EB

电子商务专业系列教材

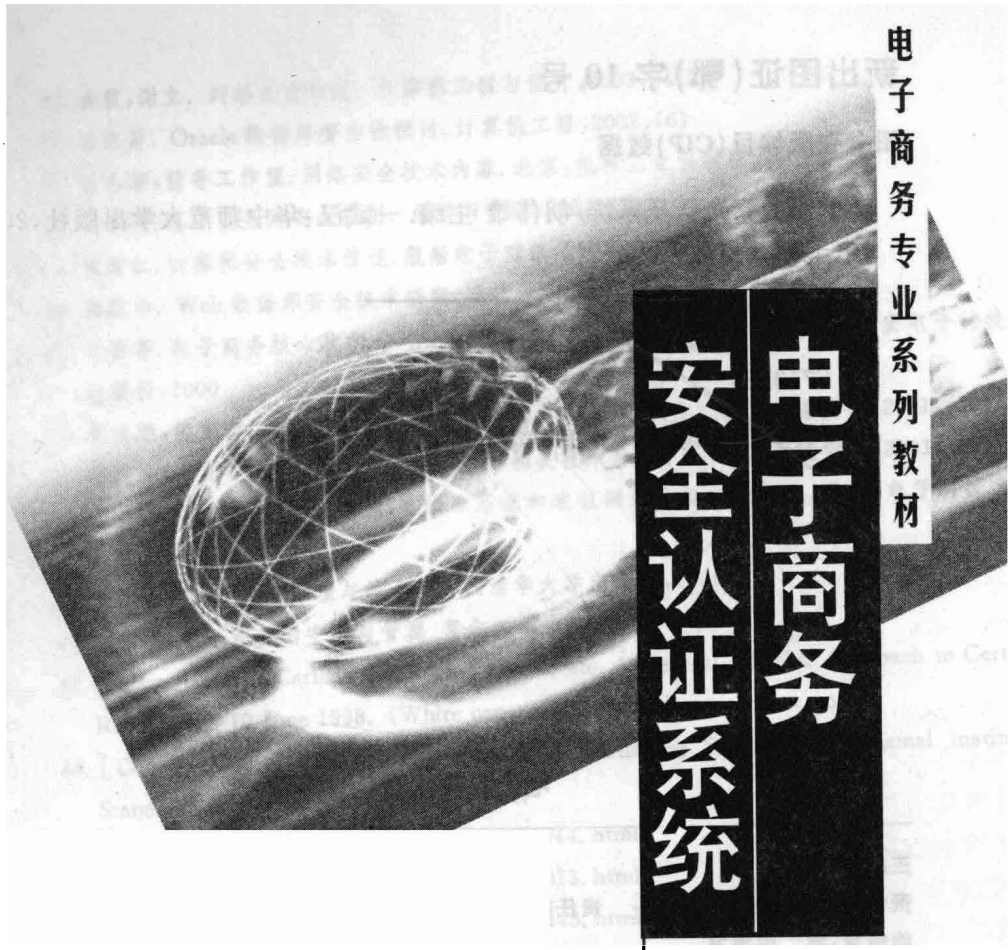
电子商务安全认证系统

胡伟雄　主编

华中师范大学出版社

电子商务专业系列教材

电子商务安全认证系统



主编 胡伟雄

参编 张园园 李伟 洪慧平 杨鹏

华中师范大学出版社

新出图证(鄂)字 10 号

图书在版编目(CIP)数据

电子商务安全认证系统/胡伟雄 主编. —武汉:华中师范大学出版社,2005.9
(电子商务专业系列教材)
ISBN 7-5622-3253-9/F·151
Ⅰ.电… Ⅱ.胡… Ⅲ.电子商务—安全技术
Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2005)第 108240 号

