电子·教育

高职高专计算机系列教材

中国计算机学会高职高专教育学会推荐出版

电子商务安全

冯矢勇 编著　　庄燕滨 主审

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

高职高专计算机系列教材

电子商务安全

冯矢勇　编著
庄燕滨　主审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

本书全面介绍了电子商务的安全隐患、安全技术的基础理论和实际的解决方案，内容包括：物理设备、因特网、客户机/服务器和电子商务中的种种不安全性；建立安全的电子商务流程概念、加密与密钥体系、如何实现数据完整性、数字签名、数字认证、安全协议与标准；物理设备和客户机/服务器的安全措施，防火墙的使用，对访问的认证和控制，S/MIME，SSL，SET 和数字认证的使用；如何进行安全的管理等。本书论述深入浅出，内容全面，每章附有习题，特别适合作为高职高专电子商务专业、计算机应用专业和营销专业的教材，也适合供大专院校学生和从事电子商务人士参考。

图书在版编目(CIP)数据

电子商务安全/冯矢勇编著 .—北京：电子工业出版社，2002.4
高职高专计算机系列教材
ISBN 7-5053-7387-0

Ⅰ.电… Ⅱ.冯… Ⅲ.电子商务—安全技术—高等学校：技术学校—教材 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2001)第 093360 号

责任编辑：吕 迈 张云怡
印 刷：北京大中印刷厂
出版发行：电子工业出版社 http://www.phei.com.cn
北京市海淀区万寿路 173 信箱 邮编 100036
经 销：各地新华书店
开 本：787×1 092 1/16 印张：14.25 字数：365 千字
版 次：2002 年 4 月第 1 版 2002 年 4 月第 1 次印刷
印 数：5 000 册 定价：18.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：(010)68279077

前　言

电子商务诞生在经济全球化时代，经济全球化需要一个与其相配合的运作平台，电子商务是最合适不过了。可以预见电子商务将是 Internet 上最重要的应用之一。高效率、高效益和低投入的电子商务将会征服全世界。尽管目前 Internet 和电子商务还处于“婴儿期”，但是许多国家的政府都把普及上网、发展电子商务作为近期的重要策略，我国政府有关部门也把电子商务作为经济发展新的增长点。

电子商务要飞速发展将面临好几个难点，其中安全问题无疑是重中之重。经过十几年的努力，目前已经有几个可在 Internet 网上从事安全交易的成熟技术，它们正被使用着，而另外一些新的安全方案正在加速研究。由于电子商务中信息所拥有的巨大价值，因此安全威胁是始终存在的；又由于电子商务技术的复杂性，它的安全问题并不为多数人理解。人人都要用 Internet 和接触电子商务，各商家都牵连着电子商务，因此，其安全知识必须普及成人人知道的常识，其安全技术必成为从事与电子商务有关人员所了解和掌握的知识。电子商务无疑将作为经济发展新的增长点，随之而来将出现一批与电子商务安全有关的新兴职业，例如：电子商务安全系统工程师，电子商务安全维护工程师，电子保安，电子商务法律专家，电子商务律师，电子商务司法人员，电子商务安全策划，电子商务法官，电子商务安全警察，电子商务安全员，……毫无疑问，电子商务安全将是普及率极高的知识和应用技术。

一、本书需要的基础知识

本书需要的基础知识是因特网的基本概念和电子商务的基本概念。虽然电子商务的安全技术涉及到很多新概念，但都是普通读者可以理解的。以许多安全技术的基础——双钥加密体制为例，只需要中学数学知识，加上本书附录中一点素数的知识就可以理解了。编者曾在课堂上讲完其理论后，许多学生立即可以解出例子中的加密和解密值。其他用到的数学知识是散列函数，也是不难理解的。本书也不涉及较深的网络理论。

二、适用范围

本书论述深入浅出，内容全面，每章附有习题，特别适合作高职高专电子商务专业、计算机应用专业和营销专业的教材，也可供大专院校学生参考。此外，对于已经从事电子商务的人士或者希望了解电子商务如何解决安全问题的广大读者，本书也可作为一本参考读物。

三、本书结构

本书共分三大篇：

第一篇是电子商务安全隐患篇，主要概述电子商务安全隐患，介绍物理设备、因特网、客户机/服务器和电子商务中的不安全性。

第二篇是电子商务安全基础篇，主要陈述电子商务安全解决方案中所需的基本理论和基本知识，包括电子商务安全基础，安全的电子商务流程，加密与密钥体系，数据完整性和安全的概念，数字鉴别知识，安全协议与标准。

第三篇是电子商务安全解决篇，主要陈述电子商务种种实际安全解决方案，具有可操作性。具体介绍了物理设备和客户机、服务器的安全措施，Internet 上的安全措施、安全协议，密钥管理，数字认证的应用以及如何进行安全的管理。

