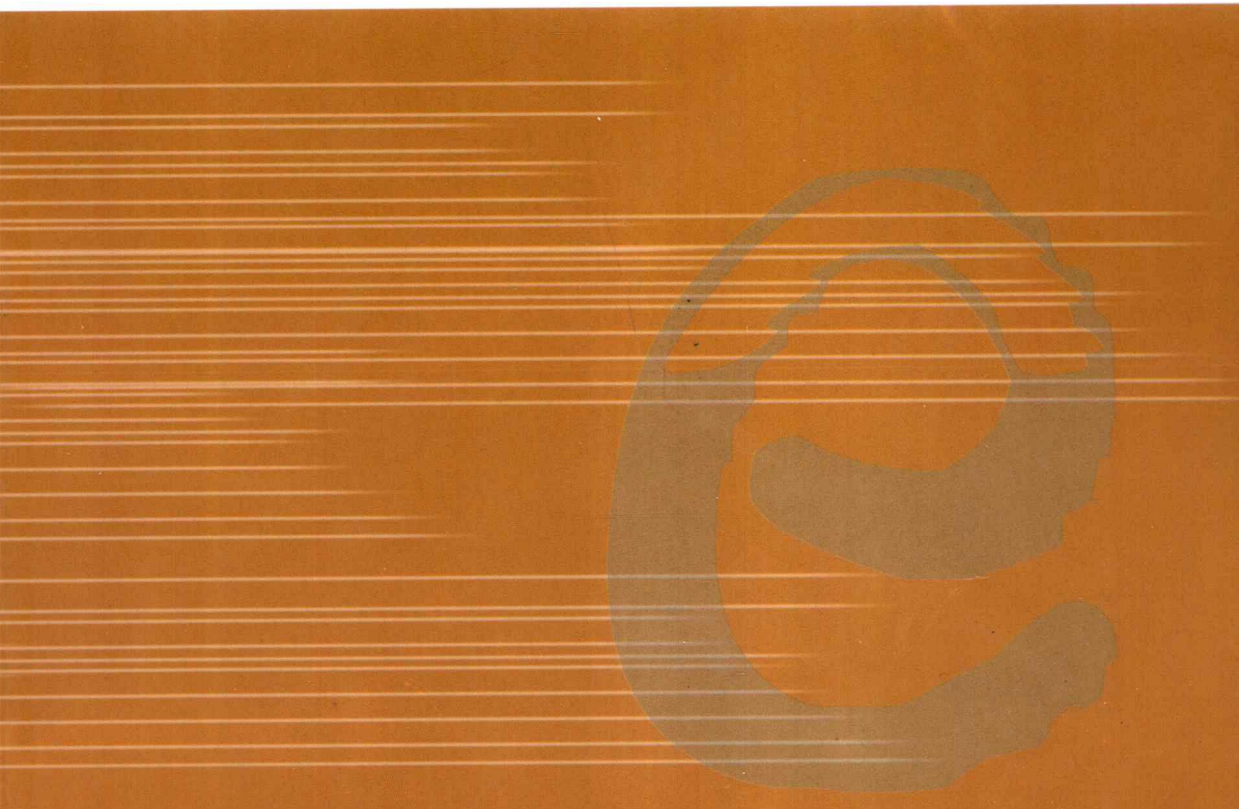
教育部职业教育与成人教育司推荐教材

高等职业教育电子商务专业新编系列教材

网络信息安全

主编 陈月波



武汉理工大学出版社
WUTP Wuhan University of Technology Press

教育部职业教育与成人教育司推荐教材
高等职业教育电子商务专业新编系列教材

网络信息安全

主　编：陈月波
副主编：李华霖　李京川

武汉理工大学出版社
武汉

内 容 提 要

全书分为9章，介绍了网络信息安全概述，网络安全技术，信息加密技术，数字签名与CA认证技术，防火墙技术，Internet安全技术，网络信息安全协议与安全标准，网络信息安全防范策略，最后介绍了网络信息安全法律等。该书遵从高职高专教学规律，从网络信息安全基础出发，重点介绍了信息加密技术、数字签名与CA认证技术、防火墙技术、Internet安全技术，同时每章配有针对性的实验，具有较强的可操作性。

本书可以用作本科以及高职高专信息安全、计算机、电子商务等相关专业的教材，同样适合广大计算机网络与信息安全爱好者阅读参考。

图书在版编目(CIP)数据

网络信息安全/陈月波主编. —武汉：武汉理工大学出版社，2005
教育部职业教育与成人教育司推荐教材
高等职业教育电子商务专业新编系列教材
ISBN 7-5629-2203-9