电子商务安全认证系统

主编:胡伟雄
责任编辑:苏春艳　　责任校对:罗少琳　　封面设计:新视点
编辑室:第二编辑室　　电话:027—67867362
出版发行:华中师范大学出版社 ©
社址:湖北省武汉市珞喻路 152 号
电话:027—67863040(发行部)　　027—67861321(邮购)
传真:027—67863291
网址:http://www.ccnup.com.cn　　电子信箱:hscbs@public.wh.hb.cn
经销:新华书店湖北发行所
印刷:石首市印刷厂印刷　　督印:姜勇华
字数:400 千字
开本:787mm×960mm　1/16　　印张:22
版次:2005 年 9 月第 1 版　　印次:2005 年 9 月第 1 次印刷
印数:1—4000　　定价:33.00 元
欢迎上网查询、购书

电子商务专业系列教材

编委会

（以姓氏笔画为序）

前　言

当迎来21世纪第一个春天之际，我国教育部批准在对外经济贸易大学、西安交通大学、华中师范大学等13所高校试办电子商务本科专业，这是适应经济全球化和我国加入世贸组织需要，加快培养高素质电子商务人才的重要举措。为了迎接新世纪的挑战，华中师范大学信息管理系于1998年开始筹办电子商务专业。1999年开始招收电子商务高等职业技术教育专科生，2000年设立电子商务本科(方向)，2001年正式设立电子商务本科专业，并招收电子商务双学位学生及电子商务硕士生(方向)。在师资队伍建设、课程建设、实验室建设等方面积累了一定的经验。

为了适应教学的需要，我们组织编写了这套电子商务专业系列教材，旨在为学科建设和人才培养作出应有的努力。

我们认为，电子商务专业教育是一种建立在信息管理学、经济学、计算机科学及通讯技术、网络技术等学科基础之上的综合性应用学科教育。在考察国内外电子商务专业教育现状及电子商务活动的本质内涵的基础上，此套系列教材以电子商务活动中的信息流、物流、资金流互动为主线，集合信息资源管理、经济学、管理学、计算机技术、通讯技术、网络技术等学科知识单元，组成三大模块的核心课程教材体系——反映电子商务活动基础的《电子商务概论》、《电子商务物流》、《网络营销》、《电子商务安全认证系统》、《网上支付与电子银行》、《电子商务政策法规导论》等教材；反映电子商务技术基础的《电子商务网络建设》、《电子商务数据库》、《Web站点设计与管理》等教材；反映电子商务活动应用领域的《CI与电子广告》、《电子证券与投资分析》、《电子出版与网上发行》等教材。

此套系列教材的编写立足于新，即反映电子商务的新理念、新知识、新技术；规范于质，即反映电子商务活动的信息流、物流、资金流的运动机理；重在于用，即反映电子商务的应用与操作技能知识。因此，此套系列教材特别适用于各类学校电子商务专业及电子商务从业人员、研究人员、管理人员的教学与培训。

编委会

2001年9月

目　录

第一章 概 论

随着 Internet 的快速发展和普及，它所面临的各种安全问题也成了人们关注的热点。信息安全已成为关系到国家、企业安全的重大问题。一方面，通过计算机安全模块所构筑的信息安全屏障逐渐增多；另一方面，计算机犯罪越来越猖獗，计算机犯罪所使用的技术手段也越来越高明。在国际上有关非法侵入计算机网络的事件层出不穷，给各国的政治、经济造成极大的损失。

在 Internet 上开展电子商务的一个首要问题是解决商务过程中各环节的安全性和可靠性问题。任何电子商务系统必须提供高度的安全性、可靠性和可用性，才能赢得客户和商家的信赖。

1.1 安全性概念

在 ISO 安全框架文件中，“安全”被解释为“一种使资产和资源遭受攻击的可能性减少到最小的方法”。可见，安全是相对的，并没有绝对安全的网络实体。

电子商务建立在因特网之上，电子商务安全的基础是因特网安全，它与密码安全、计算机安全、网络安全、信息安全等是密不可分的。因此，为了理解本书所述的各种安全性的含义，有必要先了解上述术语的定义。

1.1.1 密码安全

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安全保护。密码安全是通信安全最核心的部分，通过在技术上提供强有力的加密保护及其正确的应用来实现。

