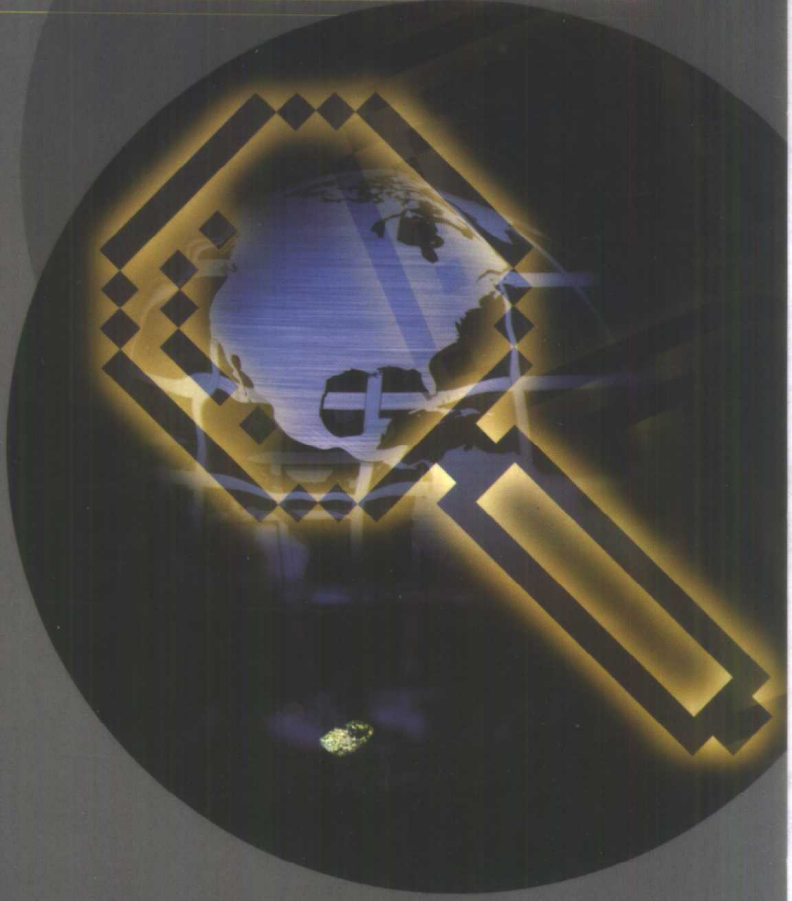
电子商务系列丛书
Electronic Business

电子商务安全

书缘工作室　编著

Electronic Business
Electronic Business
Electronic Business



人民邮电出版社
www.pptph.com.cn

电子商务系列丛书

电子商务安全

书缘工作室　　编著

人民邮电出版社

图书在版编目(CIP)数据

电子商务安全/书缘工作室编著 .—北京:人民邮电出版社 .2001.6
(电子商务系列丛书)
ISBN 7-115-09324-5

Ⅰ.电 ... Ⅱ.书 ... Ⅲ.电子商务-安全技术 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2001)第 027125 号

电子商务系列丛书

电 子 商 务 安 全

◆ 编　　著　书缘工作室
责任编辑　梁　凝

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ pptph.com.cn
网址　http://www.pptph.com.cn
读者热线　010-67129212　010-67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:787×1092　1/16
印张:11.75
字数:279 千字　　2001 年 6 月第 1 版
印数:1-5 000 册　　2001 年 6 月北京第 1 次印刷

ISBN 7-115-09324-5/TN·1722

定价:20.00 元

内容提要

本书从电子商务安全的现状出发，深入浅出地论述了电子商务安全的方方面面。主要内容包括：电子商务的安全范围、安全协议、安全技术、防火墙技术、支付安全、非法入侵的防范等，并例举了一些电子商务安全解决方案。

本书通俗易读，实用性强，可供企事业单位的管理人员及从事电子商务的工程技术人员学习参考。

丛书编委会

丛书前言

Internet 是 20 世纪人类最伟大的发明之一，它以无与伦比的优势描绘了一幅全球化的网络风景。Internet 带来的不仅是一场信息革命，更重要的是它引起了人类经济活动方式的深刻变革。电子商务的出现便是其中最为鲜明的一个例证。