Ⅰ.网… Ⅱ.陈… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2005)第006520号

出版发行：武汉理工大学出版社(武汉市洪山区珞狮路122号 邮编430070)
http://www.techbook.com.cn 理工图书网
E-mail:duanchao@mail.whut.edu.cn
经 销 者：各地新华书店
印 刷 者：武汉理工大印刷厂
开 本：787×960 1/16
印 张：24
字 数：455
版 次：2005年1月第1版
印 次：2005年1月第1次印刷
印 数：1—5000册
定 价：33.00元

出版说明

国家“十五”规划中明确指出：“通过电子商务特别是企业间电子商务的应用，推动营销、运输和服务方式的变革，降低成本，扩大工业品市场规模。”为了实现我国“以信息化带动工业化”的经济发展战略目标，加速发展电子商务正在成为我国谋求跨越式发展的重要选择之一。

为了满足国家经济发展与建设对电子商务专门人才的迫切需要，教育部根据教学规律已建立了一套科学、系统、操作性强的宏观培养体系规划。在高等职业教育方面，教育部已批准370多所高职院校开办电子商务专业。

为了能出版一套反映当前电子商务发展现状、适合我国高等职业教育特点并能体现教育部高职三年制向两年制转轨的精神，在中国电子商务协会高校工作委员会副主任宋文官教授、中国电子商务专业建设协作组及“EC管理”指导委员会主任王学东教授的大力支持下，我社组织了全国30余所高等职业技术院校及有关单位共60多位专家、学者编写了这套“高等职业教育电子商务专业新编系列教材”。

本套高等职业教育电子商务新编系列教材的编写具有以下特色：

■ 定位准确，服务高职教育

本系列教材明确提出就是为高等职业教育服务。在编写高职教材时，必须围绕高等职业教育是具有一定理论水平、有较强实际技能的职业性人才这个培养目标，改变过于重视知识的传授过于强调学科体系的严密、完整的做法，精选学生终身发展的基础知识和基本技能，充分体现社会需要、学科特点和学生身心发展三者有机的统一。

■ 可读性强，体例风格新颖

针对高职学生特点，我们设置了教学目的与要求、关键词汇、典型例题、典型案例、阅读材料、创新视点、案例分析、知识归纳、知识结构图表、技能达标、实训指南、习题与思考题等栏目。从栏目到版式上耳目一新。

■ 与时俱进，内容科学先进

我国电子商务经历了发展、停顿、高速发展的过程，电子商务高职教育也在不停地摸索中发展。我们希望通过本系列教材的推出，把最新的教改精神融入其中。力图打造一套知识内容最新、课程设置科学系统、紧跟电子商务发展的高职教材。

■ 应用性强，强调技能实训

将实习实训课纳入课程体系是高职教学模式的一大特色。本系列教材力争做到：实训教材、案例教材相配套；同一专业的基础课、专业基础课、专业主干课教材配套；同一门课程的基本教材、辅助教材、教学参考书成系列配套；同一门课程文字教材、电子教材同步配套。

在组织编写教材的过程中，《中华人民共和国电子签名法》已经于2004年颁布实施。2005年初国务院又制订了《关于加快电子商务发展的若干意见》。我国的电子商务已经步入正规化高速发展时期。

本套教材首批在2005年秋季出齐。根据学科发展，我们将不断增补。我们的编审者、出版者不敢稍有懈怠，一定高度重视，兢兢业业，按最高的质量标准工作。教材建设是我们共同的事业和追求，也是我们共同的责任和义务，我们诚恳地希望大家积极选用本套教材，并在使用过程中给我们多提意见和建议，以便我们不断修订、完善全套教材。

武汉理工大学出版社

2005年1月

高等职业教育电子商务专业
新编系列教材编审委员会

前　言

随着网络的开放性、共享性和互连程度的扩大，网络的重要性和对社会的影响也越来越大，同时网络上各种新业务的兴起，比如电子商务、电子现金、数字货币、网络银行、网上证券、网上理财以及网上保险等等，使得网络与信息系统的安全与保密问题显得越来越重要，成了关键之所在。进入21世纪以来，我国的网络信息安全形势更加严峻，研究和解决我国的网络信息安全问题刻不容缓。各个高校纷纷开设信息安全专业和有关课程，培养紧缺的信息安全专业人才。