信息安全问题是国家信息化建设的关键问题，对信息安全问题的重视和解决程序，将直接制约信息化发展的进程。信息安全所要求的信息机密性、有效性、完整性和可用性，可以通过数据加密、完整性检验、身份认证和访问控制等技术来实现。这些技术的核心是密码技术。

密码具有特殊性，密码安全关系到国家的安全和利益。密码同时又是一种技术手段，是为保护国家利益和市场经济领域中的各种商业活动服务的。我国对密码采取既大力发展又严格管理的基本政策，实行“统一领导、集中管理、定点研制、专控经营、满足使用”的发展和管理方针。全国用于金融商业的密码由国家密码管理委员会统一分配，国家密码管理委员会办公室具体管理。研究、生产和经销密码

须经国家密码主管部门批准。未经批准，任何部门和单位不得研制、生产和经销密码。需要使用密码技术手段保护信息安全的部门和单位，必须按照国家密码管理规定，使用国家密码管理委员会指定研制、生产的密码，不得使用自行研究的密码，也不得使用从国外引进的密码。

1.1.2 计算机安全

计算机安全，又称为计算机系统安全。目前，对它的定义并不统一，常见的定义是：计算机系统的硬件、软件和数据受到保护，不因偶然的和恶意的原因而遭到破坏、更改和显露，系统连续正常运行。

“计算机安全”一词的含义首先是信息的机密性，机密性是指防止静态信息被非授权访问和动态信息被截取解密；其次是信息的完整性，完整性是指信息在存储或传输时不被非授权地修改、破坏，信息能保持一致性。另一个与计算机安全紧密相关的概念是拒绝服务。所谓拒绝服务，包括三个方面的含义：临时降低系统性能，系统崩溃而需人工重新启动，因数据永久性丢失而导致较大范围内的系统崩溃。

计算机安全包括物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安全包括信息完整性、机密性和可用性。可用性是指合法用户的正常请求能及时、正确、安全地得到服务或回应。

1.1.3 网络安全

网络安全，又称为计算机网络安全，是指保证任何两个实体之间的信息交流以及通信的安全可靠，满足计算机网络对信息安全的可用性、实用性、完整性、真实性、机密性和占有性的要求。

实用性是指信息加密密钥不可丢失，丢失了密钥的信息也就丢失了信息的实用性，成为垃圾。

可用性是指主机存放的静态信息的可用性和可操作性。病毒就常常破坏信息的可用性，使系统不能正常运行，数据文件面目全非。

占有性是指存储信息的主机、磁盘等信息载体被盗用，导致对信息占用权的丧失。保护信息占有性的方法有使用版权、专利权、商业秘密性，提供物理和逻辑的存取限制方法；维护和检查有关盗窃文件的审计记录；使用标签等。

网络安全的研究内容从广义上说，包括物理安全、通信安全、计算机安全、管理安全、人事安全、媒体安全和辐射安全。从系统外来看，研究内容还包括管理和法律两个方面，两者的综合构成了一个合理的研究结构和层次。

物理安全包括门锁、门卫以及其他物理访问控制设施的安全；敏感设备的防篡改能力，如红外线报警装置等不能被侵入者随意停用；环境控制包括温度、湿度、防尘等内容。

人事安全包括员工的素质，敏感岗位的身份识别；雇员筛选过程；安全培训和安全意识；安全监察等内容。

管理安全包括对软件从外部进入的控制，安全泄露事件调查，审计跟踪和责任控制检查的操作程序等。

媒体安全指存储的信息保护；控制敏感信息的记录、再生和销毁过程；确保废弃的纸张或含有敏感信息的磁性介质得到安全的销毁；对媒体进行扫描，以便发现病毒。

辐射安全是指控制射频(RF)及其他电磁(EM)辐射所造成的信息泄露。

1.1.4 信息安全

信息安全是指信息系统的系统资源与信息资源不受自然或人为有害因素的威胁和危害，防止窃取、篡改和非法操作；在信息的采集、存储、处理、转播和运用过程中，信息的机密性、完整性、可用性和共享性等都能得到良好保护的状态。信息安全传输是指在网络上传递的信息没有被故意的或偶然的非法授权泄露、更改、破坏或是信息没有被非法系统识别、控制，网络信息的机密性、完整性、可用性、可控性得到良好保护的状态。

