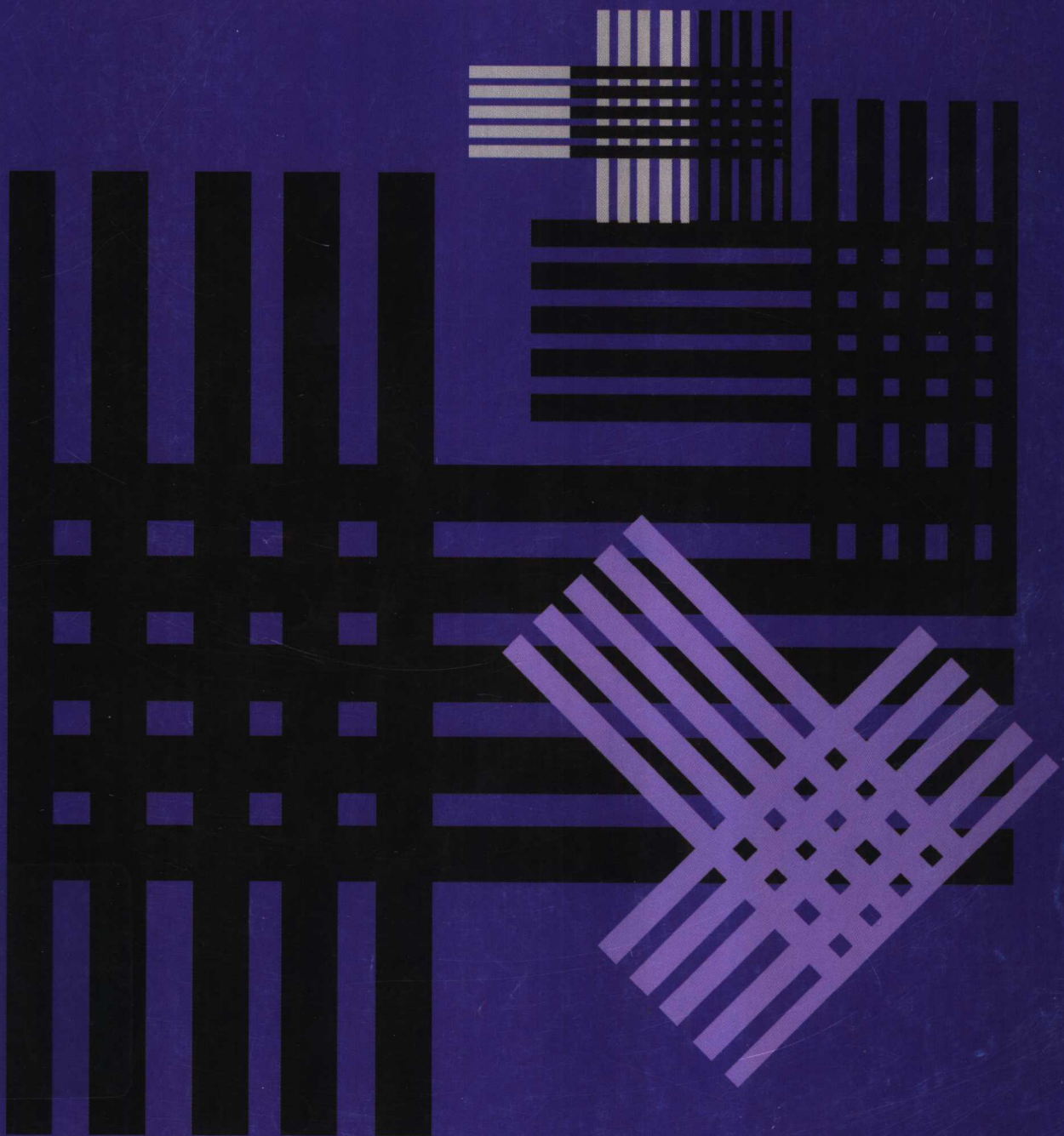
全国中等职业技术学校电子商务专业教材

Quanguozhongdengzhiyejishuxuexiaodianzishangwuzhuanyejiaocai

电子商务安全技术



中国劳动社会保障出版社

zhongguolaodongshehuibaozhangchubanshe

全国中等职业技术学校电子商务专业教材

电子商务安全技术

劳动和社会保障部教材办公室组织编写

顾巧论　主编

中国劳动社会保障出版社

本书根据劳动和社会保障部培训就业司审定颁发的《电子商务专业教学计划》和《电子商务安全技术教学大纲》编写，供中等职业技术学校电子商务专业使用。主要内容有：电子商务安全概述、电子商务的安全需求、电子商务安全的保障技术、电子商务安全的解决方案、电子商务安全的法律法规等。