本书针对当前高校开设的“网络信息安全”课程编写，可以用作本科以及高职高专信息安全、计算机和电子商务等相关专业的教材。本书的总参考学时数控制在72课时范围内。

全书共9章，第1章主要介绍了网络信息安全概述，内容包括网络与信息安全、网络信息安全及其体系结构、网络信息安全的基本要素、网络信息安全威胁、网络信息安全技术、信息安全模型及其主要评价准则；第2章介绍了网络安全技术，内容包括网络安全概述、网络操作系统安全、防火墙、虚拟专用网(VPN)技术、网络入侵检测；第3章介绍了信息加密技术，内容包括信息加密技术概述、密码技术、密钥管理、网络加密技术；第4章介绍了数字签名与CA认证技术，内容包括数字签名原理、种类与方法、数字证书、身份认证技术、数字证书的申请、PKI基础等；第5章介绍了防火墙技术，内容包括防火墙概述、防火墙的设计和实现、防火墙的安全体系结构、防火墙的组合变化、典型防火墙产品与防火墙技术发展；第6章介绍了Internet安全技术，内容包括Internet安全概述、FTP安全、E-Mail安全、Web安全、Proxy技术等；第7章介绍了网络信息安全协议与安全标准，内容包括安全协议概述、安全套接层协议SSL、安全电子支付、安全电子交易(SET)；第8章介绍了网络信息安全防范策略，内容包括信息安全策略、安全防范策略概述、网络信息安全防范体系、常见的网络攻击与防范、物理安全防范策略、访问权限控制、黑客攻击防范策略、灾难恢复；第9章介绍了网络信息安全法律，内容包括网络信息安全法律概述，主要有互联网引起的法律问题、网络犯罪的形式、网络犯罪的特点、我国网络信息安全立法状况等。

该书遵从实训教学规律，从网络信息安全基础出发，重点介绍了信息加密技术、数字签名与CA认证技术、防火墙技术和Internet安全技术，同时每章配有

针对性的实验，各章的实训内容，学校可以根据自己的实验室实际情况选做。

本书内容丰富，结构合理，同样适合广大计算机网络与信息安全爱好者和大专院校相关专业的师生阅读参考。

本书由陈月波老师主编并总撰全书，同时编写第1、8、9章、第4.5节和第6章的修改，李华霖老师编写第4、7章，吕侃徽老师编写第2章和第8.4节，李京川老师编写第3章，杨国震老师编写第5章，雷承达老师编写了第6章的部分内容。

在本书的编写过程中，得到了武汉理工大学出版社段超工作室的指导，并对本书的大纲提出了许多宝贵的意见，在此深表敬意！

本书还参考了许多有关的教材和互联网网址，大部分已经列出来，对于疏忽遗漏列出来的参考教材和网址，一并致谢并表歉意。

编 者

2004年12月

目　录

1 网络信息安全概述

教学目的和要求

本章主要介绍了信息安全、网络信息安全的概念，内容涉及网络信息安全威胁、安全的要素以及安全技术、安全工作目的等。通过本章的教学，要求学生掌握网络信息安全的有关概念，了解网络信息安全的体系结构、安全模型、安全技术与评价准则，深刻理解网络信息安全威胁，掌握网络信息安全要素的主要内容。

关键词汇

信息安全(Information Security)
网络信息安全(Network and Information Security)
实体安全(Physical Security)
运行安全(Operation Security)

在信息化时代的今天，信息化引发的网络信息安全问题，越来越受到广泛的关注和重视。因为网络信息安全不仅仅涉及到国家的经济、金融和社会的安全，也涉及到国防、政治和文化的安全，可以说，信息安全就是国家安全。

我们知道，企业的信息化促进了电子商务的蓬勃发展，同时，电子商务的发展也推动了企业的创新与结构调整，进而大大提高了企业的效率。但是，在发展的过程当中存在着严峻的安全问题，其中比较大的问题依然是信息安全问题。我们必须解决电子商务交易中信息的机密性、完整性、可用性和不可抵赖性等问题。可以说，信息安全是电子商务发展的基础和动力。

开放的、自由的和国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得他们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力。通过 Internet，可以从异地取回重要数据，但同时又要面对 Internet 开放带来的数据安全的新挑战和新危险。如何保护企业的机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要

考虑的重要事情之一。

进入21世纪以来，我国的网络信息安全形势更加严峻，研究和解决我国的网络信息安全问题刻不容缓。

本章就信息安全、网络与信息涵盖范围、安全威胁和安全技术等方面进行了深入浅出的介绍。

1.1 信息安全基本概念

1.1.1 信息安全

“安全”概念就是指“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施”。安全不是技术，安全是一个过程。

