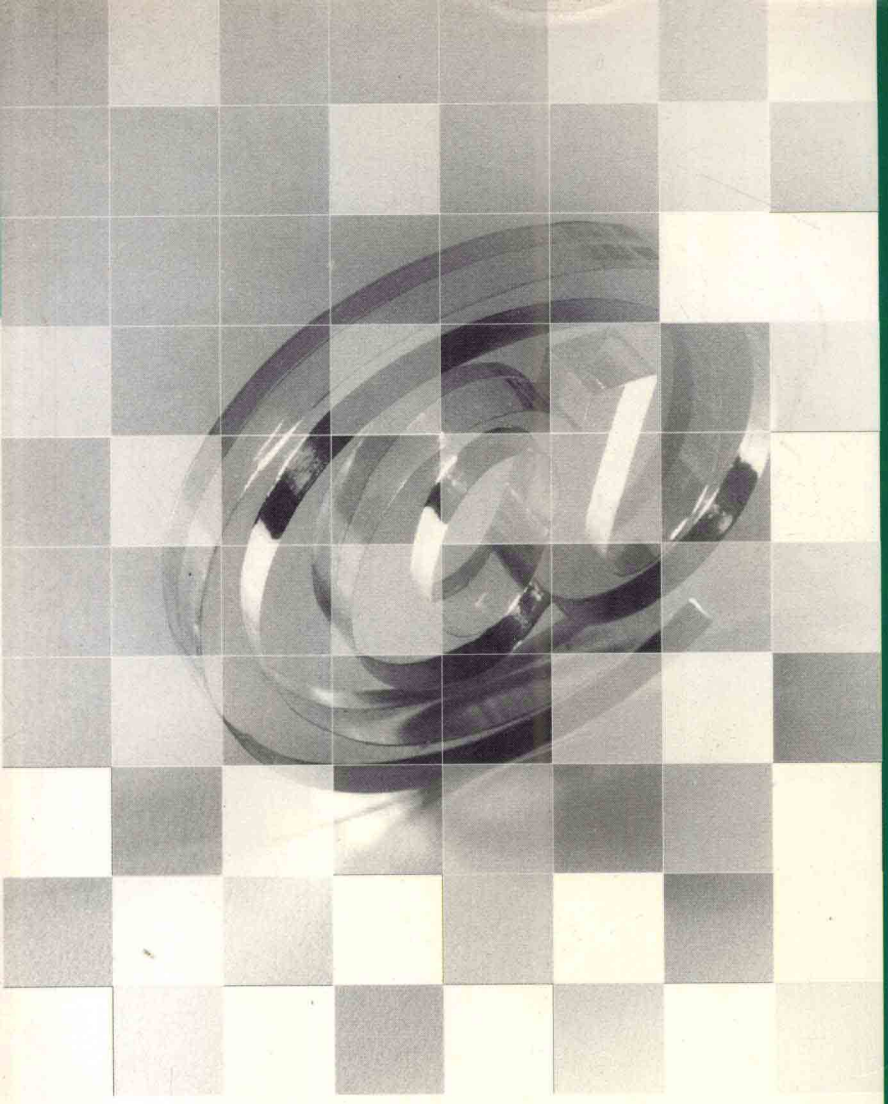
新编



e-commerce

XINBIAN GAOZHI GAOZHUAN
DIANZI SHANGWU
XILIE JIAOCAI

高职高专
电子商务系列教材

网络安全与认证

WANGLUO ANQUAN YU RENZHENG

◎ 编著　李　艇　冯　勇

重庆大学出版社

新编高职高专电子商务系列教材

网络安全与认证

Wangluo Anquan Yu Renzheng

■李 艇 冯 勇 编著

重庆大学出版社

内容提要

在计算机网络发展过程中网络安全技术是理论性和实践性都很强的一个新的发展方向和研究领域。本书对于网络安全基础、网络安全技术、电子商务的安全性及网络安全工具进行了较全面的介绍，并以任务驱动的方式，介绍网络安全工具的使用，使学生能够对 Windows 平台安全管理问题进行初步的分析和解决。

通过本书的学习，读者可以掌握计算机网络安全的基本概念，熟悉现行的网络安全技术应用。本书适合高职高专院校电子商务专业及相关专业的学生使用。

图书在版编目(CIP)数据

网络安全与认证/李艇，冯勇编著. —重庆：重庆大学出版社，2005.2
(新编高职高专电子商务系列教材)
ISBN 7-5624-3335-6

Ⅰ.网… Ⅱ.①李…②冯… Ⅲ.计算机网络—安全技术—高等学校：技术学校—教材
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 011226 号