信息安全涉及到信息存储的安全(又称信息状态安全，即存储保密)、信息传输的安全(又称信息状态转移安全，即传输保密)和对网络传输信息内容的审计三方面，当然也包括对用户的鉴别和授权。为保障数据传输的安全，需采用数据传输加密技术、数据完整性鉴别技术；为保证信息存储的安全，必须保障数据库安全和终端安全；信息内容审计，则是实时对进出内部网络的信息进行内容审计，以防止或追查可能的泄密行为。

互联网络信息安全的传统含义是指信息的机密性、完整性和可靠性。可靠性是指信息的可信度，包括信息的完整性、准确性和发送人的身份证实等方面，是信息安全性的基本要素。

以上几类安全性之间的关系，可用如图 1-1 所示的安全环表示。

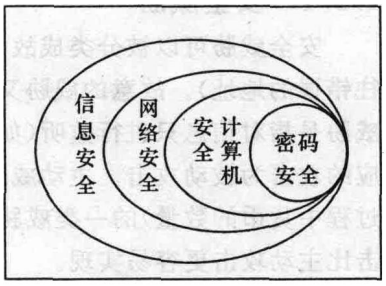


图 1-1 安全环

1.1.5 电子商务安全

电子商务安全是指通过制定安全策略，并在安全策略的指导下构建一个完整的综合保障体系，来屏蔽信息传输风险、信用风险、管理风险和法律风险，以保证网上交易的顺利进行，满足开展电子商务所需的机密性、认证性、完整性、可访问性、防御性、不可否认性和合法性等安全性需求。认证性是指确认通信双方身份的合法性；可访问性是指确保系统、数据和服务只能

由合法的人员访问；防御性是指能够阻挡黑客和不合法信息的进入；不可否认性是指防止通信或交易双方对已进行的业务的否认；合法性是指保证各方的业务符合可适用的法律或法规。

密码安全、计算机安全、网络安全和信息安全是电子商务安全的基础。它们所采用的安全技术都是电子商务安全技术的重要组成部分。

电子商务安全与网络安全、信息安全等一样，包括相互关联的两个方面：一是面向技术的安全系统的研究与应用；二是社会人文环境的建设，包括法律、法规以及信息道德、伦理等网络文化的构建。本书主要从技术层面讨论电子商务的安全需求、安全服务和安全机制，并结合电子商务自身的属性，探讨电子商务安全认证系统的原理、设计、实施和应用。

1.2 安全威胁与防护措施

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性或可用性所造成的危险。某种攻击就是某种威胁的具体体现。

所谓防护措施，是指保护资源免受威胁的一些物理上的控制、机制、策略或过程。脆弱性是指在防护措施中或在缺少防护措施时系统所具有的弱点。

所谓风险，是关于某个已知的、可能引发某种成功攻击的脆弱性的代价的测度。当某个脆弱的资源的价值较高，以及成功攻击的概率较高时，风险也就高；与之相反，当某个脆弱的资源的价值较低，以及成功攻击的概率较低时，风险也就低。风险分析能够提供定量的方法来确定防护措施的支出是否应予以保证。

1.2.1 安全威胁

安全威胁可以被分类成故意的威胁（如黑客渗透）和偶然的威胁（如信息被发往错误的地址）。故意的威胁又可以进一步被分类成被动威胁和主动威胁。被动威胁是指对信息只进行监听（如搭线窃听），而不对其进行修改的一类威胁，它所对应的攻击为被动攻击。主动威胁指对信息进行故意的修改（如改动某次金融会话过程中货币的数量）的一类威胁，它所对应的攻击为主动攻击。总的来说，被动攻击比主动攻击更容易实现。