本书也可作为职业培训教材。

本书第二章、第三章由顾巧论编写，第一章、第五章由李莉编写，第四章由蔡振山编写，顾巧论主编；安淑芝主审。

图书在版编目(CIP)数据

电子商务安全技术/顾巧论主编. —北京：中国劳动社会保障出版社，2002.12
全国中等职业技术学校电子商务专业教材
ISBN 7-5045-3796-9

Ⅰ.电… Ⅱ.顾… Ⅲ.电子商务-安全技术 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2002)第 098175 号

中国劳动社会保障出版社出版发行
(北京市惠新东街 1 号　邮政编码：100029)
出 版 人 ：张梦欣
*
北京新华印刷厂印刷　新华书店经销
787 毫米×1092 毫米　16 开本　9.25 印张　216 千字
2003 年 4 月第 1 版　　2003 年 4 月第 1 次印刷
印数：5000 册
定价：13.00 元
读者服务部电话：64929211
发行部电话：64911190
出版社网址：http://www.class.com.cn

前　言

随着计算机技术和网络技术应用的迅猛发展以及人们物质生活和精神生活水平的不断提高，电子商务作为一个新兴的商业模式，已经显示出强劲的发展前景，并逐渐走进人们的日常生活中，由此带动了对电子商务技术人才的需要，以及职业技术学校电子商务专业教学的发展。为适应上述要求，促进电子商务专业教学在各职业技术学校的开展，劳动和社会保障部培训就业司于2003年3月颁发了《电子商务专业教学计划与教学大纲》。

根据部颁教学计划及相关课程的教学大纲，劳动和社会保障部教材办公室组织了电子商务专业教材的开发工作，并在开发工作中始终坚持以下几个原则。

第一，坚持以能力为本位，重视实践能力的培养，突出职业教育的特色。根据电子商务专业毕业生所从事职业以及劳动力市场的实际需要，确定学生应具备的能力结构与知识结构，在保证学生必备专业基础知识的同时，加强实践性教学内容。

第二，充分考虑计算机技术、网络技术的发展，以及电子商务的最新应用，体现教材的先进性，以保证学生所学技能在实际工作中得以运用。

第三，贯彻国家关于职业资格证书与学业证书并重的政策，教材内容力求涵盖国家职业标准《电子商务师》中的电子商务员（国家职业资格四级）的知识和技能要求，确实保证毕业生达到中级技能人才的培养目标。

这次开发的电子商务专业教材有：《电子商务基础理论与实践》《电子商务数据库》《电子商务网页设计》《电子商务网站建设》《电子商务物流与配送》《电子商务安全技术》《网络营销》《电子商务会计》。

这次教材的开发工作得到了有关省、直辖市、自治区劳动和社会保障厅（局）及天津职业技术师范学院的大力支持，对此，我们表示诚挚的谢意。电子商务专业教学尚处于发展阶段，希望广大师生结合本地的教学实践对教材提出宝贵意见，以供我们在修订教材时参考和借鉴。

劳动和社会保障部教材办公室

2003年6月

目　录

第一章　电子商务安全概述

电子商务是利用计算机网络开展的商务活动，它具有巨大的潜在市场及十分诱人的发展前景。在因特网上开展的电子商务，其安全是否能得到保障，这是每个客户、商家、银行及诸多参与者最为关心的切身利益问题，也是各国政府、国际组织及业内人士致力于研究的现实问题。只有在电子商务安全得到了相应的保障，使其变得可信、有序，才能使更多的用户愿意投身于电子商务之中，并在应用电子商务的同时发展电子商务。因此，电子商务安全问题是发展电子商务的关键之一。