随着世界经济的全球化、多极化、区域化和国际贸易自由化的发展，电子商务的影响已逐步渗透到社会经济的各个层面，对传统的企业组织形式、管理模式、经营方式、贸易活动和营销观念等多方面提出了强有力的挑战。电子货币的出现，虚拟银行的诞生，电子商务金融的发展等，使“金融经济”脱离实际商品交易而空前繁荣起来。这些变化充分反映了电子商务对社会经济的深刻影响，并预示着一种新的商业理念的诞生。

电子商务的应运而生及其快速增长，不仅意味着商机的无限增加，还意味着一种崭新的全球性电子商务经济时代的来临。随着上网人数及网上交易的急速增加，电子商务所形成的网上市场正在逐渐成为一个真正的全球性的“新兴市场”。任何企业要想不断扩大其市场影响，增加其市场份额，提高其盈利水平，保持其竞争优势，就必须加入电子商务行列。

在全球电子商务如火如荼、飞速发展的时代潮流面前，中国企业也不甘人后。中国企业从 1994 年开始涉足电子商务以来，已取得了喜人的成绩。今天，中国的证券交易网覆盖全国，有效地保证了中国证券市场的发展；中国的金融结算系统网遍及全国，大大提高了转汇效率，缩短了资金的周转时间；中国电子商务技术市场已经初具规模。可以预见，在未来的几年内，中国将会成为全球最大的电子信息市场。这也就更要求中国企业的决策者们未雨绸缪，及早对电子商务经济进行科学的探讨和深入的分析。

基于上述诸种原因，更为了配合中国电子商务的发展，我们推出了这套《电子商务系列丛书》，以期对电子商务活动进行多角度的、系统的分析、研究、探讨，并希望通过此套丛书能够为中国的电子商务事业贡献一点微薄之力。我们组织了各个领域特别是专门研究和从事电子商务的专家、教授、博士、硕士等共同努力合作，历时 11 个月，终于完成了这套丛书的编写工作。在此，对参加编写本套丛书的工作人员，表示衷心的感谢，并致以崇高的敬意！

本套丛书共 6 册，书名及主要编著者如下：

★《电子商务企业》，张政新、成璐等；

★《电子商务金融》，王明思、马桥等；

★《电子商务交易》，展鸿得、王诗章等；

★《电子商务技术》，吴小军　李林玲等；

★《电子商务安全》，弋　清、李万鲁等；

★《电子商务法律》，何帅领等。

本套丛书是一套比较深入地对电子商务各个领域进行研究的丛书，具有覆盖面广，应用技术新，内容叙述精练，实用性强，案例选择经典等特色。由于电子商务不仅是目前的时代潮流，而且是全球经济发展的新经济增长点，现在与未来都将是一个热点问题，因此，本套丛书在编

写的过程中难免会因电子商务的不断发展而出现一些缺点和漏洞，在此恳请并期待学术界权威人士及广大读者给予批评、指正。

对为了这套丛书的出版做出不懈努力的作者、同事、朋友再次表示深深的谢意。

书缘工作室

2001 年 3 月　于北京

前　言

无庸置疑，电子商务已成为业界的新秀，同时它也带来了商务活动的全新运作模式。商务运作的一系列过程都体现着参与商务活动的权力、责任、义务和利益。传统的商务运作模式经历了漫长的社会实践，在社会的意识、素质、道德、政策、法规、技术等各个层面，都已逐步完善，大体形成了适应的规范和支撑环境。然而，对于迅速发展的电子商务热潮，这一切却处于刚刚起步阶段，其发展和完善将是一个漫长的过程。如何确保网上采购、网上支付和资金调度等各种网上服务的安全实现，是电子商务运作中无法回避的事情，因此，电子商务的安全问题已成为阻碍电子商务发展的“瓶颈”。

电子商务的兴起对网上交易和信息安全提出了更高的要求。无论商家、银行还是个人，人们都想知道在网上与之交易和通信的人是谁(即所谓的身份认证)，担心信息在传输过程中被篡改(即信息的完整性)，还担心信息在传送途中被外人看到(即隐私性)。可见，如果电子商务的安全问题得不到很好的解决，电子商务的应用就不会顺利实施，电子商务也就发挥不了应有的效益。

因为我国电子商务的发展还处于初级阶段，在理论和技术上还需要进一步研究和探索，所以电子商务的安全问题也就显得更加突出，为此，我们编写了本书，使广大读者了解关于电子商务安全的知识。

本书从电子商务的安全现状出发，深入浅出地论述了电子商务的安全范围、安全协议、安全技术、防火墙技术、支付安全及安全解决方案等内容。不仅让读者了解到电子商务安全的广泛内容，更重要的是让读者清楚地看到解决电子商务安全问题的重要性和可行性。