1. 基本安全威胁

(1)信息泄露：指信息被泄露或透露给某个非授权的人或实体。这种威胁来自诸如窃听、搭线，或其他更加错综复杂的信息探测攻击。

(2)完整性破坏：指数据的一致性通过非授权的增删、修改或破坏而受到损坏。

(3)服务拒绝：指对信息或其他资源的合法访问被无条件地阻止。这可能由以下攻击所致：攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量

的负荷，从而导致系统的资源在合法用户看来是不可使用的。也可能是由于系统在物理上或逻辑上受到破坏而导致业务中断。

(4)非法使用：指某一资源被某个非授权的人或以某一非授权的方式使用。这种威胁的例子如：侵入某个计算机系统的攻击者会利用此系统作为侵入其他系统的突破口。

以上 4 种安全威胁又总称为基本安全威胁。基本安全威胁是通过使用下述主要的可实现威胁中的一种或几种而实现的。

2. 主要的可实现威胁

可实现威胁又可以分成渗入威胁和植入威胁。

(1)渗入威胁

①假冒欺骗：指某个实体(人或者系统)假装成另外一个不同的实体。这是越过某个安全防线的最为通用的方法。某个非授权的实体欺骗某个防线的守卫者，使守卫者相信它是一个合法的实体，从而骗取到合法实体的权利和特权。黑客大多采用假冒攻击。一般采用源 IP 地址欺骗攻击，入侵者伪装成源自一台内部主机的一个外部地点传送信息包，这些信息包中包含有内部系统的源 IP 地址。

②旁路控制：为了获得非授权的权利或特权，攻击者会发掘系统的缺陷或安全性上的脆弱之处。例如，攻击者通过各种手段发现原本应保密，但是却又暴露出来的一些系统“特征”。利用这些“特征”可以精心设计一条绕过安全控制的路由，把信息包传送到目的站点，并绕过守卫者防线侵入系统内部。

③身份攻击：指用户身份在通信时被非法截取。常用的攻击方法有缺省的登录界面(Shell Scripts)攻击法和诱入法。

④授权侵犯指被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也被称作内部攻击。

(2)植入威胁

①特洛伊木马(Torojan Horse)：是指包含在合法程序里的未授权代码。未授权代码执行不为用户所知(或不希望)的功能；或者是已被未授权代码更改过的合法程序，执行不为用户所知(或不希望)的功能；或者是看起来像是执行用户希望和需要的功能但实际上却执行不为用户所知(或不希望)的功能(由于含有未授权代码)。例如，一个外表上具有合法目的的应用程序——文本编辑器，它具有一个暗藏的目的，就是将用户的文件拷贝到一个隐藏的秘密文件中，这个文本编辑器就是特洛伊木马。

②陷阱门：指在某个系统或其部件中设置“机关”，使得当提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许存在一个特别的用户身份号，可以免除通常的口令检测。

3. 潜在威胁

对安全威胁中任何一种基本安全威胁或可实现威胁进行分析，就可以发现某些特定的潜在威胁。而任何一种潜在威胁的出现都可能导致一些更基本的威胁的产生。例如，考察信息泄露这样一种基本安全威胁，可以得出除主要可实现威胁以外的下述潜在威胁：