§1—1　电子商务安全的重要性

因特网（Internet）是一个高度开放的网络，电子商务是在因特网上进行的，并完全依赖于网络。电子商务的安全性是由网络的安全性来保证的。网络及应用系统能够为电子商务的安全性、可靠性和可用性提供足够高的保证，是进行电子商务的前提。

一、电子商务安全面临的严峻形势

传统交易过程中买卖双方是面对面的，交易过程中的安全性和信任感是不言而喻的。在电子商务过程中，由于买卖双方是通过网络来进行的，其中的欺诈性以及网络开放造成的不安全性，会使电子商务的安全性降低。随着经济信息化进程的加快，网上犯罪也日趋猖獗。黑客（Hacker）的袭击在计算机网络最发达的国家尤为严重。一些黑客组织在因特网上公开网址，免费提供黑客工具软件，介绍黑客手法，出版网上黑客杂志和书籍，使普通人也能轻而易举地学会网络攻击方式。计算机网络上黑客的破坏已经对经济秩序、经济建设、国家信息安全构成了严重的威胁。

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；中等层次威胁是有组织的威胁，包括一些机构“黑客”、有组织的犯罪、工业间谍；最高层次威胁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。其具体表现为假冒行为、越权行为、破坏行为、窃听行为、干扰行为和否认行为等。

假冒行为主要是指没有经过授权的人采用一定的手段，假冒合法用户进入系统内部，搜集、篡改、使用系统资源等非法行为。

越权行为主要是指虽经授权进入系统，但所干之事已经超越允许范围，对系统造成威胁等非法行为。

破坏行为主要是指向系统装入非法程序，破坏系统正常工作，破坏系统中的硬件或软件，破坏信息和网络资源等非法行为。

窃听行为主要是指搭线进行通信监视、截获军事和经济情报等非法行为。

干扰行为主要是指对通信数据的内容或对通信时间和先后次序进行修改、伪造等非法行为。

否认行为主要是指对自己在通信或交易中做过的事情拒不承认等非法行为。

电子商务系统在黑客的破坏性活动面前有时会显得软弱无力。同传统的金融管理方式相比，电子商务的金融资金是在计算机网络上进行流通的，因此，电子商务金融系统就成了一个新的犯罪活动目标。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顾此失彼；由于大多数管理者对网络安全不甚了解，加之信息犯罪是跨国界的高技术犯罪，因而用现有的法律想有效地预防是十分困难的。罪犯只需用一台计算机、一条电话线，以及一个调制解调器就能达到远距离做案的目的。现有的科技手段有时也难以侦察到这些黑客的行踪。

目前，我国电子商务金融系统的计算机犯罪案件亦呈上升趋势，从已发生的多起利用计算机网络进行电子商务金融犯罪的案件中，可以看出我国目前电子商务金融系统安全的现状。正如专家们所比喻的：用不加锁的储柜存放资金（形容电子商务企业缺乏安全防护）；用“公共汽车”运送钞票（形容电子支付系统缺乏安全保障）；用“邮寄托寄”方式传送资金（形容转账支付缺乏渠道）；用“平信”邮寄机密信息（形容对于敏感信息缺乏保密措施）；用“商店柜台”方式存取资金（形容授权缺乏安全措施）等。在银行计算机犯罪案件中，篡改数据是犯罪类型之一，而银行对数据的保护、操作密码的保护及储户密码的保护则缺乏有力的措施。

电子商务的前景是诱人的，而安全问题是目前亟待解决的头等大事。

二、电子商务安全问题的类型

电子商务安全可以分为物理安全、网络安全、数据安全、交易不同方所表现出的不同的安全等几种类型。

1. 物理安全

所谓物理安全主要是指主机硬件和物理线路的安全，其中包括火灾等自然灾害、辐射、

硬件故障、搭线窃听、盗用等。

2. 网络安全

网络安全是指计算机联网所带来的安全问题。由于大部分因特网软件协议没有安全性设计，所以网络计算机可以被任何一台上网计算机攻击。而且网络服务器经常用超级用户特权来执行，这样就存在着大量的安全隐患，如非法授权访问、攻击信息的完整性、冒充主机和用户、干扰服务等一系列的安全问题。

3. 数据的安全

在电子商务活动中，相关数据在因特网公用数据传输线上传递，例如通过网络进行资金的划拨等，这种交易方式的安全性是交易各方极为关心的问题。其安全性主要包括数据的保密性、数据的完整性和数据的不可否认性等。

