中分析,内容涵盖 PKI、防火墙、虚拟专网、入侵检测和病毒防护;第三部分(第 8 章)以电子商务作为网络安全应用技术进行分析。每章后面配有习题,以巩固相关知识。

本书可作为高等院校计算机、通信、信息等专业研究生和高年级本科生的教材,也可作为计算机、通信、信息等领域研究人员和专业技术人员的参考书。

图书在版编目(CIP)数据

网络安全/ 徐国爱主编 .—北京:北京邮电大学出版社,2003
ISBN 7-5635-0647-0

Ⅰ .网 . . . Ⅱ .徐 . . . Ⅲ .计算机网络—安全技术—教材 Ⅳ .TP393 .08

中国版本图书馆 CIP 数据核字(2003)第 113198 号

书　　名:网络安全
主　　编:徐国爱
责任编辑:王晓丹
出版发行:北京邮电大学出版社
社　　址:北京市海淀区西土城路 10 号(邮编:100876)
电话传真:010-62282185(发行部)　010-62283578(FAX)
电子信箱:publish@bupt .edu .cn
经　　销:各地新华书店
印　　刷:
开　　本:787 mm×1 092 mm　1/ 16
印　　张:19
字　　数:414 千字
印　　数:1—5 000 册
版　　次:2004 年 5 月第 1 版　2004 年 5 月第 1 次印刷

ISBN 7-5635-0647-0/ TP·79　　定　价:29 .00 元

前　言

随着计算机和网络应用在社会政治、经济、文化、生产等领域的普及，社会信息化建设已初具规模，这给我国经济发展和社会进步带来了前所未有的机遇。然而，同时产生的信息安全问题，不仅阻碍了计算机和网络应用的进一步普及，而且还影响现有的应用，直接给国家和人民带来经济或名誉的损害；网络和相关信息系统价值的进一步挖掘更是受到制约，信息安全已成为制约社会信息化发展的瓶颈。网络安全作为信息安全的一个主要方面，已受到业内专家和学者的广泛关注。提高全社会的网络安全意识，已成为保障我国信息化建设长期、稳定、健康发展的关键工作之一。

北京邮电大学信息安全中心从 1984 年以来，一直专注于信息安全领域的理论和应用研究，先后承担过数项国家级信息安全相关课题的研究，并成功地将其中的大部分成果的实现商业转化，为国家信息化建设做出了贡献。信息安全系列是专为信息安全教学和科研推出的一款系列书籍，内容涵盖信息安全领域的方方面面。系列教材既可作为高等院校信息安全及相关专业研究生和高年级本科生的教材用，也可作为相关专业人员全面参考的系列手册。

本书作为信息安全系列教材之一，全面系统地介绍了作为信息安全主要内容之一的网络安全的基本原理、主流技术和典型应用。本书在编写过程中，除引用了作者自身的研究内容和成果之外，还大量参考了众多国内外优秀论文、书籍以及互联网上公布的相关资料，我们尽量在参考文献中列出，但由于互联网上资料数量众多、出处杂乱，可能无法将所有文献一一注明出处。我们对这些资料的作者表示由衷的感谢，同时声明，原文版权属于原作者。全书内容分为 3 个部分，第一部分(第 1～2 章)在对互联网系统简要介绍的基础上，对网络系统进行了细致的安全性分析；第二部分(第 3～7 章)是对网络安全主流技术的集中分析，内容涵盖 PKI、防火墙、虚拟专网、入侵检测和病毒防护；第三部分(第 8 章)以电子商务作为网络安全经费应用进行分析。每章后面配有习题，以巩固相关知识。

本书对网络安全技术的介绍较为全面。作为教材，教师在授课时可以根

据学时安排做出一些取舍。本书全部讲授建议 40 学时;如果只有 34 学时,建议将第 8 章作为选讲内容。

本书由北京邮电大学信息安全中心组织编写。第 1、2、3、4、5、6 和 8 章由徐国爱编写。第 7 章由魏文强编写,同时魏文强还参与了第 1、2 章的编写工作。徐庆参与了第 5 章的编写工作。邓玉峰参与了第 3 章的编写工作。全书由徐国爱统稿,魏文强协助。张胜、徐庆和曹华平等参与了部分资料的收集、整理、录入和校订工作。此外,本书得到了胡正明教授和编委会其他老师的大力支持和指导,他们对书中的内容提出了宝贵的意见,在此一并表示衷心的感谢。

网络安全是一门应用性很强的学科,在网络大规模普及的今天,已得到了长足的发展。本书尝试对此领域的理论和技术做一些归纳,以期有益于读者。由于作者的水平有限,书中难免有一些缺点和错误,真诚希望读者不吝赐教,以期再版修订。