网络安全与认证

李 艇 冯 勇 编著

责任编辑：王启志 梁 涛 版式设计：梁 涛
责任校对：任卓惠 责任印制：秦 梅

*

重庆大学出版社出版发行
出版人：张鸽盛
社址：重庆市沙坪坝正街 174 号重庆大学(A 区)内
邮编：400030
电话：(023) 65102378 65105781
传真：(023) 65103686 65105565
网址：http://www.cqup.com.cn
邮箱：fxk@cqup.com.cn (市场营销部)
全国新华书店经销
重庆铜梁正兴印务有限公司印刷

*

开本：787×960 1/16 印张：8.5 字数：153 千
2005 年 2 月第 1 版 2005 年 2 月第 1 次印刷
印数：1—4 000
ISBN 7-5624-3335-6 定价：14.00 元

编委会

总 序

近几年来，随着经济的发展和计算机应用技术的普及，电子商务作为现代商务活动中的交易方式已经得到了全社会的关注。据媒体介绍，有关部门已经将其列为当今最具热门的十大职业技术岗位之首。去年，由于“非典”的出现，诸多制造业、加工业、商业的经营者更加体会到电子商务应用于非接触经济后将会产生巨大的社会和经济效益。纵观较发达国家电子商务发展的历史，结合我国目前电子商务应用现状，可以预见，电子商务在现代商务活动中必将成为重要的交易方式和工具，其在经济发展和企业经营管理中的地位将是有目共睹，不可替代的。

但是，在构思本系列教材之前，系列教材编写委员会在部分地区和相关高职、高专院校进行过调研，深感无论是在电子商务应用方面，还是在电子商务专业的教学方面，依然存在着不容忽视的问题，而这些问题的存在严重制约着电子商务的普及和发展。目前，许多厂家、商家对于应用电子商务尚未从认识上予以高度重视，企业由于各方面条件的限制，商业网站建设及推广等硬件设施配置尚显不足，具有电子商务系统知识的专业人员十分缺乏，国家相应的法律、法规尚不完善等等。从高等职业教育发展看，尽管诸多高职院校近几年纷纷设置了电子商务专业并已经取得了相应的教学成果，但也存在着对电子商务培养目标定位、理论课和实训课程教学体系建设、校外实训基地建设等方面认识不清、重视不够等问题。天津职业大学在1999年较早开设了电子商务专业，并已经有了三届毕业生。该专业作为天津市市级教学改革试点专业，教学人员在专业建设方面为此付出了许多努力，并取得了相应的成果。在教材建设方面，广大教师在教学实践中体会到，

虽然近几年不同门类的电子商务教材诸多，有的教材编写也颇具水平，但存在着教材内容之间连贯性不够，知识广度和应用技能深度不一致等诸多问题。为此，作为电子商务专业建设的成果之一，天津职业大学联合了全国部分高职院校教师在重庆大学出版社的支持下编著并出版了“新编高职高专电子商务系列教材”。本系列教材共计14册，包括：商务基础、商务统计、电子商务法律、电子商务概论、网络营销、网络技术应用、网站建设与管理、网络安全与认证、网上支付与结算、数据库、电子商务与物流、网络广告、商务网页制作、电子商务模拟实验。

本系列教材的特点在于除系统介绍电子商务相关理论知识和应用技术外，侧重于各册书体现统一的教学目标和专业课程教学大纲，在内容方面，要求各册书相互衔接，互相补充，着重体现高职教育应用型教学特点的要求。在编写结构、体例方面，编委会要求力求做到简明、扼要，各册书均列出学习目的、本章小结和复习思考题及相关案例，以便教师教学和学生的学习。本系列教材的主编均是高职院校中具有副高级以上职称，从事多年电子商务专业的教学，在相关教材编写方面有着丰富经验的教师。编委会在教材编写过程中召开了数次研讨会，以保证系列教材的编写质量。在系列教材编写过程中，重庆大学出版社的领导和编辑给予了极大的支持和帮助，对此，编委会表示真挚的感谢。本系列教材预计在2005年春季出齐，届时，还请广大教师、同学和读者提出宝贵意见。