由于作者水平有限，且编写时间紧迫，书中难免有不当之处，敬请广大读者及专业人士批评指正。

作者

2001 年 2 月

目　录

第 1 章　电子商务安全概述

随着 Internet 的迅速发展和广泛应用，其安全性已变得日益重要起来。当然，对于生存和依赖于 Internet 的电子商务，安全问题更是网上企业和消费者急待解决的头等大事。

电子商务已成为业界新热点，同时它也带来了商务活动的全新运作模式。商务运作的一系列过程都体现着参与商务行为各方的权力、责任、义务和利益。在传统的商务运作模式中，由于经历了漫长的社会实践，所以对上述种种方面，如在社会的意识、素质、道德、政策、法规、技术等各个层面，都已逐步完善，形成了大体适应的规范和支撑环境。然而，对于迅速发展的电子商务热潮，这一切却处于刚刚起步阶段，其发展和完善将是一个漫长的过程。而电子商务运作中的安全问题，已不可否认地成为阻碍电子商务发展的一个“瓶颈”。

在 Internet 环境中开展电子商务，客户、商家、银行等诸多参与者都会担心自己的利益是否能够真正得到保障。因此，各国政府、国际组织以及 IT 业界人士都在致力于安全问题的研究，期望逐步把网上的混沌世界变得有序、可信、安全。只有保证了电子商务的安全，才能够吸引更多的社会公众投身电子商务，应用电子商务，发展电子商务，才能使电子商务健康地生存，高速地发展。

1.1　电子商务的安全现状

运作在 Internet 上的电子商务，每天需要进行千百万次的安全交易，而 Internet 本身又是一个高度开放性的网络，这与电子商务所需要的保密性是矛盾的，而 Internet 又没有完整的网络安全体制。因此，基于 Internet 上的电子商务在安全上无疑会受到严重威胁，电子商务交易的安全性问题将是实现电子商务的关键。

在电子商务的发展过程中，各产业对网络的技术依赖达到空前的程度。军事、经济、社会、文化各方面都越来越依赖于网络。这种高度依赖性使社会变得十分“脆弱”，一旦计算机网络受到攻击不能正常运作时，整个社会就会陷入危机的泥沼，甚至比电影中描述的情节还要恐怖。因此，电子商务安全日益受到各国的高度重视。

随着经济信息化进程的加快，计算机网络上黑客的破坏活动也随之猖獗起来。黑客及黑客行为已对经济秩序、经济建设、国家信息安全构成严重威胁。“黑客”是 Hacker 的音译，原意是指有造诣的电脑程序设计者。现在则专指那些利用自己掌握的电脑系统，偷阅、篡改或窃取他人机密数据资料，甚至在网络上犯罪的人，或者是指利用通信软件，通过网络非法进入他人系统，截获或篡改他人计算机数据，危害信息安全的电脑入侵者或入侵行为。

“黑客”的袭击在计算机网络最发达国家尤为严重。在 Internet 上，黑客组织公开网址、信道，提供免费的黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍。因此普通人很容易

学到网络攻击方式。目前,国际黑客对各国计算机系统中高度敏感保密信息的攻击和窃取正在日益上升。例如,对美国国防部的攻击行动每年达25万次以上,并且在不断增长。

正是基于上述种种原因,无形中加大了依法惩治黑客犯罪行为的难度,给反黑客工作带来了相当大的困难。一方面科学家很难开发出对保障网络安全普遍有效的技术,另一方面又缺乏足以保证这些手段得到实施的社会环境。随着Internet的普及,电子商务安全问题已成为信息时代必须尽快加以解决的重大课题。统计显示,到1999年底,全球个人电脑总数已达4.4亿台,Internet使用者达2.59亿。据预测,到2005年全球Internet用户将达到7.65亿。此外,基于Internet的电子商务的迅速发展,预计到2002年,全球通过电子商务达成的贸易额将达5万亿美元。人们不难想像,黑客的攻击一旦得逞,小则使网络某项服务瘫痪,大则导致长时间内无法恢复的整个商务系统的瘫痪,造成不可估量的损失。

黑客攻击可分为三个层次:低层次威胁是局部的威胁,包括消遣性黑客、破坏公共财产者;中间层次是有组织的威胁,包括一些机构"黑客"、有组织的犯罪、工业间谍;最高层次是国家规模上的威胁,包括敌对的外国政府、恐怖主义组织发起的全面信息战。

