21

21世纪高职高专规划教材
电子商务专业系列

电子商务
网络安全与防火墙技术

陈孟建 徐金华 邹玉金 编著

清华大学出版社

21

21世纪高职高专规划教材

电子商务专业系列

电子商务

网络安全与防火墙技术

陈孟建 徐金华 邹玉金 编著

清华大学出版社
北京

内 容 简 介

本书是通用的电子商务网络安全与防火墙技术教材，从电子商务网络安全技术角度出发，讲授构建和实施安全电子商务系统所必需的基本理论、方法和技术，全书在编排上注意由浅入深和循序渐进，力求通俗易懂、简洁实用。本书主要内容包括：电子商务网络安全基础、网络体系结构与协议、电子商务密码技术、电子商务安全认证体系、Windows 操作系统安全、防火墙基础、防火墙技术与应用、防火墙管理与测试、综合实训。

本书观点新颖，论述深入浅出，内容丰富，可读性好，实践性强，特别适合作为高职高专学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材，也可以作为计算机和电子商务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

电子商务网络安全与防火墙技术/陈孟建，徐金华，邹玉金编著. —北京：清华大学出版社，2011.4
(21 世纪高职高专规划教材. 电子商务专业系列)
ISBN 978-7-302-24814-9

Ⅰ. ①电… Ⅱ. ①陈… ②徐… ③邹… Ⅲ. ①电子商务－网站－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 033031 号

责任编辑：孟毅新
责任校对：袁　芳
责任印制：何　芊
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：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京市清华园胶印厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：19　**字　数**：448 千字
版　　次：2011 年 4 月第 1 版　　**印　　次**：2011 年 4 月第1 次印刷
印　　数：1～3000
定　　价：38.00 元

产品编号：037522-01

前　言

因特网的发展已成燎原之势，它的应用也从原来的军事、科技、文化和商业渗透到当前社会的各个领域。越来越多的网络联入了因特网，越来越多的信息进入了因特网。因特网吸引了亿万用户，很多人已经离不开因特网，并且每天都在访问它、应用它。

随着因特网的发展，网络与信息的安全问题也越来越受到人们的重视。电子商务是因特网应用发展的必然趋势，也是国际金融贸易中越来越重要的经营模式。安全是保证电子商务健康有序发展的关键因素。目前安全问题已成为电子商务的核心问题。由于Internet本身的开放性，使电子商务系统面临着各种各样的安全威胁。

大量的事实说明，要保证电子商务的正常运作，就必须高度重视电子商务的安全问题。防火墙已经成为保护网络和计算机的代名词，只有全面理解防火墙的作用、防火墙的部署、防火墙的不同类型等才能完善安全防范手段。

本书从电子商务信息安全技术角度出发，讲授构建和实施安全电子商务系统所必需的基本理论、方法和技术，全书在编排上注意由浅入深和循序渐进，力求通俗易懂、简洁实用。本书主要内容包括：电子商务网络安全基础、网络体系结构与协议、电子商务密码技术、电子商务安全认证体系、Windows操作系统安全、防火墙基础、防火墙技术与应用、防火墙管理与测试、综合实训。本书观点新颖，论述深入浅出，内容丰富，可读性好，实践性强，特别适合作为高职高专学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材，也可以作为计算机和电子商务领域研究人员和专业技术人员的参考书。

本书由浙江经贸职业技术学院陈孟建、浙江工商大学徐金华和邹玉金共同编写。在编写过程中，得到了张贵君、陈奕婷、李锋之、袁志刚、傅俊等专家、教授们的帮助，在此表示衷心的感谢！

由于编者水平有限，书中不当之处敬请读者批评指正。

编　者

2011年3月于杭州

目　录

第 1 章

电子商务网络安全基础

电子商务运营在因特网上，因此，电子商务网络的安全问题正日益突出且越来越复杂。一方面电子商务网络为用户提供了丰富的共享资源；另一方面，电子商务网络的脆弱性和网络安全问题的复杂性使得电子商务应用变得更为复杂。本章主要介绍电子商务网络安全的基础知识。通过本章的学习，要求：