作　者

2004 年 3 月

目　　录

第 2 章　安全分析

第 3 章　PKI 认证

第 1 章　网络基础

TCP/ IP 协议使世界上不同体系结构的计算机网络互联在一起,形成了一个全球性的广域网络——Internet,全球范围内的信息共享成为现实。TCP/ IP 是 Internet 事实上的协议标准,本章集中介绍 TCP/ IP 的层次结构和各层所包含的不同协议的关键流程和相关规格。

1.1　TCP/ IP 体系

1.1.1　网络概念

计算机网络(也称网络)是为满足应用的需要而发展起来的。对网络可做如下定义:将处于不同地理位置,并具有独立计算能力的计算机系统经过传输介质和通信设备相互连接,在网络操作系统和网络通信软件的控制下,实现资源共享的计算机的集合。

网络是一个独立自治、相互连接的计算机集合。独立自治意味着每台联网的计算机是完整的计算机系统,可以独立运行用户的作业;相互连接意味着两台计算机之间能够相互交换信息。计算机之间的连接是物理的,由硬件实现。计算机连接所使用的介质可以是双绞线、同轴电缆或光纤等有线介质;也可以是无线电、激光、大地微波或卫星微波等无线介质。计算机之间的信息交换具有物理和逻辑上的双重含义。在计算机网络的最底层(通常为物理层),信息交换体现为直接相连的两台机器之间无结构的比特流传输;而在物理层之上的各层所交换的信息便有了一定的逻辑结构,越往上逻辑结构越复杂,也越接近用户真正需要的形式。信息交换在低层由硬件实现,而到了高层则由软件实现。

网络的分类标准很多,比如按拓扑结构、介质访问方式、交换方式以及数据传输率等划分。按网络覆盖范围的大小,我们将计算机网络分为局域网(LAN, Local Area Network)、城域网(MAN, Metropolitan Area Network)、广域网(WAN, Wide Area Network)和互联网(Internet),如表 1-1 所示。不同规模的网络将采用不同的技术,下面将简要介绍上述几种网络。

表 1-1　计算机网络分类(按网络覆盖范围分)

类型	分布距离	覆盖范围
局域网	1 000 m	房间、建筑物、校园
城域网	10 km	城市
广域网	100 km	国家
互联网	1 000 km 以上	全球范围

1.局域网

局域网是指范围在几百米到十几公里内办公楼群或校园内的计算机相互连接所构成的计算机网络。局域网被广泛应用于连接校园、工厂以及机关的个人计算机或工作站,以利于个人计算机或工作站之间共享资源(如打印机)和数据通信。

局域网区别于其他网络主要体现在下面 3 个方面:

网络所覆盖的物理范围;

网络所使用的传输技术;

网络的拓扑结构。

局域网中经常使用共享信道,即所有的机器都接在同一条电缆上。传统局域网具有高数据传输率(10 Mbit/s 或 100 Mbit/s)、低延迟和低误码率的特点。新型局域网的数据传输率可达每秒千兆位,甚至更高。

局域网有不同的拓扑结构。图 1-1 给出了两种不同网络拓扑结构的示意图。

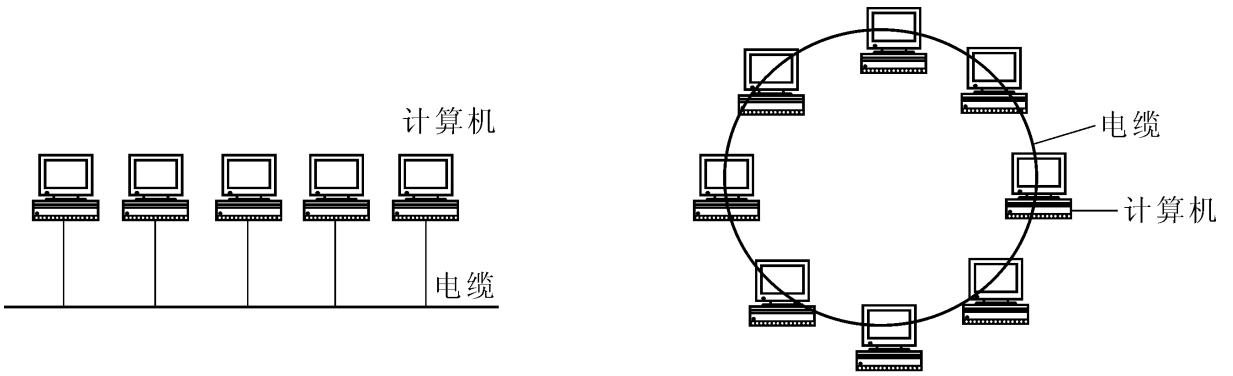

图 1-1　局域网的两种拓扑结构

如图 1-1(a)所示,在总线结构的网络中,任何时刻只允许一台机器发送数据,而所有其他机器都处于接收状态。当有两台或多台机器想同时发送数据时,必须进行仲裁,仲裁机制可以是集中式也可以是分布式的。例如 IEEE 802.3(以太网),它是基于共享总线、采用分布控制机制和数据传输率为 10 Mbit/s 的局域网。以太网中的站点机器可以在任意时刻发送数据,当发生冲突时,每个站点机器立即停止发送数据,并等待一个随机长的