目前我国发生的"黑客"事件,大多属于低层次的攻击。1999年4月26日的CIH病毒的爆发,就使我国4万多台电脑不能正常运行,大多数电脑的硬盘数据被毁。中国民航的20多台电脑也被感染,其中在1999年下半年的航班时刻表的数据被毁,使工作人员4个多月的辛苦付之东流。国内很多企业的数据都或多或少地被破坏,不能不说是一种遗憾。因此,电子商务安全应受到我国政府与企业的高度重视。

威胁来自多方面,包括建立模仿合法Web网址的欺骗行为,另外还包括模仿和更改截取的电子信息,以及非法侵入专用企业网数据库等。美国每年因电子商务安全问题所造成的经济损失达75亿美元,电子商务企业的电脑安全受到侵犯的比例从1997年的49%升到1999年的54%。1997年,美国出现了两次大的企业网站瘫痪事件。1999年,美国中情局也受到黑客的攻击。

著名的美国联机公司因人为操作和技术上的失误,使其600万用户陷入瘫痪10小时。另一家大公司网络联机通信服务公司的主干网出现重大故障,40万用户被迫中断联络40小时。电子商务网站停机和服务局部中断现象明显增多,所造成的影响面在扩大。《USA Today》曾援引一位分析家的话说:"对500多家企业、大学及政府机构的调查表明,86%都出现过不同程度的欺骗与盗窃案件以及病毒的发作,总损失达到1亿美元。"

电子商务系统在防不胜防的破坏性活动面前,有时会显得软弱无力,谁都无法预测将会受到什么样的挑战。信息安全漏洞难以堵塞,一方面是由于缺乏统一的信息安全标准、密码算法和协议在安全与效率之间难以两全;另一方面,则是由于大多数管理者对网络安全不甚了解。另外,信息犯罪属跨国界的高技术犯罪,要用现有的法律来有效地防范十分困难,现有的科技手段也难以侦察到计算机恐怖分子的行踪,罪犯只需要一台计算机、一条电话线、一个调制解调器就能远距离作案。

同传统的金融管理方式相比,电子商务金融使资金流动在计算机网络里实现流通。于是,电子商务金融系统成了犯罪活动的新目标。

我国电子商务金融系统发生的计算机犯罪也呈上升趋势。近年来最大一起犯罪案件造成的经济损失高达人民币2100万元。目前,我国已发生了180多起利用计算机网络进行电子商务金融犯罪的案件。对我国电子商务金融系统安全现状,专家们有一些形象的比喻:使用不加

锁的储柜存放资金(电子商务企业缺乏安全防护);使用"公共汽车"运送钞票(电子支付系统缺乏安全保障);使用"邮寄托寄"的方式传送资金(转帐支付缺乏安全渠道);使用"商店柜台"方式存取资金(授权缺乏安全措施);使用"平信"邮寄机密信息(敏感信息缺乏保密措施)。在银行计算机犯罪案件中,具有破坏性的犯罪类型是篡改数据,而各银行对数据的保护、操作密码保护和储户密码保护都缺乏有力的措施。

与发达国家相比,发展中国家的电子商务安全更显得脆弱不堪。其原因是多方面的,发展中国家的许多部门只着重电子商务的应用带来的巨大财富,没有意识到电子商务安全的漏洞,忽视电子商务支付系统的安全技术防范,给基础安全埋下了隐患。与此同时,电子商务安全保卫工作严重滞后,不少单位还停滞在传统的"看家护院"的工作模式,行之乏效,没有从管理制度、人员和技术上建立相应的电子化业务安全防范机制。

在电子商务交易中,商家、客户和银行等各参与方是通过开放的 Internet 连接在一起的,相互之间的信息传递也要通过 Internet 来进行,这一变化使得交易的风险性和不确定性加大,从而对网络传输过程中数据的安全和保密提出了更高的要求,尤其对于电子商务支付中涉及到的敏感数据,则更需确保其万无一失。

电子商务的安全性是由计算机的安全性,特别是计算机网络的安全性发展而来的。安全问题是电子商务系统所要解决的核心问题。电子商务对网络及应用系统提出了许多安全要求,只有建立起科学、合理的安全体系结构,才能保证电子商务交易的安全实施。