（1）掌握电子商务网络安全的基本概念。

（2）了解威胁电子商务网络安全的主要攻击手段。

（3）掌握电子商务网络安全模型。

（4）掌握电子商务网络安全保障机制。

1.1 计算机网络概述

1.1.1 计算机网络定义

随着计算机技术的发展和应用的深入，越来越多的用户希望能共享信息资源，也希望各台计算机之间能互相传递信息。微型计算机的硬件和软件配置一般都比较低，其功能也有限，因此希望将大型与巨型计算机的硬件和软件资源以及它们所管理的信息资源共享给众多的微型计算机，以便充分利用这些资源。基于这些原因，计算机开始向网络化发展，分散的计算机被联成网，组成计算机网络。

1. 计算机网络定义

资源共享观点将计算机网络定义为“以能够相互共享资源的方式互联起来的自治计算机系统的集合”。也就是说，将在地理上分散的、具有独立功能的多台计算机通过通信媒介连接在一起，按照网络协议进行数据通信，实现相互之间的通信和信息交换，并配以相应的网络软件，实现资源共享（包括硬件和软件）的系统，称为计算机网络。

通过对计算机网络定义的分析，可以看出作为一个计算机网络必须具备以下基本要素。

（1）至少有两台具有独立操作系统的计算机。

（2）计算机之间要采用一定的通信手段相互连接起来。

（3）计算机之间要遵守相互通信的规则，也就是协议。

(4) 配有网络软件。

(5) 实现计算机资源共享。

从资源、用户和管理角度来看,计算机网络的定义如下。

(1) 从资源角度来看,网络是能够共享外部设备(例如,打印机、专用设备、外部大容量磁盘等)和公共信息的系统(例如,公共数据库系统、数据库等)。

(2) 从用户角度来看,网络是能够把个人与众多的计算机用户连接在一起的系统。

(3) 从管理角度来看,网络是能够对数据进行集中管理的系统(例如,备份服务、系统软件安装服务等)。

2. 计算机网络的功能

(1) 资源共享

资源共享是计算机网络的主要功能,也是计算机网络最具有吸引力的地方。资源共享指的是网络上的用户都能够部分或全部地享受网络中的各种资源,如文件系统、外部设备、数据信息以及各种服务等,使网络中各地区的资源互通有无,分工协作,从而大大提高系统资源的利用率。

(2) 远程传输

计算机已经由科学计算向数据处理方面发展,由单机向网络方面发展,且发展迅速。相距很远的用户可以互相传输数据信息,互相交流,协同工作。

(3) 集中管理

计算机网络技术的发展和应用,已使现代办公、经营管理等发生了很大变化。目前,已经有许多 MIS(Management Information System,管理信息系统)、OA(Office Automation,办公自动化)系统等,通过这些系统可以实现日常工作的集中管理,提高工作效率,增加经济效益。

(4) 实现分布式处理

网络技术的发展,使得分布式计算成为可能。对于大型的课题,可以将其分为许多小题目,由不同的计算机分别完成,然后再集中起来解决问题。

(5) 负载平衡

负载平衡是指工作被均匀地分配给网络上的各台计算机。网络控制中心负责分配和检测,当某台计算机负载过重时,系统会自动将部分工转移给负载较轻的计算机去处理。

(6) 综合信息服务

通过计算机网络可以向全社会提供各种经济信息、商业信息、物流信息、科研情报和咨询服务等。特别是最近掀起的电子商务热潮,就是利用 Internet 实现企业与企业之间、企业与消费者之间、消费者与消费者之间、企业与政府之间的各种综合信息的服务。又如,综合业务数据网络就是将电话、传真机、电视机、复印机等办公设备纳入计算机网络中,提供数字、声音、图形、图像等多种信息传递功能的系统。

3. 计算机网络的特点

虽然各种计算机网络系统的具体用途、系统结构、信息传输方式等各不相同,但这些

网络系统都具有一些共同的特点，就是可靠性高、可扩充性强、易于操作和维护、效率高、成本低，可实现资源共享等。

1.1.2　计算机网络组成

1. 计算机资源子网和通信子网

从网络系统功能的角度来看，计算机网络是由资源子网和通信子网组成的，如图 1-1 所示。

（1）资源子网主要负责全网的信息处理，为网络用户提供网络服务和资源共享功能等。它主要包括网络中所有的主计算机、I/O 设备、终端、各种网络协议、网络软件和数据库等。

（2）通信子网主要负责全网的数据通信，完成数据传输、转接、加工和变换等通信处理工作。它主要包括通信线路（即传输介质）、网络连接设备（如网络接口设备、通信控制处理机、网桥、路由器、交换机、网关、调制解调器、卫星地面接收站等）、网络通信协议和通信控制软件等。