高职高专“电子商务系列教材”编委会

2004年7月

前言

信息共享与信息安全永远是互相矛盾的。而互联网的发展使信息安全的概念发生了根本性的变化，信息安全从单机扩展到网络连接的世界范围，同时，安全技术也得到新的发展，其内容极为丰富。而电子商务的安全问题实质上还是网络安全的问题，网络安全是从事电子商务领域的人员应该熟悉和掌握的一门技术。

电子商务安全主要包括网络安全和商务安全两个方面。网络安全是指计算机和网络本身可能存在的安全问题，也就是要保障电子商务平台的可用性和安全性，其内容包括计算机物理安全、系统安全、数据库安全、网络设备安全、网络服务安全等。商务安全则指商务交易在网络这种媒介中体现出的安全问题，包括防止商务信息被窃取、篡改、伪造以及交易行为被抵赖，也就是要实现电子商务的保密性、完整性、真实性和不可抵赖性。

安全性问题一直是电子商务令人担心的方面和关注的焦点，也将成为电子商务全面推广的主要障碍。有调查表明，电子商务网站越来越容易受到黑客的攻击，这不仅表现在网站受攻击而不能提供正常服务上，还经常表现为用户信用卡密码被非法获取并被冒用。可见网络安全是电子商务的基础。

本书针对高职和高专的特点组织编写，为从事电子商务安全维护方面的应用打下良好的基础。

本书分为网络安全基础、网络安全技术与协议、基于公钥的安全服务基础设施 PKI、防火墙与虚拟专用网、电子商务的安全性和网络安全工具 6 章，并选用免费版的网络安全工具作为教学实训软件。读者可以通过重庆大学出版社的网站

http://www.cqup.com.cn 下载本书所使用的实训工具及相关的辅助教学演示软件。

本书第1~2章、第4~6章由李艇编写，第3章由冯勇编写，全书由李艇统编。

本书中的部分实验由张峰晓、李睿同学做了一些基础性的工作，在此表示真诚的感谢。

本书在编写过程中始终得到了天津职业大学经济与管理学院的领导和老师的支持与帮助，在此对他们表示衷心的感谢。

限于编者的学术水平，书中错误和不当之处敬请读者批评指正。

作　者：李艇　冯勇

E-mail：litingcn@sina.com

2004年11月29日于天津

目　录

第1章 网络安全基础

〔学习要求〕

- 安全服务及安全机制
- 网络安全体系及评估标准
- 密码学基本原理
- 网络加密与密钥管理
- 安全威胁

网络在为人们提供更多的机会和方便，更加绚丽多彩地将世界展现在人们面前的同时也带来了一些新的问题。例如，人们的生活越来越依赖于网络及其存储的信息，一旦网络由于种种原因发生故障，陷于瘫痪，人们的生活也必然受到极大的影响。另外，计算机犯罪的日益增多也对网络的安全运行和进一步发展提出了挑战。因此，如何保证网络的安全以及如何保证网络上数据的完整性等问题越来越受到人们的高度重视。

1.1 安全服务及安全机制

计算机网络的安全性可以定义为：保障网络信息的保密性、完整性、网络服务可用性和可审查性，即要求网络保证其信息系统资源的完整、准确和具有一定的传播范围，并能及时提供所有用户所选择的网络服务。

ISO 7498—2 从体系结构的观点描述了 ISO 基本参考模型之间的安全通信必须提供的安全服务和安全机制，并说明了安全服务及其相应机制在安全体系结构中的关系，从而建立了开放互联系统的安全体系结构框架。

1.1.1 安全服务

安全服务(security services)是指开放某一层所提供的服务,用以保证系统或数据传输有足够的安全性。根据 ISO 7498—2 中提出的建议,一个安全的计算机网络应当能够提供以下的安全服务:

(1)认证

认证(authentication)安全服务是防止主动攻击的重要措施。认证就是识别和证实,即识别一个实体的身份和证实该实体身份的真实性。身份认证是授权控制的基础,它必须是无二义性地将对方识别出来,同时还应提供双向认证。

对于单机状态下的身份认证一般有用户口令、一次性密码和生理特征等方法。而网络环境下的身份认证要采用高强度的密码技术,一般为对称密钥加密或公开密钥加密的方法。

(2)访问控制

访问控制(access control)是确定不同用户对信息资源的访问权限,也是针对越权使用资源的防御措施。

(3)数据保密性

数据保密性(data confidentiality)的安全服务是针对信息泄漏的防御措施,使系统只对授权的用户提供信息,对于未被授权的使用者,这些信息是不可获得或不可理解的。