4. 交易不同方所表现出的不同的安全

电子商务交易是买卖双方通过网络进行联系的。在整个交易过程中，客户将姓名、信用卡的账号、用户的口令、密码、订货内容及付款信息等都输入到网上，如果被不法之徒盗用，那么对客户而言就等于自己的钱袋被别人“共享”；对交易的另一方来说，如果信息被竞争对手获得，那么自己的经济利益无疑将受到极大的损害。

三、电子商务安全问题的表现形式

任何以干扰、破坏电子商务系统为目的的非法授权行为都称为网络攻击（黑客攻击）。入侵者对电子商务网络发起的攻击是多样的，其攻击层次与电子商务所采用的安全措施紧密相关。它的表现形式也不尽相同，主要表现形式如下：

1. 程序处理错误

在使用计算机的过程中，有时系统会陷入混乱的局面，此时机器对任何的输入都没有反应，这是程序出错或者使用了盗版软件的缘故。通过网络也可以使正在使用的计算机出现这种无响应、死机现象。这是一种处理 TCP/IP 协议或者服务程序的错误，是故意在输入端口的数据包的偏移字段和长度字段中写入一个过大或过小的值所致。操作系统不能处理这种情况，从而造成死机情况发生。

2. Web 欺骗

Web 欺骗是一种在因特网上使用的针对 WWW 的攻击技术。这种攻击方法会窃取某人的隐私或破坏数据的完整性，危及到使用 Web 浏览器的用户（包括使用 Netscape Navigator 和 Internet Explorer 的用户）。有时，Web 管理员、Web 设计者、页面制作人员、Web 操作员以及编程人员无意地犯一些错误，这些都将导致安全问题的发生。编程的错误可能导致系统崩溃或是损害系统的安全。

3. 网络协议漏洞

因特网中的 TCP/IP 协议在创建之初，从安全性方面考虑不多。黑客千方百计地寻找网络协议的问题或漏洞，对系统进行攻击，致使系统不能正常工作，甚至崩溃。

4. IP 欺骗

通过 IP 地址的伪装使得某台主机能够伪装成另外一台主机，被伪装的主机具有某种特权或被其他的主机信任。IP 欺骗通常都要用程序来实现。通过作用 Rax Socket 编程，可以发送带有假冒的源 IP 地址的数据包。另外，目前在网上也有大量可发送伪造 IP 地址的工具包可以使用，使用这些工具包可以任意指定源 IP 地址，以免留下自己的痕迹。

5. 缓冲区溢出

缓冲区溢出是一个非常普遍、非常危险的漏洞。该漏洞在各种操作系统、应用软件程序中广泛存在。缓冲区溢出主要是向一个有限空间的缓冲区中拷贝了过长的字符串，由此带来了两种后果：一是过长的字符串覆盖了相邻的存储单元，引起程序运行的失败，严重的可能引起计算机死机、系统重新启动困难等后果；二是利用这种漏洞可以执行任意的指令，甚至可以取得系统的特权。缓冲区溢出的漏洞早已为人们所熟知，但直到近两年才引起软件和系统人员的重视。

6. 远程攻击

远程攻击指专门攻击除自己计算机以外的计算机。进行远程攻击的第一步并不需要和攻击目标进行密切接触，入侵者的首要任务是决定它要对付谁。

四、电子商务安全问题的引发因素

安全是任何商业活动都应具备的保证，电子商务更是如此。由于因特网的开放性和不安全性使得通过电子商务交易的双方都面临着许多安全方面的威胁。产生安全问题的因素很多，涉及商务活动的各个方面。

1. 人的因素

在任何商业交往中人是最关键的。在电子商务交易中交易双方互相隔离，很难用传统的方法验证对方的身份，只有通过因特网交换信息才能完成交易，其不确定性和隐蔽性是导致电子商务安全问题的一个因素。由于电子商务是一种全新的商务方式，参与电子商务交易中的各方及系统管理人员道德素质的高低、在电子商务中所涉及的法律规范、安全技术等方面都有一个逐步健全和完善的过程，因此在电子商务中人是一个非常重要的因素。