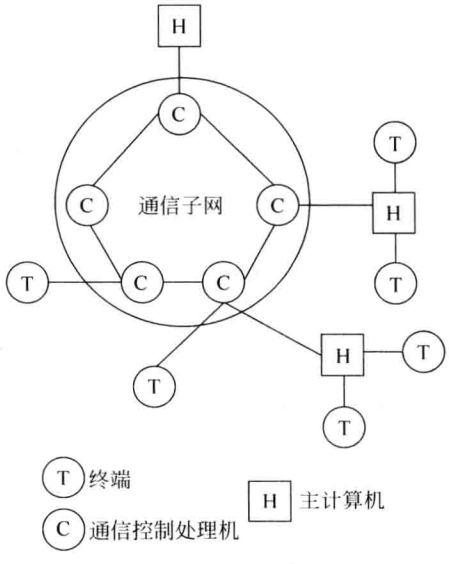

图 1-1　资源子网和通信子网

2. 计算机网络硬件

计算机硬件包括主机、终端、用于信息变换和信息交换的通信节点设备、通信线路和网络互联设备等。

（1）主机负责处理网络中的数据、执行网络协议、进行网络控制和管理等工作，也包括管理供用户共享访问的数据库，它与其他主机系统互联后构成网络中的主要资源。

（2）终端是用户访问网络的设备，其主要作用是把用户输入的信息转变为适合传送到网络上的信息，或把网络上其他节点输出的、经过通信线路的信息转变为用户能识别的信息。

（3）用于信息变换和信息交换的通信节点设备主要有通信控制处理机、调制解调器、集中器和多路复用器等。通信控制处理机是在数据通信系统或计算机网络系统中执行通信控制与处理功能的设备；调制解调器是把用户数据设备与模拟通信线路连接起来的一种接口设备，它主要实现数字信号与模拟信号的变换功能；集中器是设置在终端密集处、完成终端一侧的通信处理与复用的设备；多路复用器是实现多路信号在同一条线路上传输的设备。

（4）通信线路是传输信息的媒体，计算机网络中的通信线路有有线线路（包括双绞线、同轴电缆、光纤）和无线线路（包括微波线路和卫星线路等）。

（5）网络互联设备用于将两个或两个以上的网络连接起来，构成一个更大的互联网络系统，常用的网络互联设备有网桥、路由器、交换机和网关等。

1.1.3 计算机网络类型

1. 根据网络传输技术进行分类

网络所采用的传输技术决定了网络的主要技术特点，因此，根据网络所采用的传输技术对网络进行分类是一种很重要的方法。

(1) 广播式网络

广播式网络所采用的传输技术是广播通信信道技术，该传输技术采用多个节点共享一个通信信道的方式，一个节点广播信息，其他节点必须接收信息。因此，在广播式网络中，所有连接网络的计算机都共享一个公共通信信道。当一台计算机利用共享通信信道发送报文分组时，所有其他的计算机都会“接收”到这个分组。由于发送的分组中带有目的地址与源地址，接收到该分组的计算机将检查目的地址是否与本节点地址相同，如果接收报文分组的目的地址与本节点地址相同，则接收该分组，否则丢弃该分组。

(2) 点到点式网络

点到点式网络所采用的传输技术是点到点通信信道技术，该传输技术采用一个信道线路与一对节点相连接的方式，其他计算机都不能“接收”信息。因此，在点对点网络中，每条物理线路连接一对计算机。如果两台计算机之间没有直接连接的线路，那么，它们之间的分组就要通过中间节点来接收、存储、转发直至目的节点。由于连接多台计算机之间的线路结构一般来说是比较复杂的，因此，从源节点到目的节点可能存在多条路由，决定分组从通信子网的源节点到达目的节点的路由需要通过路由选择算法来计算。

从以上内容可以看出，采用分组存储转发还是采用路由选择是区分广播式网络和点到点式网络的重要依据之一。

2. 根据网络的覆盖范围进行分类

根据网络的覆盖范围来划分网络类型，通常可划分为局域网(Local Area Network，LAN)、城域网(Metropolitan Area Network，MAN)、广域网(Wide Area Network，WAN)等类型。