(4)数据完整性

数据完整性(data integrity)的安全服务是针对非法地篡改信息、文件和业务流而设置的防范措施,以保证资源的可获得性。

(5)不可否认性

不可否认性(non-reputation)的安全服务是针对对方进行抵赖的防范措施,可用于证实发生过的操作。一般有发送防抵赖、递交防抵赖和公证。

1.1.2　安全机制

安全机制(security mechanisms)分为实现安全服务和对安全系统的管理2种类型。ISO 7498—2 建议的安全机制有:

(1)加密机制

加密机制(encipherment mechanisms)用于加密数据或流通中的信息。它可以单独使用,也可以同其他机制结合使用。具体到加密手段,一般有软件加密和硬件加密。软件加密成本低且实用灵活,更换方便;而硬件加密效率高且本身安全性高。

(2)数字签名机制

数字签名机制(digital signature mechanisms)是由对信息进行签字和对已签字的信息进行证实这样 2 个过程组成。它必须保证签字只能由签字者的私有信息产生。

(3)访问控制机制

访问控制机制(access control mechanisms)是根据实体的身份及其有关信息来决定该实体的访问权限。一般采用访问控制信息库、认证信息(口令等)和安全标签等技术。

(4)数据完整性机制

数据完整性机制(data integrity mechanisms)能保证在通信中,发送方根据要发送的信息产生一条额外的信息(如校验码),并将其加密后随信息本体一同发出;收方接收到信息本体以后,产生相应的额外信息,并与接收到的额外信息进行比较,以判断在通信过程中信息本体是否被篡改过。

(5)认证机制

认证机制(authentication mechanisms)可通过认证信息(如口令、指纹等)实现同级之间的认证。

(6)通信业务填充机制

通信业务填充机制(traffic padding mechanisms)通过填充冗余的业务流来防止攻击者进行业务流量分析。填充过的信息要加密保护方才有效。

(7)路由控制机制

路由控制机制(routing control mechanisms)可预先安排网络中的路由或对其动态地进行选择,以使用安全的子网和链路。

(8)公证机制

公证机制(notarization mechanisms)是由第三方参与的签名机制,是基于通信双方对第三方的绝对信任,让公证方备有适用的数字签名、加密或完整性机制等。公证方可以利用公证机制对实体间的通信进行实时的或非实时的公证,可防止伪造签字和抵赖等。

1.2 网络安全体系及评估标准

一个网络的整体由网络硬件、网络操作系统和应用程序构成。而若要实现网络的整体安全,还需要考虑数据的安全性问题。此外,无论是网络本身还是操作系统和应用程序,最终都是由人来操作和使用的,这样一个重要的安全问题就是用户的安全性。因此,在考虑网络安全问题的过程中,应主要对网络安全、操作系统安全、用户安全、应用程序安全以及数据安全这5个方面进行分析。

1983年美国国家计算机安全中心(NCSC)发布的“桔皮书”,即“可信计算机系统评估标准”(trusted computer system evaluation criteria,简称TCSEC),规定了安全计算机系统的基本准则和评估标准。

1.2.1 网络安全5层体系

从体系上看,网络安全问题可分为5个层次,即操作系统层、用户层、应用层、网络层和数据链路层,如图1.1所示。

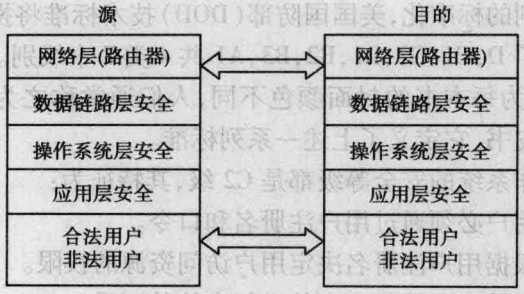


图 1.1　网络系统安全体系

(1)用户层安全

对于用户的安全性问题,主要考虑的是使用系统中资源和数据的用户是否是真正被授权的用户。一般是对用户进行分组管理,即根据不同的安全级别将用户分为若干等级。如 Windows 网络操作系统中的用户(user)、组(groups)和管理员(administrator),其每一等级的用户只能访问与其等级相对应的系统资源和数据。用户层安全包括保护合法用户的安全权限及限制非法用户的不安全进入途径,它主要涉及对用户的识别、认证和数字签名等问题。

由于网络的目的是便于资源访问,而网络的安全又与用户密切相关,因而人们通常关心如何保护网络资源,以确保非法用户不能访问它们。所以,商用网络操作系统都提供了一些安全系统来限制对共享文件、打印机等资源及系统本身的访问。