2. 网络的因素

由于网络的全球性、开放性、无缝连通性、共享性、动态性等，使得任何人都可以自由地进入网络进行商务活动。也正是这样一个开放的环境，使得企业发布商务信息更简便，客户选择所需要的产品更方便，因而在实际交易过程中传递的信息也更容易被截获。开放（共享）和保密是相互矛盾的，既要保持系统开放，又要保证交易的安全、保密，解决这一矛盾在实际运作时所需要的技术是比较复杂的。

3. 其他因素

电子商务的交易过程是建立在非常复杂的网络环境上的，它的运作过程基本是通过以二进制位（比特）为单位的电子信息流在网上传递实现的。它对系统安全的依赖性很强，特别

是对数据库服务器的可靠性、网络通信设备及数据的安全性要求很高。各种人为的因素，例如黑客的闯入，自然的、物理的不安全因素都会给这样一个复杂的系统带来威胁。

五、电子商务所需的安全服务

电子商务系统必须利用安全技术来满足电子商务的安全要求，为电子商务的参与者提供必需的鉴别服务、机密性服务、访问控制服务、不可否认服务、可用性服务、防御性服务等安全服务项目。

1. 鉴别服务

对进行电子商务交易双方的身份进行鉴别，确认交易双方真实身份，也就是说，能够提供一种服务以确保其身份的真实性。

2. 机密性服务

信息的来源是可信的、完整的，电子商务的参与者获得的信息是真实可靠的，并在信息的存储、处理、传输过程中提供机密性保证。

3. 访问控制服务

合法用户只能访问系统授权和指定的资源，拒绝非法用户访问系统资源，这将有助于达到机密性、完整性、可控性和建立责任机制。

4. 不可否认服务

要求信息的发送方不能否认自己所发出的信息，反之，信息的接收方也不能否认已收到的信息。它的服务是为交易双方提供不可否认的证据。实际上它是保证交易双方的不可抵赖性和信息的完整性。

5. 可用性服务

保证授权用户可以持续访问信息和资源。

6. 防御性服务

可使参与电子商务的各方得到阻挡不希望信息或黑客攻击的服务。

§1—2　电子商务安全策略

电子商务的安全需要有完整的综合保障体系，安全管理的基本思路不应只单纯地从技术角度思考，而应综合技术、管理、法律等方面来认识和解决。一个完整的网络安全体系至少包括三方面的内容，缺一不可。一是技术保障，如防火墙技术、网络防病毒、信息加密存储，通信、身份认证、授权等；二是管理保障，如政府有关部门、企业的主要领导及信息服务商都要确实履行相关的职能，切实做好交易的安全制度保证，交易安全的实时监控，提供实时改变安全策略的能力，对现有安全系统进行漏洞检查以及安全教育等；三是法律的保障。只

有切实加强网上交易的防范措施，才能使电子商务系统安全运作。

一、建立电子商务的安全体系

目前，人们谈论的电子商务的安全问题主要还是从企业内部网（Intranet）出发，考虑基于因特网的电子商务安全问题。为了保证网络之间的正常联系和信息安全，企业内部必须建立一套较完整的电子商务的安全体系，这是一项极其复杂的工作。

1. 安全管理措施

建立内部网络的安全管理措施，一般要具备完整的内部网络口令系统，设置一些权限，制定辨别非法入侵的条件以及检查非法操作的规则。对于非法入侵者均记录在案。需记录的非法入侵事件主要包括：被拒绝的访问，用户进出网络情况，使用关键资源情况，敏感数据的传输，消极和积极侵入事件，对资源的威胁与破坏，网络设备启动、关闭、再启动情况等。

2. 安全技术措施

(1) 防火墙技术　防火墙是第一道防线，它在企业内部网与因特网之间形成一道屏障，可防止非法用户的访问并防止内部机密信息流出。防火墙具有以下优点：保护易受攻击的服务；控制对特殊站点的访问；集中化的安全管理；对网络访问进行记录和统计。