(1) 局域网

局域网是属于某一个单位在某一个小范围内(即某一幢大楼、某一个建筑物、某一个学校内、某一所医院等)组建的计算机网络，该网络一般在10km范围内。该网络具有组网方便、使用灵活、操作简单等特点，组成该网络的计算机并不一定是微型计算机，该网络是目前计算机网络中发展最为活跃的一种网络，它起源于20世纪80年代初期，是随着微型计算机的大量使用而迅速发展起来的一种新型的网络技术。如果这一网络中的计算机都是微型计算机，则称这种网络为微机型局域网。

局域网具有以下几个特点。

① 局域网覆盖有限的地理范围，适用于学校、机关、公司、工厂等有限距离内的计算机、终端与各类信息处理设备的联网。

② 局域网一般为一个单位所有，易于建立、维护和扩展。

③ 局域网具有高数据传输速率(10～100Mb/s，甚至高达1Gb/s)、低误码率的高质量数据传输环境。

④ 决定局域网特性的主要技术要素有网络拓扑、传输介质、介质访问控制方法等。

⑤ 局域网从介质访问控制方法的角度可以分为两类，即共享介质局域网与交换局域网。

(2) 城域网

城域网的范围可以覆盖一组单位(如一个地区教育局及所属的所有学校)甚至一个城市。它基本上是一种大型的局域网，通常使用与局域网相同的技术，因此也可以归为局域网一类。其关键之处是使用了广播式介质，与其他类型的网络相比，极大地简化了设计。

(3) 广域网

广域网是一种涉及范围较大的远距离计算机网络，即一个地区、一个省、一个自治区、一个国家以及在它们之间甚至全世界建立的计算机网络，因此，又称为远程网，例如，环球网络 WWW、因特网 Internet 等。Internet 把全世界 180 多个国家的 30000 多万台计算机主机和近 3 亿个用户紧密地联系在一起，使用户之间互通信息，共享计算机和各种信息资源。

广域网传输的距离远，传输的装置和介质由电信部门提供，例如，长途电话线、微波和卫星通道、光缆通道等，也有使用专线电缆的。广域网是由多个部门或多个国家联合建立的，其规模大，能够实现较大范围内的资源共享。

广域网具有以下几个特点。

① 广域网覆盖地理范围广，信息传递距离可以从几十千米到几万千米甚至几十万千米。

② 信息传递速率比较低，一般都小于 0.1Mb/s。

③ 传输误码率在 10^{-4}～10^{-6}之间。

④ 广域网一般可以由多个局域网互联而成，广域网中包含了多种网络结构，并可以根据用户的需要进行随意组网。

1.2　电子商务网络安全概述

1.2.1　网络安全概述

1. 网络安全的定义

网络安全泛指网络系统的硬件、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，网络服务不被中断。

网络安全包括系统安全和信息安全两个部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全；信息安全主要指各种信息的存储、传输的安全，具体体现在保密性、完整性及不可抵赖性上。

2. 网络安全的内容

网络安全包括物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共和国家信息安全。

(1) 物理安全

物理安全是指保护计算机网络中的传输介质、网络设备和机房设施的安全。物理安

全包括防盗、防火、防静电、防雷击和防电磁泄漏等方面的内容。

物理上的安全威胁主要涉及对计算机或人员的访问，可用于增强物理安全的策略有很多，将计算机系统和关键设备布置在一个安全的环境中，销毁不再使用的敏感文档，保持密码和身份认证部件的安全性，锁住便携式设备等。物理安全的实施更多依赖于行政的干预手段并结合相关技术。如果没有基础的物理保护，例如带锁的开关柜、数据中心等，物理安全是不可能实现的。

(2) 逻辑安全

计算机网络的逻辑安全主要通过用户身份认证、访问控制、加密等方法来实现。

① 用户身份认证。身份证明是所有安全系统不可或缺的一个组件。它是区别授权用户和入侵者的唯一方法。为了实现对信息资源的保护，并知道何人试图获取网络资源的访问权，任何网络资源拥有者都必须对用户进行身份认证。当使用某些更尖端的通信方式时，身份认证特别重要。

② 访问控制。访问控制是制约用户连接特定网络、计算机与应用程序，获取特定类型数据流量的方法。访问控制系统一般针对网络资源进行安全控制区域划分，实施区域防御的策略。在区域的物理边界或逻辑边界使用一个许可或拒绝访问的集中控制点。