时间继续尝试数据发送。

局域网的第二种类型是环形网,如图 1-1(b)所示。在环形网中,数据沿着环不停地旋转。同样的道理,在环形网中必须有一种机制用于仲裁不同机器站点对环的同时访问。IEEE 802 .5(IBM 令牌环)就是一种常用的数据传输率为 4 Mbit/ s 或 16 Mbit/ s 的环形局域网。

2 .城域网

城域网所采用的技术基本上与局域网相类似,只是规模上要大一些。城域网既可以覆盖相距不远的几栋办公楼,也可以覆盖一个城市;既可以是私人网,也可以是公用网;既可以支持数据和语音传输,也可以与有线电视相连。城域网一般只包含一到两根电缆,没有交换设备,因而其设计就比较简单。

将城域网作为一种网络类型的主要原因是其有标准而且已经实现,该标准的名称为分布式队列双总线(DQDB, Distributed Queue Dual Bus),它现在已经成为国际标准,编号为 IEEE 802 .6。DQDB 的工作范围一般是 160 km,数据传输率为 44 .736 Mbit/ s。

DQDB 采用两条单向总线,如图 1-2 所示,这两条平行的单向总线贯穿于整个城市,每个站点都同时与这两条总线相连。其中每条总线都有一个端接点,各自产生一个 53 字节的信元流,每个信元都从端接点沿着总线往下传,当它到达终点时,就从总线中消失。

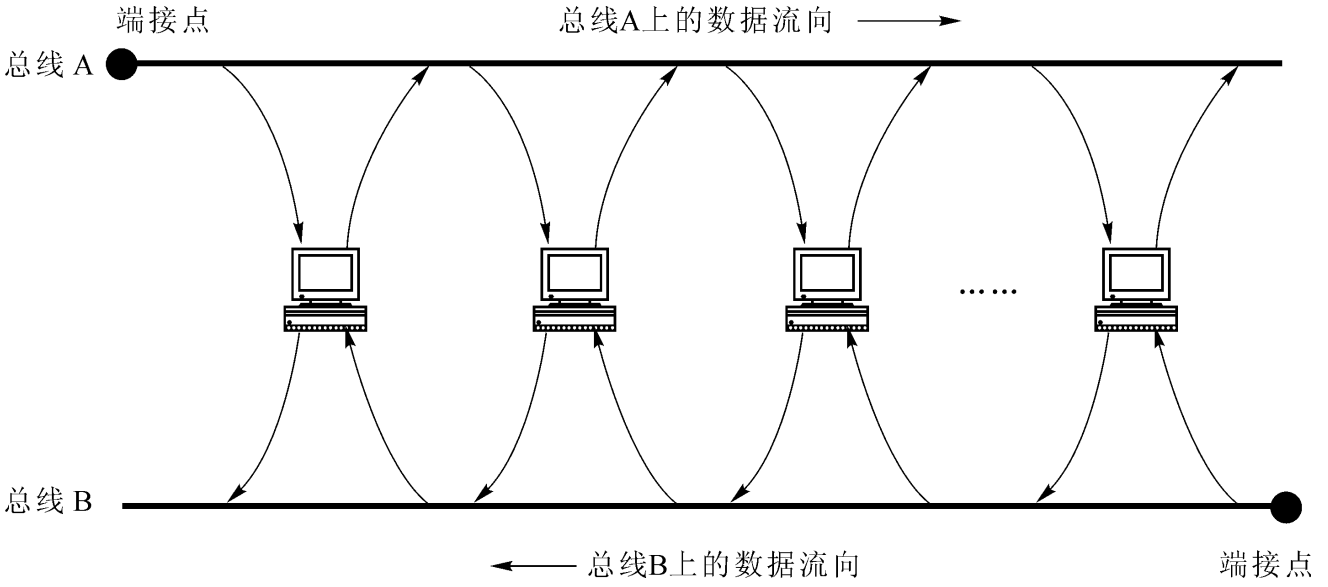

图 1-2　DQDB 城域网的结构

每个信元带有 44 字节的有效载荷,而且每个信元中带有两个标志位:“忙(Busy)”位和“请求(Request)”位。当“忙”标志位为 1,表示该信元已被占用;当某站点想发出请求时,将信元的“请求”标志位置为 1。