(1)窃听：信息从被监视的通信过程中泄露出去。

(2)电磁/射频截获：信息从电子或机电设备所发出的无线频率或其他辐射中被提取出来。

(3)人员疏忽：一个被授权的操作人员为了金钱和利益，或者由于粗心，将信息泄露给一个非授权的人。

(4)业务流分析：非授权的实体通过对通信业务流模式进行观察，而获得秘密信息。

(5)媒体废弃物：信息从废弃的磁性介质或打印的媒体中被获取。

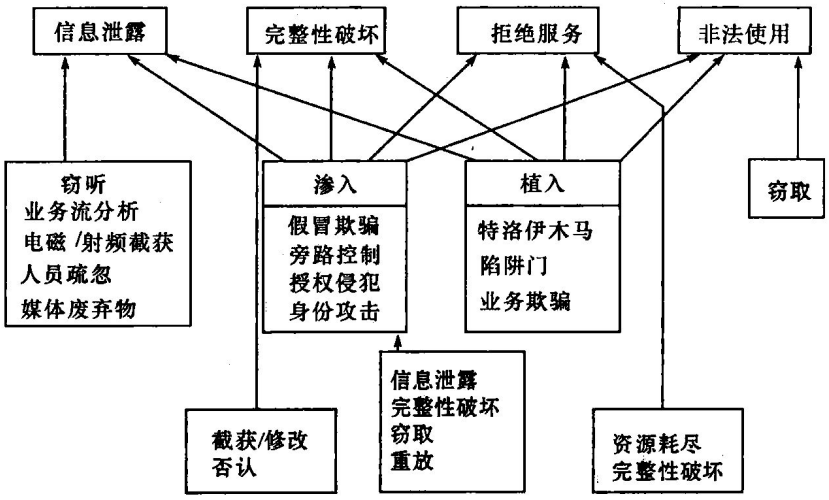


图 1-2　典型的潜在威胁及其相互关系

图 1-2 给出了一些典型的威胁以及它们之间的相互关系。注意图中的路径可能回旋。例如，假冒威胁构成所有基本威胁的基础。然而，假冒威胁本身也有信息泄露的潜在威胁(因为信息泄露可能泄露的是一个口令，攻击者使用此口令能够实施假冒攻击)。

在一次抽样调查中发现，按照出现频率由高至低排列，几种最主要的威胁是授权侵犯、假冒欺骗、旁路控制、特洛伊木马或陷阱门、媒体废弃物。

4. 网络安全威胁

在网络环境中，除了上述安全威胁以外，其他的安全威胁还有：

(1)数据截收:这是一种常见的网络威胁,指非法用户截取通信网络中的数据。很多网络间谍、黑客正是通过截取大量的信息包,进行分析解密,从而获取信息或密码。

(2)篡改数据:非法用户改变信息的内容。即对数据进行替换、更改、插入、排序等非法操作。

(3)物理侵入:一个侵入者通过避开系统的物理控制设施,获得对系统的访问权。

(4)重放:出于非法的目的的用户将所截获的某次合法通信数据进行拷贝,重新发送到网络中。

(5)业务否认:通常是指通信中某一方事后否认曾经参与某次通信活动的行为,不承认曾发送或接收信息的事实。

(6)资源耗尽:由于某一资源(如访问接口)被故意超负荷地使用,使得无法响应其他用户的服务请求,导致服务中断。

(7)业务欺骗:某一非法系统(或系统部件)欺骗合法的用户(或系统),使它们自愿地提供敏感信息。

(8)窃取:某一安全攸关的物品(如令牌或身份卡)被偷盗。

(9)中继攻击:指非法用户截取信息后延时发送。

1.2.2 防护措施

在安全领域有多种类型的防护措施。除了采用密码技术构造防护措施之外,还可以在物理安全、人员安全、管理安全、媒体安全、辐射安全和产品的生命周期控制等方面采取相应的防护措施,以保证整个系统的安全。

根据木桶原理,一个安全系统的强度与其最弱保护点的强度是相同的。为了提供有效的安全性,需要将属于不同种类的防护措施联合起来使用。例如,当用户将口令遗忘在某个不安全的地方,或者受到欺骗而将口令暴露给某个未知的用户时,即使技术上是完备的,用于防范假冒攻击的口令系统也将是无效的。

防护措施可用来对付大多数的安全威胁,但是每个防护措施均要付出代价。一个网络用户需要仔细考虑这样一个问题,即为了防止某一攻击所付出的代价是否值得。例如,在商业网络中,一般不考虑防范电磁(EM)或射频(RF)泄漏,因为对商用系统来说其风险是很小的,而且其防护措施又十分昂贵。对于某一特定的网络环境,究竟采用什么安全防护措施,作出何种决策属于风险管理的范畴。