1.2　电子商务所面临的安全威胁

Internet 为人类交换信息,促进科学、技术、文化、教育、生产的发展,提高现代人的生活质量提供了极大的便利,但同时对国家、企业和个人的信息安全也带来极大的威胁。由于网络的全球性、开放性、无缝连通性、共享性、动态性发展,使得任何人都可以自由地接入 Internet,自由地进行商务活动,其中有善者,也有恶者。恶者(黑客)会采用各种攻击手段进行破坏活动。他们对电子商务系统的主要威胁有:

(1)系统穿透:未授权人通过一定手段对认证性(真实性 Authenticity)进行攻击,假冒合法用户接入企业内部系统,实现对文件进行篡改、窃取机密信息、非法使用资源等。一般采取伪装(Masquerade)或利用系统的薄弱环节(如绕过检测控制)、收集情报(如口令)等方式实现。

(2)违反授权原则:一个授权进入系统做某件事的用户,他在系统中进行未经授权的其他事情。表面看来这是系统内部的误用或滥用问题,但这种威胁与外部穿透有关联。一个攻击者可以通过猜测口令接入一个非特许用户账号,进而可揭示系统的薄弱环节,取得特许接入系统权,从而严重危及系统的安全。

(3)植入:一般在系统穿透或违反授权攻击成功后,入侵者常要在系统中植入一种能力,为以后攻击提供方便条件。如向系统中注入病毒、蛀虫、特洛尹木马、陷门、逻辑炸弹等来破坏系统正常工作。特洛尹木马为攻击者服务,例如一种表面上合法的文字处理软件能将所有编辑文档复制存入一个隐蔽的文件中,供攻击者检索。

(4)通信监视:这是一种在通信过程中从信道进行搭线窃听(Interception)的方式。通过搭线和电磁泄漏等对机密性进行攻击,造成泄密,或对业务流量进行分析,获取有用情报。侦察

卫星、监视卫星、预警卫星、间谍飞机、预警飞机、装有大型综合孔径雷达的高空气球、无数微型传感器都可用于截获和跟踪信息。

(5)通信窜扰:攻击者对通信数据或通信过程进行干预,对完整性进行攻击,篡改系统中数据的内容,修正消息次序、时间(延时或重放),注入伪造消息。

(6)中断:对可用性进行攻击,破坏系统中的硬件、硬盘、线路、文件系统等,使系统不能正常工作,破坏信息和网络资源。高能量电磁脉冲发射设备可以摧毁附近建筑物中的电子器件,正在研究中的电子生物可以吞噬电子器件。

(7)拒绝服务:指合法接入信息、业务或其他资源受阻,例如一个业务口被精心地策划进行滥用而使其他用户不能正常接入,又如 Internet 的一个地址被大量信息垃圾阻塞等。

(8)否认:一个实体进行某种通信或交易活动,稍后否认曾进行过这一活动,不管这种行为是有意的还是无意的,一旦出现再要解决双方的争执就不太容易了。

因此,在 Internet 上发展电子商务的一个首要问题是解决 Internet 商务的安全性和可靠性。任何成功的电子商务系统必须能提供足够高的安全性、可靠性和可用性,才能赢得客户的信赖和欢迎。Web 将提供可用性,而安全技术和设施将解决安全可靠性,确保电子商务中商家和客户的隐私、产权和钱财的安全。

安全技术中的主要分支有通信安全和计算机安全。通信安全对从一个系统传送到另一个系统的信息进行保护。计算机安全对计算机系统中的信息进行保护,其中包括操作系统软件和数据库管理软件的安全特性。衡量这两大类的安全性常常要考察下述几个方面:

(1)物理安全:门锁、门卫以及其他接入控制,敏感设备的防患能力等。

(2)人事安全:雇员的素质,敏感岗位的身份识别,安全培训,安全检查等。

(3)管理安全:海外软件进口控制,入侵检测,安全审计追踪和责任分工评估。

(4)媒体安全:如标记控制、敏感的存储信息复制控制和含敏感信息的磁媒质、光盘片的销毁等。

(5)安全策略:它是针对特定安全区制订的与安全有关的规定。

适当设置防护措施可以减低或防止来自现实的威胁。在通信安全、计算机安全、物理安全、人事安全、管理安全和媒体安全方面均可采取一定的措施,整个系统的安全取决于系统中最薄弱环节的安全水平,这需要从系统设计上进行考虑,折中选取。在通信安全和计算机安全中的防护措施被看做是安全业务(Security Services),在面向人的意义上,系统所能提供的安全业务有下述几类:

(1)保密业务:保护信息不被泄露或披露给未经授权的人或组织。保密性可用加密和信息隐匿技术实现。

(2)认证业务:保证身份的精确性,分辨参与者所声称身份的真伪,防止伪装攻击。认证性可用数字签字和身份认证技术实现。

(3)接入控制业务:保护系统资源(信息、计算机和通信资源)不被未经授权人或以未授权方式接入、使用、披露、修改、毁坏和发出指令等。接入控制是对认证的强化。

(4)数据完整性业务:保护数据不被未授权者建立、嵌入、删除、篡改、重放。可用数据杂凑等技术实现。

(5)不可否认业务:主要用于保护通信用户对付来自其他合法用户的威胁,如发送用户对他所发消息的否认、接收用户对他已收消息的否认等,而不是对付来自未知的攻击者。可采用

仲裁签名、不可否认签名等技术实现。一般，不可否认性不能制止某合法用户对某业务的否认，但可以提供足够充分的证据迅速地辨别出谁是谁非。

不可否认业务不仅是为了解决通信双方相互之间可能的欺诈，而且也反映了现实系统的不完善性，现实环境中，当一个事件结束时，双方常会持不同的看法。特别是对商务中起关键作用的纸面文件，如合同、报价、标书、定货单、发票、支票等，在处理过程中常会出现问题，如票据丢失、损坏、被涂改、签章不全或不符、持票人身份不符、时间戳不符、票据伪造等。为了解决这类问题常采用各类手段，如签字、拒台签字、仲裁签字、收据、邮戳、挂号邮件等。一个好的商务系统都采用适当的票据来解决可能出现的争执。必要时可提供足够的证据，有时需要第三者(如邮局、代理人、仲裁等)协助。类似地，在电子商务系统中也需要不可否认业务，而且解决起来比传统商务更为困难，需要采用新的技术，如数字签字等。

(6)匿名性业务：隐匿参与者的身份，保护个人或组织的隐私。可用盲签名和信息隐匿技术实现。

可靠性和安全性是相互关联的。可靠性用以保证系统的可用性，即保证授权用户正常访问信息和资源不被拒绝。电子商务系统的可靠性不高就不能保证服务质量。可靠性可能要求安全性来提供保密性、认证性、完整性、匿名性和不可否认性。可靠性不等于安全性，服务器上的可靠协议对攻击者和授权用户都能提供可靠的服务。

匿名性和安全保密性是彼此不同但又相互关联的特殊性。保密性意味信息的主人可以控制信息，安全性要完全控制信息。匿名意味找不到信息的主人，即身份与信息不关联，匿名保证个人隐私(匿名货币可能带来一些风险，如传送匿名恐吓信和接受有关赎金、匿名敲诈、逃税等)。不可否认性主要是防止其他合法用户对所进行的操作的欺诈和抵赖。

换一种方式，我们从信任的角度来看一下电子商务所面临的安全威胁。

传统的买卖双方是面对面的，很容易保证交易过程的安全性，建立起信任关系。但在电子商务过程中，买卖双方通过网络来联系，受到距离的限制，因而产生安全感和建立信任关系相当困难。电子商务交易双方(销售者和消费者)都面临安全威胁。

(1)卖方面临的安全威胁

①系统中心安全性被破坏：入侵者假冒成合法用户来改变用户数据(如商品送达地址)、解除用户订单或生成虚假订单。

②竞争者的威胁：恶意竞争者以他人的名义来订购办公商品而了解有关商品的递送状况和货物的库存情况。

③商业机密的安全：客户资料被竞争者获悉。

④假冒的威胁：不诚实的人建立与销售者服务器名字相同的另一个 WWW 服务器来假冒销售者；虚假订单；获取他人的机密数据，比如，某人想要了解另一人在销售商处的信誉时，以另一个的名字向销售商订购昂贵的商品，然后观察销售商的反应。假如销售商认可该订单，说明被观察者的信誉高；否则，说明被观察者的信誉不高。

⑤信用的威胁：买方提交订单后不付款。

(2)买方面临的安全威胁

①虚假订单：一个假冒者可能会打着客户的名字来订购商品，并有可能收到货，而此时此刻真正的客户却被要求付款或返还商品。

②付款后不能收到商品：在要求客户付款后，销售商中的内部人员不将订单和钱转发给执