(2)应用层安全

应用层安全是指合法的用户对特定数据进行合法的操作。应用层安全与应用系统直接相关,即包括不同用户的访问权限设置和用户认证、数据加密的完整性确认以及对不良信息的过滤等。

(3)操作系统层安全

操作系统的安全问题主要是用户口令的设置与保护以及同一 LAN 或 VLAN 内的共享文件和数据库的访问控制权限的设置等。无论是服务还是客户机,目前常用的操作系统主要是 UNIX 系列和 Windows 系列。由于用户的应用系统都在操作系统上运行,因而大部分的安全工具或软件也都在操作系统上运行,因此,操作系统的安全性直接影响网络安全。

为了安全级别的标准化，美国国防部(DOD)技术标准将操作系统的安全等级由低到高分成了 D，C1，C2，B1，B2，B3，A1 共 4 类 7 个级别。这些标准发表在一系列的书上，因为每本书的封面颜色不同，人们通常称之为“彩虹系列”。其中最重要的是桔皮书，它定义了上述一系列标准。

目前主要操作系统的安全等级都是 C2 级，其特征为：

①系统识别用户必须通过用户注册名和口令。

②系统可以根据用户注册名决定用户访问资源的权限。

③系统可以对其发生的每一事件进行审核并记录。

④可以创建其他具有系统管理权限的用户。

(4)数据链路层安全

数据链路层的安全主要涉及传输过程中的数据加密及数据完整性问题。此外，还涉及物理地址盗用的问题。解决的方法有：

①加强内部管理人员的法律意识。

②采用防火墙技术。

③对数据和 IP 地址进行加密后传输。

④使用用户认证和数据签名技术。

(5)网络层安全

网络层安全问题的核心是网络是否能得到控制，这也是网络安全中最重要的部分。它涉及 3 个方面：

①IP 协议本身的安全性。

②网络管理协议的安全性。

③交换设备的安全性。

1.2.2 网络安全评估标准

许多政府与组织通常不会与未经第三方标准证实其安全性的另一方进行交流，也就是说安全性往往是一个局部的概念。对于不同的生产商、组织、国家政府彼此具有不同的安全措施与标准体系。近些年来，人们试图建立一个全球性的 ISO 安全档案。下面的标准档案并不专门针对 UNIX 或 Windows NT，旨在为不同类型的网络提供一个框架。

(1)欧洲信息技术安全评估标准(ITSEC)

在欧洲,ITSEC BS 7799 列出了网络威胁的种类以及各种可以降低攻击的危害的方法。要了解关于 ITSEC 的更多情况,请访问 www. itsec. gov. uk。BS 7799 档案于 1999 年重写,增加了以下内容:

①审计过程。

②对文件系统审计。

③评估风险。

④保持对病毒的控制。

⑤正确处理日常事务及安全保护的 IT 信息。

(2)可信计算机系统评估标准(TCSEC)

在美国,NCSC 负责制定关于可信的计算机产品的安全标准。NCSC 创立了 TCSEC 与 DOD Standard 5200. 28, 用于建立信任级别。TCSEC 用于标明一个系统的安全特性和安全防护能力。

在 TCSEC 中,系统安全程度分为 4 类,每类又分为若干等级,如 D,A1,B1,B2,B3,C1,C2,数字越大,表示的安全性越好。D 级系统的安全程度最低,通常为无密码保护的个人计算机系统。A 级别最高,用于军队计算机。具体描述如下:

1)D 级为安全保护欠缺级

凡经检测安全性能达不到 C1 级的均划归为 D 级。

2)C1 级为自主安全保护级

实施机制允许命名用户和用户组的身份规定并控制资源共享,防止非授权用户读取敏感信息。该级别提供基本的访问控制。

3)C2 级为受控存取保护级

与 C1 级相比,计算机处理系统安全保护策略的机制实施了粒度更细的自主访问控制。系统级的保护主要在资源、数据、文件和操作上。通过登录规程,系统不仅要识别用户还要考虑其惟一性,并通过审计安全性相关事件以及隔离资源,使用户能对自己的行为负责。Windows NT 属于 C2 级系统。

4)B1 级为标记安全保护级

B1 级除具有 C2 级的所有功能外,系统还提供更多的保护措施。UNIX 的 MLS 及 IBM 的 MVS/ESA 属于 B1 级系统。

5)B2 级为结构化保护级