四、本书特点

一是较全面介绍了电子商务安全问题，使读者对电子商务安全有一个完整的概念。

二是既避免涉及复杂的网络理论，又较完整地介绍了基础知识，使读者对电子商务安全有一个深层次的理解。

三是实用性。第一篇和第二篇是为第三篇作准备的。在第三篇中，陈述的各种电子商务安全实际解决方案都具有实用性和可操作性。

四是对较复杂的概念配有图解，每章附有习题，便于教学。

本书由电子工业出版社组织编写，经江苏省许多大专和高职院校讨论而定。作者感谢江苏省大专和高职院校许多老师和同仁的支持；感谢苏涛、刘成荣、李峰等老师预读稿件并提出意见，感谢顾成喜编写 PGP 的安装和使用部分；作者还特别感谢常州工学院庄燕滨副教授审稿，提出不少切实有用的建议，使本书的质量得以提高，使作者受益匪浅。

本书涉及面较广，同时因为作者水平有限，错误之处在所难免，恳请读者的批评指正。有关意见请发电子邮件至 feng@ sz.js.cn。不胜感激。

作　者

目　录

电子商务安全隐患篇

火，大概是没有人发明的；电子商务，大概也是没有人发明的。它们都是人类活动的产物。

现在，人离开了火是难以生存的；不久的将来，人离开了电子商务也是难以生活的。

火的灾难天天能听得到，看得到；电子商务运行的网络事故也时有传闻。

引起火灾，太容易了，一烧是一堆，一烧是一片；网络病毒的攻击太容易了，一传是一批，一传是整个世界。

预防火灾、消灭火灾已经有许许多多的措施和办法，新的方法还在不断地发明；网络安全的防范、电子商务的安全措施也有许许多多，新的方案、新的技术、新的措施、新的法律、新的设施，也在不断出台。

如何预防火灾的隐患人们都知道：不要乱扔烟头，不要把火种带入危险区，……时常有宣传，经常有检查，但有的人我行我素，听不进任何警告，到头来追悔莫及。电子商务的安全隐患和对安全的防范知识知道的人很少很少，因为它是新事物，理解它有技术难度。今后知道的人必然会多起来，但即使知道了，防范起来也比预防火灾烦琐多了，是否有的人也是我行我素？

人类几千年的文明史中，构成国家和民族的安全要素是军队、武器、情报机构、警察、法院、监狱、……而机构、家庭和个人安全的防范措施是钥匙、防盗门、保安、密码箱、防弹衣、监视系统。这一系列防范措施的出现是因为人们已经掌握了对安全构成威胁的来源。在电子商务中也有一系列防范措施，不久的将来还会出台许多新的防范措施。要理解和使用这些电子商务的安全防范措施，也要了解威胁的来源。

在电子商务时代到来的时候，时时刻刻要把电子商务的安全威胁记在心中。

那么，电子商务安全要素是什么？我们要对电子商务提供些什么样的安全保障呢？

电子商务的安全要素一共有六项：机密性、完整性、认证性、不可否认性、不可拒绝性和访问控制性。所有的安全威胁都是针对这六项内容中的某一部分，所有的安全技术都是为了保证这六项内容。

本篇的各章阐明了破坏上述六项安全要素的各种安全威胁、安全隐患、人为错误和失误。

让我们看看：种种现代化的、先进的计算机网络物理设备上出现过的故障和事故，忘了这一点，一时的疏忽会带来巨大的经济损失。

让我们看看：攻击者、黑客能有那么多的途径入侵到电子商务系统。他们能侵犯网络服务器，可在网络上截获数据，许多机构遭受过网络安全侵害，受到过病毒的攻击。攻击者可以从 TCP/IP 协议、Web 站点、IP 地址、HTTP 或 TCP 连接入侵，还有伪装、欺骗、口令猜测、数据偷窃、利用工具、自编程序等数不清的手段达到攻击电子商务系统的目的。

再让我们看看：“人祸”。除了外部攻击者外，内部的“叛变”和“出卖”对安全的威胁更大。此外，人是很容易犯错误的：管理者的失职、操作人员精力不集中、缺乏经验、蓄意报复、蓄意破坏等等。他们的一点点小错误，对一个机构的破坏可能很严重。

电子商务时代可谓处处有安全漏洞，时时有安全隐患。

水火无情，但人离不开水和火。电子商务处处有漏洞、时时有隐患，但电子商务已经显露出的高利益性、高便利性、高效率性，使人不得不加速进入电子商务时代。

在我国，电子商务还刚刚起步。电子商务在因特网上实现了“物流、信息流、资金流”三者的统一，流动的是金钱和财富（信息）。金钱和财富刺激着有人去冒险，不管安全技术发展到何等完善的地步，对安全的威胁仍永远存在。

我们应时刻警惕着！