(2) 加密技术　加密技术是为了防止信息在因特网上传输时被窃听与伪造。在信息的传输过程中，通过某种算法把源信息进行变换，使之成为无法识别的密文，这一过程就是加密。对于那些需要保护的重要信息进行传输时一般都用密文表示。最流行的加密方法是公开密钥加密。每个用户具有两把密钥，一把是公钥，另一把是私钥。信息发送者使用接收者的公钥加密，接收者用私钥解密，以防止窃听。信息发送者用自己的私钥加密，接收者用发送中的公钥解密，以防止伪造。信息发送者先用自己的私钥加密，然后用接收者的公钥再加密;接收者先用自己的私钥解密,再用发送者的公钥解密,这样既防止了伪造,又防止了窃听。

(3) 认证技术　认证技术是保证电子商务交易安全的一项重要技术。在某种情况下，信息认证显得比信息加密更为重要。交易双方应当能够确认哪些信息是对方发送的或接收的，同时接收方还能确认信息在通信过程中没有被修改或替换。认证技术主要包括数字签名技术、身份识别技术、信息的完整性校验技术等。

1) 数字签名技术　在电子商务中人们希望快速传递贸易合同，因此就产生了数字签名技术，它能够使接收者核实发送者对文件的签名、发送者事后不能抵赖对文件的签名、接收者不能伪造对文件的签名等。只有加入数字签名和验证才能真正实现在公共网络上的安全传输。

在数字签名技术中通常一个用户拥有两个密钥对，一个密钥对用来对数字签名进行加密、解密，另一个密钥对用来对秘密密钥进行加密、解密。数字签名使用的是发送方的密钥对，发送方用自己的私钥进行加密，接收方用发送方的公钥进行解密。任何拥有发送方公钥的人都可以验证数字签名的正确性。秘密密钥使用的是接收方的密钥对，任何知道接收方公

钥的人都可以向接收方发送加密信息，而只有具有接收方私钥的人才能对信息进行解密。

2）身份识别技术　身份识别是确认和识别贸易双方真实身份不可缺少的环节。在电子商务中，非法用户对网络进行攻击，如窃取口令、修改或伪造服务、阻断服务等都对系统造成威胁，阻止系统资源的合法管理和使用。通过身份识别技术能够做到：确信信息不是由冒充者发出的；在传输的过程中该信息没有被修改或替换；信息的发送方和接收方都不能对自己所发出的和接收到的信息加以否认；拒绝非法用户对系统资源的访问等。身份识别的基本方式主要有：用户的口令；用户的合法智能卡；用户具有的特征，如指纹、声音、视网膜扫描等。

3）认证机构　认证机构（CA）由一个或多个用户信任的组织实体组成。通过认证机构来认证买卖双方的身份是保证网络交易安全的重要措施。

CA 认证的一般过程是：为了确定商家的真实性，持卡人请求 CA 对其进行认证；CA 在对商家进行调查、识别后，将含有商家标识名称、公用密钥和经过 CA 数字签名的证书传给持卡人。当然，商家也可对持卡人进行认证。

二、制定电子商务安全协议

电子商务安全协议是指能抵抗任何攻击，完成与加密、认证、密钥分配等有关的用于安全交易的协议。制定电子商务安全协议是电子商务发展对安全的需要，是规范电子商务市场安全交易的需要。一个比较完善的安全协议应具备明确性、完整性、安全性和有效性等特点。

明确性是指该协议中的每一项规定都明白无误，没有歧义性。在实际执行协议的过程中，如果发生了纠纷，可通过公正、可信赖的第三方执行事先制定好的裁决协议；也可不需要第三方的参与，被欺骗方可通过执行事先制定好的自动执行协议，立即停止交易。

完整性是指对电子商务中可能发生的各种情况都事先做出应对的措施，一旦发生纠纷，可根据协议中的规定进行处理，避免无章可循的情况发生。

安全性是指能够抵抗已知的攻击，如网络协议攻击等。目前在网络中使用最普遍的协议就是 TCP/IP，黑客多数是利用协议中处理程序的错误对系统进行攻击，从而使系统死机、挂起或崩溃。