1.2.3 电子商务的安全风险

电子商务既带来了巨大的机遇,也存在着各种风险。电子商务的安全风险,主要包括信息传输风险、信用风险和管理风险。

1. 信息传输风险

信息传输风险是指进行网上交易时,因传输的信息失真或者信息被非法窃取、

篡改或丢失，所造成网上交易的不必要损失。

(1)客户面临的风险

客户面临的风险是指客户一方的私有信息被盗用或破坏的可能性。私有信息包括：客户的账号及密码、信用卡信息、客户计算机系统及数据等。被盗取的途径主要有以下四种：利用欺骗性网站盗取；从销售商或网络服务提供商(ISP)那里盗取；从客户计算机上的 Cookies 文件中盗取；直接骗取。

①欺骗性网站：欺骗性网站主要有两种，一种是黑客设立的假冒网站，另一种是黑客利用现有网站程序的漏洞欺骗客户。假冒网站是黑客在 Internet 上设立的，假冒某个合法的销售站点的网站。客户在访问或购物时，会被要求提供信用卡号及其他的信息，黑客在骗取了大量的客户信息后，便撤销网站。而黑客利用已有网站程序中的漏洞来欺骗客户，这种情况更不容易被发现。黑客利用一些现有网站程序中的漏洞来监控，记录用户的账号、密码等信息，或利用网络浏览器的漏洞窥探访问者的硬盘，或者由一个临时性的假冒网站产生一个 Bug 程序，黑客利用这个程序可以查看用户的硬盘并盗窃客户机器上的文件。

②从销售商和网络服务提供商那里盗取客户的信息：在电子商务中，客户在进行商务活动时要提供给销售商和 ISP 大量的隐私信息(如信用卡号等)。如果黑客入侵了销售商和 ISP 的服务器，客户的私有信息就有可能被盗取。

③从 Cookies 文件中盗取客户的信息：当客户第一次访问一个网站时，主机会分配给用户一个独立的标识码，并创建一个 Cookies 文件，将用户的账号、密码存放在里面，并将该文件存在用户的机器的硬盘上。当用户的计算机被非法访问或侵入时，Cookies 文件会泄露用户信息。

④直接骗取密码：直接骗取是指黑客假扮系统管理员等，通过 E-mail 或电话与客户联系，谎称网络有故障，要求得到客户的密码。

(2)销售商面临的风险

在电子商务中，销售商面临的风险主要有三个方面：假客户、被封锁服务和数据被窃取。

①假客户：指一些人假扮客户来订购产品或服务。例如，用假信用卡来骗取免费服务或免费产品，或者要求送货而没有人来支付。

②服务拒绝：指销售商的计算机和网络资源被黑客攻击和封锁，从而导致无法提供正常的销售服务。

③数据被窃取：销售商们面临的一种很常见的风险，黑客可以随时、随地作案，而且很难被追踪到。

(3)企业自身面临的风险

企业内部网也存在很大的风险性，归纳起来主要有以下三个方面：灾难性风

险、企业内部网的风险、企业间进行商务活动时的风险。

①灾难性风险：包括自然灾难和人为制造的灾难。自然灾难包括火、洪水、飓风、地震、电子风暴等。人为制造的灾难包括计算机病毒和硬件设备的人为破坏。硬件设施的风险，主要有网络设备和通讯线路被他人破坏，或者网络线路被他人搭线监听等。

②企业内部网的风险：据统计，对网络系统的攻击有85%是来自企业内部的黑客。企业内部网的风险主要有两种：金融诈骗、盗取文件或数据。

金融诈骗是指更改企业计算机内部有关财务方面的记录，以骗得企业的钱财或为减免税等。这种风险的作案手段很多，有采用黑客程序的，更多的则是贿赂有关操作人员。

盗取文件或数据是一种很常见的黑客作案方式。由于Intranet将各个雇员的计算机同企业各种重要的数据库、服务器等连接起来，所以雇员进行越权访问和复制机密数据或文件的机会就会大大增加。这就需要企业加强网络管理及网络的审计、监督机制等来加强防范。