对于信息安全，国内有几种不同的回答。中国工程院权威人士认为，可以把信息安全保密内容分为实体安全、运行安全、数据安全和管理安全四个方面。很多教科书上认为计算机安全包括：实体安全、软件安全、运行安全和数据安全。而国家信息安全等级保护条例中认为，计算机信息人机系统安全的目标是着力于实体安全、运行安全、信息安全和人员安全维护。安全保护的直接对象是计算机信息系统，实现安全保护的关键因素是人。这种观点是从信息安全分层结构提出的，主要面向应用的信息安全框架，如图1.1所示。

对于信息安全的定义，国外也有几种类似的观点。有人认为，信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性和可用性。有人认为信息安全就是对信息的机密性、完整性、可用性的保护。也有人认为信息安全涉及到信息的保密性、完整性、可用性和可控性。综合起来说，就是要保障电子信息的有效性。这些观点都是从信息安全的属性角度提出的，参看信息安全的金三角框架，如图1.2所示。

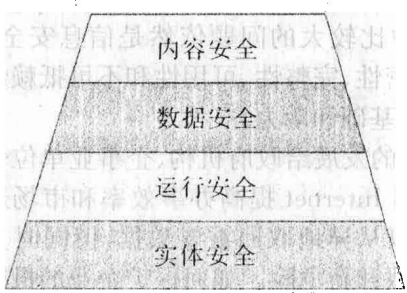


图1.1 信息安全分层结构

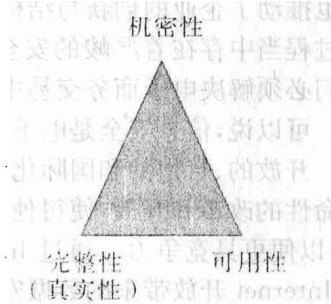


图1.2 金三角的信息安全框架

我们认为信息安全是指防止信息资源被故意的或偶然的非授权泄露、更改和破坏，或者信息被非法系统辨认、控制和否认。即确保信息的完整性、秘密性、可用性、可控性和不可否认性。

信息安全分层结构观点与信息安全的属性的观点，从不同的角度来分析，实际上其本质是统一的。

实体安全(物理安全)就是指保护计算机设备、设施(含网络)以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施和过程。它包括：(1)保证系统不以电磁等方式向外泄漏信息(保证信息的机密性)；(2)保证系统至少能够提供基本的服务(保证信息的可用性)。

运行安全就是为保障系统功能的安全实现，提供一套安全措施(如风险分析、审计跟踪、备份与恢复、应急等)来保护信息处理过程的安全。包括：(1)保证系统的机密性，使得系统任何时候不被非授权人所恶意利用(保证信息的可控性)；(2)保障网络的正常运行，确保系统时刻能为授权人提供基本服务(保证信息的可用性)。

数据安全就是指：(1)保证数据的发送源头不被伪造(保证信息的真实性)；(2)保证数据在传输、存储过程中不被获取并解析(保证信息的机密性)；(3)保证数据在传输、存储等过程中不被非法修改(保证信息的完整性)；(4)保证系统的可用性，使得发布者无法否认所发布的信息内容(保证信息的不可否认性)。

内容安全是要：(1)防止阻断信息传输系统，使得被传播的内容不能送达目的地(保证信息的可用性)；(2)防止删除局部内容，或附加特定内容(保证信息的完整性)；(3)防止对传递信息进行捕获并解析(保证信息的机密性)；(4)防止路由欺骗，域名欺骗(保证信息的真实性)。

信息安全涵盖范围如图 1.3 所示。信息安全分层结构与信息安全的属性之间的关系如表 1.1 所示。

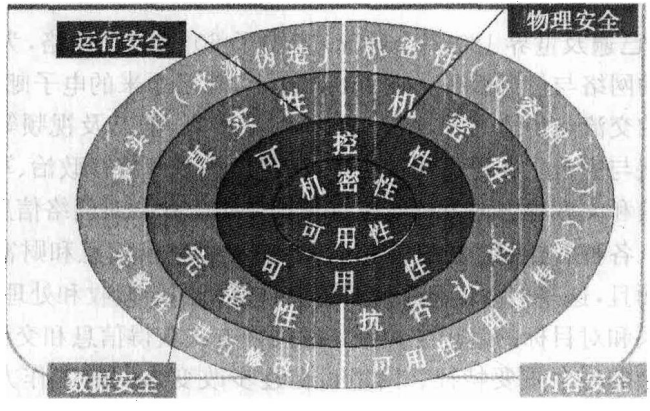


图 1.3 信息安全涵盖范围