有效性是指协议的每一个步骤的执行都是必须的，无论是从减少通信，还是从节省计算资源来看都是必不可少的。

目前，已制定好的并正在应用的有关电子商务安全的协议主要有加密协议、认证安全协议、密钥管理协议与保护协议等。

加密协议是对网上传输的数据进行等级划分，采用多级控制的安全模式，使非授权人无法解读数据，使保密数据在公共网络中自由发送。

认证安全协议是为防止欺骗，如 Web 欺骗、IP 欺骗等，它包括消息认证、数据源认证和身份识别等。

密钥管理协议是处理密钥自产生到最终销毁的整个过程中的有关问题的协议，包括密钥的生成、分发、存储、保护、公证等内容。它将影响系统的安全性和有效性。密钥管理系统中一般需要公证系统的参与，从而实现密钥的分配和证实，保证文件本身的真实可靠性，签字者不能否认其签名，并在发生纠纷时进行仲裁。

保护协议主要用于对病毒、用户口令、密钥和数据等进行保护，防止未经授权者的入侵而造成对系统的威胁。

三、制定电子商务安全标准

1987 年，国际商会制定了《电传交换贸易数据统一行为守则》，为防止数据在传输过程中发生错误、泄露、篡改和欺诈，以及对贸易数据进行保护等起到了十分重要的作用。

1990 年，联合国领导下的安全联合工作组制定了国际通用的电子商务标准，其中包括有关电子商务的可靠性、完整性和不可抵赖性等方面的安全规则，安全鉴别和确认报文，电子商务机密性的安全规则，安全密钥和证书管理报告，交互式电子商务的安全规则等安全措施。

1997 年 5 月，在一些较大公司（如 IBM，Netscape，Microsoft，Oracle 等公司）的支持下，安全电子交易（SET）规范作为一个网络电子商务的开放标准使用。

另外，各国政府和国际标准化组织均采用可靠的密码算法和成熟的实现技术制定了相应的安全技术标准，例如，美国联邦信息处理（FIPS）公布的部分“安全标准”（见表 1—1）；国际标准化组织（ISO）和国际电工技术委员会（IEC）分别或联合制定的“ISO 和 ISO/IEC 通用密码技术标准”（见表 1—2）；ISO 制定的“银行业务安全标准”（见表 1—3）；ISO 和 ISO/IEC 等制定的“安全结构和安全框架标准”（见表 1—4）；美国国家标准学会（ANSI）的“加密和银行业务安全标准”（见表 1—5）等。这些标准和其他的标准都对电子商务的标准化起到了推动作用，在保障电子商务安全的互连互通中起到了积极的作用。

表 1—1　　FIPS 公布的安全标准

FIPS 号	主题	有关标准
FIPS 46 - 2	数据加密标准（DES）	ANSI X3.92
FIPS 81	DES 工作模式	ANSI X3.106
FIPS 113	数字认证（CBC - MAC）	ISO/IEC 9797
FIPS 186	数字签字标准（DSA）	FIPS 180，FIPS 180 - 1
FIPS JJJ	实体认证（非对称）	ISO/IEC 9798 - 3

表 1—2　　ISO 和 ISO/IEC 通用密码技术标准

ISO 号	主题	有关标准
9796	可恢复消息的签字	ANSI X9.31
9797	数据完整性机制	ISO 8731 - 1，ISO 9807，ANSI X9.9，ANSI 9.19

续表

ISO 号	主题	有关标准
10118 - 3	杂凑函数—采用定制的算法	SHA - I. RIPEMD - 128，RIPEMD - 166
10118 - 4	杂凑函数—采用模算术	MASH - 1，MASH - 2
11770 - 2	密钥管理—对称技术	Kerberos Otway - Rel 协议
11770 - 3	密钥管理—非对称技术	Diffie - Hellman 协议，ISO/IEC 9798
14888 - 1	有附件的签字—引论	ANSI X9.30 - 1，ISO/IEC 9796
14888 - 3	有附件的签字—基于证书的机制	DSA，EIGamal，Schvlorr，RSA 等签字

表 1—3　　ISO 银行业务安全标准（部分）

ISO 号	主题	有关标准
8731 - 1	消息认证 - CBC - MAC	ISO/IEC 9797，ANSI X9.9
11166 - 1	密钥管理/非对称的—概述	ISO 8732

表 1—4　　ISO 和 ISO/IEC 的安全结构和安全框架标准

ISO 号	主题	有关标准
7498 - 2	OSI 安全结构（按开放网络的层结构配置安全业务和安全机制）	ITU - T X.800
9594 - 8	认证框架（基于通行字和各种强化认证机制）	ITU - T X.509
10181	OSI 安全框架（认证、接入控制、不可否认、完整性、机密性和安全审计框架结构）	ITU - T X.816