③企业与其他企业进行商务活动时的风险：企业在与其他企业进行商务合作或竞争时，其他企业可能利用非法手段窃取该企业的文件或数据。这其中的风险可分为两类：传输中数据的被盗、企业计算机上的数据及文件的被盗。

2. 信用风险

信用风险主要来自三个方面：

(1)来自买方的信用风险：对于个人消费者来说，可能在网络上使用信用卡进行支付时恶意透支，或使用伪造的信用卡骗取卖方的货物行为；对于集团购买者来说，存在拖延货款的可能，卖方需要为此承担风险。

(2)来自卖方的信用风险：卖方不能按质、按量、按时寄送消费者购买的货物，或者不能完全履行与集团购买者签订的合同，造成买方的风险。

(3)买卖双方都存在抵赖。

3. 管理风险

网上交易管理风险是指由于交易流程管理、人员管理、交易技术管理的不完善所带来的风险。

(1)交易流程管理风险：在网络商品进行交易的过程中，客户进入交易中心，买卖双方签订合同，交易中心不仅要监督买方按时付款，还要监督卖方按时提供符合合同要求的货物。在这些环节上，都存在着大量的管理问题，如果管理不善势必造成巨大的潜在风险。

(2)人员管理风险：人员管理是网络交易安全管理中的最薄弱的环节。近年来我国计算机犯罪大都呈现内部犯罪的趋势，其原因主要是因工作人员职业道德修

养不高，安全教育和管理松懈所致。一些竞争对手还利用企业招募新人的方式潜入该企业，或利用不正当的方式收买企业网络交易管理人员，窃取企业的用户识别码、密码、传递方式以及相关的机密文件资料。

(3)网络交易技术管理的漏洞：有些操作系统中的某些用户是无口令的，允许被信任用户不需要口令就可以进入系统，然后把自己升级为超级用户。

1.2.4 电子商务面临的安全威胁

电子商务所面临的威胁有：

(1)假冒：这是电子商务中常见的一种破坏方式，网上“黑客”伪装成合法的用户，进行非授权的访问或作出有害于合法用户的行为，或者特权较少的用户为了得到额外的特权也可能进行冒充，以达到欺骗、占有合法用户资源的目的。

(2)篡改数据：篡改数据除破坏数据完整性外，还包括在递交不可抵赖之后对源点本地存储的订单、合同等电子单证内容作篡改，以及在递交不可抵赖之后对接收端存储的电子单证内容作篡改。

(3)偷看、窃取信息：指电子商务用户或外来者未经授权地偷看或窃取他人的报文内容以获取商业秘密。

(4)报文的丢失或重放：报文丢失在电子商务应用中被认为是很严重的。报文的重放指人为地重放支付报文。

(5)对业务系统的干扰：造成电子商务信息系统和网络的瘫痪，使其网络的服务实体忙于执行非法服务性操作，从而使系统或正常用户不能执行其功能或被阻止执行其功能，对信息资源的授权访问受阻。

(6)否认或抵赖：对合同、契约和账单等商业性文书而言，处理起草、提交、传送和投递等任何环节上发生的抵赖或矢口否认都是相当棘手的。尤其是在电子商务中采用自动转发、重新定向等安全服务时，否认或抵赖的破坏性还会增加。

(7)拒绝服务：局部系统的失误或通信协议的不一致会导致系统的中断，从而拒绝服务。局部系统出于自我保护目的而故意中断通信也会导致拒绝服务。

(8)流量分析：这是在窃取交易信息基础上的一种破坏方式，它的主要目标不是信息本身的含义，而只是通过宏观了解信息流的走向和信息流的变化大小，判断信息交换的频繁程度，再结合其他方面的情报加以利用。

1.3 安全策略

从安全风险和安全威胁等方面对系统进行安全需求分析之后，可以确定系统面临的主要攻击。面对这些攻击，为保证信息的机密性、完整性和可用性，首先应该制定安全系统的总体安全策略。