每个站点在发送信元之前必须知道目的站点是位于其右方还是左方。如果目的站点位于其右方,发送站点使用总线 A,否则使用总线 B。在 DQDB 中,每个站点的数据是通过“线或”电路输入到相应的总线中,因此某个站点的失效不会造成整个网络的瘫痪。

在 802 .6 标准中,站点是按照先进先出的原则进行排队发送数据的。802 .6 采取的发送原则是每个站点必须有“礼貌”,即每个站点必须等到其下方的站点发送完后自己才能发送。这种“礼貌”的目的是为了防止下列情况的发生,即离端接点最近的站点将经过它的所有空闲信元全部捕获并填入内容,致使其后的站点被“饿死”。

3 .广域网

广域网通常跨接很大的物理范围,如一个国家。其包含很多用来运行用户应用程序的机器集合,我们通常把这些机器叫做主机(Host);把这些主机连接在一起的是通信子网(Communication Subnet)。通信子网的任务是在主机之间传送报文。将计算机网络中的纯通信部分的子网与应用部分的主机分离开来,可以大大简化网络的设计。广域网的物理结构如图 1-3 所示。

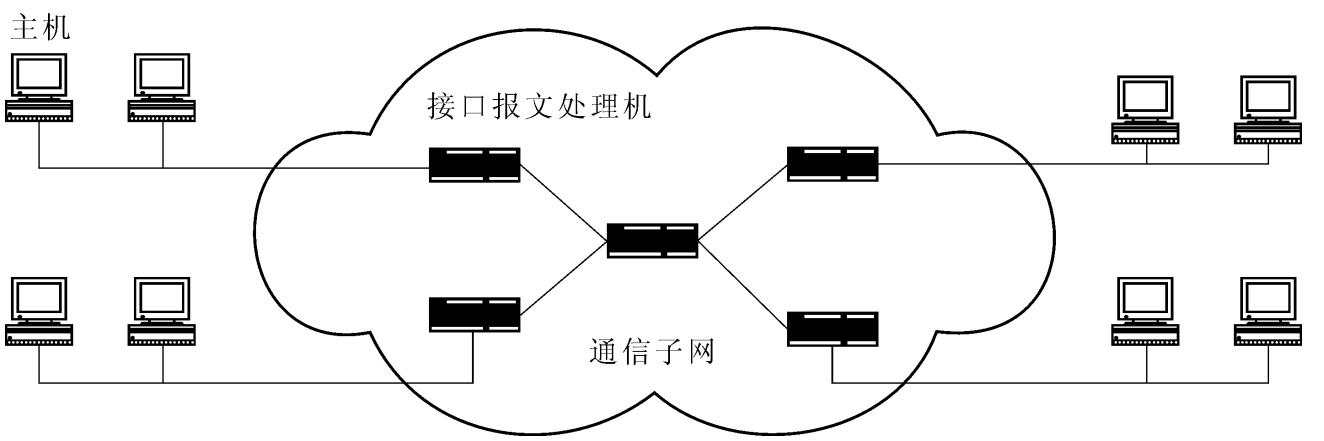

图 1-3　广域网物理结构

在大多数广域网中,通信子网一般都包括两部分:传输信道和转接设备。传输信道用于在机器间传送数据;转接设备是专用计算机,用来连接两条或多条传输线。当数据从一条输入信道到达后,转接设备必须选择一条输出信道,把数据继续向前发送。在 ARPANET 网中,转接设备叫作接口报文处理机(IMP, Interface Message Processor)。在图 1-3 所示模式中,每一台主机都至少连着一台 IMP。所有出入该主机的报文,都必须经过与该主机相连的 IMP。

绝大多数广域网中,通信子网包含大量租用线路或专用线路,每一条线路连着一对 IMP。当报文从源节点经过中间 IMP 发往远方目的节点时,每个 IMP 将输入的报文完整接收下来并储存起来,然后选择一条空闲的输出线路,继续向前传送,因此这种子网又称为点到点(Point-to-Point)子网、存储转发(Store-and-Forward)子网。除了那些使用卫星的广域网外,几乎所有的广域网都采用存储转发方式。

广域网最初只是为使物理上广泛分布的计算机能够进行简单的数据传输,主要用于交互终端与主机的连接、计算机之间文件或批处理作业传输以及电子邮件传输等。

广域网的另外一种可能的组网方式是卫星或地面无线电网。每个中间转接站点都通过天线接收和发送数据。所有的中间站点都能接收到来自卫星的信息,并能同时听到其