表 1—5　　ANSI 的加密和银行业务安全标准

ANSI 号	主题	有关标准
X3.92	数据加密算法 DEA	FIPS 46 DES
X3.106	DEA 的工作模式	FIPS 81，ISO 8372
X9.8	DIN 管理和安全性	ISO 9564
X9.30 - 1	数字签字算法（DSA）	FIPS 186，FIPS 180
X9.31 - 1	RSA 签字算法	ISO/IEC 9796
X9.31 - 2	RSA 用杂凑算法	MDC - 2
X9.45	属性证书和其他控制法	ANSI X9.57
X9.52	三重 DES 和工作模式	ISO 8372
X9.55	证书扩充（V3）和 CRLS	TTU - T X509 V.3
X9.57	证书管理	TTU - T X509，ANSI X9.30 - 1

§1—3 电子商务安全的解决方案实例

电子商务系统中所存在的电子商务安全问题，涉及企业的商业机密，乃至国家的政治和经济机密。目前很多公司都提供了一些电子商务安全的解决方案，举例简单说明如下。

一、IBM 公司电子商务安全解决方案

世界上第一个能够提供跨行业电子商务安全解决方案的公司是 IBM 公司。IBM 公司为电子商务的应用在软件领域搭建了一个坚实的基础构架，它由开发工具和组件、应用服务器软件、安全的网络和管理软件三部分组成，其特点是完全开放，可跨各种操作系统平台使用。

IBM 不仅为政府、企业建立和应用电子商务提供全面的硬件及软件，还为客户提供享誉全球的 IBM 服务。目前，IBM 通过遍布全世界的约 80 个国家的服务体系为用户提供高质量的服务，不仅提供商业服务，还提供信息安全技术方面的服务。在 1996 年奥运会的售票过程中，IBM 与 VISA 合作，顺利地完成了 500 万美元的信用卡支付交易。IBM 在网络和交易安全性方面建立了长期和公认的信誉。IBM 领导 IT 的安全解决方案已经超过了 30 年，依靠它无与伦比的技能、技术和行业经验，以及良好的信誉，为客户安全可靠地利用电子商务开展业务提供了保证。

二、康柏公司电子商务安全解决方案

康柏公司以其优异的产品、方案和服务在中国赢得了市场，有近百套系统在中国运行。中国工商银行、中国深圳证券交易所等部分金融单位也选择了康柏的计算机系统。康柏积极参与中国的“金卡工程”，如广东、海南、大连、江苏、青岛、深圳、济南等地的自动柜员机、销售点终端网络交换系统的建设。

利用康柏基于 Windows NT 的 Proliant 因特网安全解决方案，能够使系统在停止工作时也能提供进行电子商务活动的保证。

高效因特网安全解决方案提供了高效、灵活的因特网防火墙解决方案，它能使企业内部网隔离黑客和其他潜在的威胁，并使合作伙伴和顾客安全接入内部网。

三、CA 国际有限公司电子商务安全解决方案

CA 国际有限公司是世界领先的独立软件供应商，也是计算机安全管理领域最大的产品和服务供应商之一。目前，它已在 36 个国家开设了 136 个办事处或子公司，在中国先后成立了独资公司和几个合资公司。它采用开放式安全保障技术，可对系统安全对象进行完整地鉴别和访问，同时还支持数据加密等。其 eTrust 是全方位的企业级系统安全解决方案。该公司不仅提供具有多方面和多层次保护系统安全的软件产品，而且还提供专业的系统安全服务，从而帮助企业制定出更加完善的安全策略，保证了企业信息的保密性、完整性和可用性。在美国大主机安全管理产品中，该公司计算机安全控管方面的软件产品的市场占有率为 60%。CA 防火墙既可以安放在企业网络边界处，又可以安装于重要的服务器上，具有一般防火墙不具备的特殊功能，更增强了对系统的保护。

习　　题

1. 电子商务安全分为哪几种类型?
2. 电子商务安全问题的表现形式有哪些?
3. 电子商务所需的安全服务有哪些?
4. 简述电子商务安全所需的技术措施。
5. 一个比较完善的安全协议应具备哪些特点?