③ 加密。加密是指在访问控制和身份验证过程中系统完全有效，在数据信息通过网络传送时，企业仍可能面临被窃听的风险。事实上，低成本和连接的简便性已使 Internet 成为企业内和企业间通信的一个极为诱人的媒介。同时，无线网络的广泛使用也在进一步加大网络数据被窃听的风险。加密技术用于针对窃听提供保护。它通过使信息只能被具有解密数据所需密钥的人员读取来提供信息的安全保护。

(3) 操作系统安全

计算机操作系统是一个“管家婆”，担负着自身巨大的资源管理、频繁的输入输出控制，以及不可间断的用户与操作系统之间的通信任务。由于操作系统具有“一权独大”的特点，所有针对计算机和网络入侵及非法访问者是以摄取操作系统的最高权限作为入侵目的的。因此，操作系统安全的内容就是采用各种技术手段和采取合理的安全策略，以降低系统的脆弱性，使计算机处于安全、可靠的工作环境中。

(4) 联网安全

联网安全指的是保证计算机联网后操作系统安全运行和计算机内部信息的安全。联网安全性可以通过以下几个方面的安全服务来达到。

① 联网计算机用户必须采取适当的措施，确保自己的计算机不会受到病毒的侵袭。

② 访问控制服务，用来保护计算机和联网资源不被非授权使用。

③ 通信安全服务，用来认证数据机密性与完整性，以及通信的可信赖性。

1.2.2 影响网络安全的因素

影响网络安全的因素有以下几个。

1. 硬件系统

网络硬件系统的安全隐患主要来源于设计，主要表现为物理安全方面的问题，包括各

种计算机或者网络设备，除了难以抗拒的自然灾害外，温度、湿度、静电、电磁场等也可能造成信息的泄露或失效。

2. 软件系统

软件系统的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞。软件系统的安全隐患主要表现在操作系统、数据库系统和应用软件上。

3. 病毒

计算机病毒将网络作为自己繁殖和传播的载体及工具，造成的危害越来越大。Internet 带来的安全威胁来自文件下载及电子邮件，邮件病毒凭借其危害性强、变形种类繁多、传播速度快、可跨平台发作、影响范围广等特点，利用用户的通讯簿散发病毒，通过用户文件泄密信息。邮件已成为目前病毒防治的重中之重。

4. 配置不当

安全配置不当会造成安全漏洞，例如，防火墙软件配置不正确将使得它失去应有作用。对特定的网络应用程序，当它启动时，就打开了一系列的安全缺口，许多与该软件捆绑在一起的应用软件也会被启用，除非用户禁止该程序或对其进行正确配置，否则，安全隐患始终存在。

5. 网络通信协议

目前在 Internet 上普遍使用的标准主要基于 TCP/IP 架构。TCP/IP 不是一个而是多个协议，TCP 和 IP 只是其中最基本也是主要的两个协议。TCP/IP 协议是美国政府资助的高级研究计划署(Advanced Research Projects Agency，ARPA)在 20 世纪 70 年代的研究成果之一，目的是使全球的研究网络联在一起形成一个虚拟网络，也就是国际因特网。由于最初 TCP/IP 是在可信任环境中开发出来的成果，在协议设计的总体构想和设计阶段基本上未考虑安全问题，不能提供人们所需要的安全性和保密性。概括起来，Internet 存在以下严重的安全隐患。

(1) 缺乏用户身份鉴别机制

由于 TCP/IP 使用 IP 地址作为网络节点的唯一标志，在 Internet 中，当信息分组在路由器间传递时，对任何人都是开放的，路由器仅仅搜索信息分组中的目的地址，但不能防止其内容被窥视，其数据分组的源地址很容易被发现，由于 IP 地址是一种分级结构地址，其中包括了主机所在的网络，攻击者据此可以构造出目标网络的轮廓，因此使用标准 IP 地址的网络拓扑对 Internet 来说是暴露的。

另外，IP 地址很容易被伪造和更改，TCP/IP 缺乏对 IP 包中的源地址的真实性的鉴定和保密机制，因此，Internet 上的任何主机都可以产生一个带任意 IP 地址的 IP 包，从而假冒另一个主机 IP 地址进行欺骗，这样网上传输数据的真实性就无法得到保证。

(2) 缺乏路由协议鉴别认证机制

TCP/IP 在 IP 层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护。因此，可以通过 Internet 利用路由信息修改网络传输路径，误导网络分组传输。

(3) 缺乏保密性

TCP/IP 数据流采用明文传输，用户账号、口令等重要信息也无一例外。攻击者可以