 美国著名未来学家阿尔温托夫勒说：“ 电脑网络的建立和普及将彻底改变人类生存及生活的模式，控制与掌握网络的人就是未来命运的主宰。谁掌握了信息，控制了网络，谁就拥有整个世界。 ”的确，网络的国际化、社会化、开放化、个人化诱发出无限的商机，电子商务的迅速崛起，使网络成为国际竞争的新战场。然而，由于网络技术本身的缺陷，使得网络社会的脆性大大增加，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。所以，构筑安全的电子商务信息环境，就成为了网络时代发展到一定阶段而不可逾越的“ 瓶颈 ”性问题，愈来愈受到国际社会的高度关注。 一、电子商务中的信息安全技术 电子商务的信息安全在很大程度上依赖于技术的完善，这些技术包括：密码技术、鉴别技术、访问控制技术、信息流控制技术、数据保护技术、软件保护技术、病毒检测及清除技术、内容分类识别和过滤技术、网络隐患扫描技术、系统安全监测报警与审计技术等。 1.防火墙技术。防火墙(Firewall)是近年来发展的最重要的安全技术，它的主要功能是加强网络之间的访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络(被保护网络)。它对两个或多个网络之间传输的数据包和链接方式按照一定的安全策略对其进行检查，来决定网络之间的通信是否被允许，并监视网络运行状态。简单防火墙技术可以在路由器上实现，而专用防火墙提供更加可靠的网络安全控制方法。 防火墙的安全策

略有两条。一是“ 凡是未被准许的就是禁止的 ”。防火墙先是封闭所有信息流，然后审查要求通过的信息，符合条件的就让通过；二是“ 凡是未被禁止的就是允许的 ”，防火墙先是转发所有的信息，然后再逐项剔除有害的内容，被禁止的内容越多，防火墙的作用就越大。网络是动态发展的，安全策略的制定不应建立在静态的基础之上。在制定防火墙安全规则时，应符合“ 可适应性的安全管理 ”模型的原则，即：安全=风险分析 执行策略 系统实施 漏洞监测 实时响应。防火墙技术主要有以下三类： ●包过滤技术(Packct Filtering)。它一般用在网络层，主要根据防火墙系统所收到的每个数据包的源IP地址、目的IP地址、TCP/UDP源端口号、TCP/UDP目的端口号及数据包中的各种标志位来进行判定，根据系统设定的安全策略来决定是否让数据包通过，其核心就是安全策略，即过滤算法的设计。 ●代理(Proxy)服务技术。它用来提供应用层服务的控制，起到外部网络向内部网络申请服务时的中间转接作用。内部网络只接受代理提出的服务请求，拒绝外部网络其它节点的直接请求。运行代理服务的主机被称为应用机关。代理服务还可以用于实施较强的数据流监控、过滤、记录等功能。 ●状态监控(Statc Innspection)技术。它是一种新的防火墙技术。在网络层完成所有必要的防火墙功能包过滤与网络服务代理。目前最有效的实现方法是采用Check Point)提出的虚拟机方式(Inspect Virtual Machine)。 防火墙技术的优点很多，一是通过过滤不安全的服务，极大地提高网络安全和减少子网中主机的风险；二是可以提供对系统的访问控制；三是可以阻击攻击者获取攻击网络系统的有用信息；四是防火墙还可以记录与统计通过它的网络通信，提

供关于网络使用的统计数据，根据统计数据来判断可能的攻击和探测；五是防火墙提供制定与执行网络安全策略的手段，它可以对企业内部网实现集中的安全管理。防火墙技术的不足有三。一是防火墙不能防止绕过防火墙的攻击；二是防火墙经不起人为因素的攻击。由于防火墙对网络安全实施单点控制，因此可能受到黑客的攻击；三是防火墙不能保证数据的秘密性，不能对数据进行鉴别，也不能保证网络不受病毒的攻击。2.加密技术。数据加密被认为是最可靠的安全保障形式，它可以从根本上满足信息完整性的要求，是一种主动安全防范策略。数据加密就是按照确定的密码算法将敏感的明文数据变换成难以识别的密文数据。通过使用不同的密钥，可用同一加密算法，将同一明文加密成不同的密文。当需要时可使用密钥将密文数据还原成明文数据，称为解密。密钥加密技术分为对称密钥加密和非对称密钥加密两类。对称加密技术是在加密与解密过程中使用相同的密钥加以控制，它的保密度主要取决于对密钥的保密。它的特点是数字运算量小，加密速度快，弱点是密钥管理困难，一旦密钥泄露，将直接影响到信息的安全。非对称密钥加密法是在加密和解密过程中使用不同的密钥加以控制，加密密钥是公开的，解密密钥是保密的。它的保密度依赖于从公开的加密密钥或密文与明文的对照推算解密密钥在计算上的不可能性。算法的核心是运用一种特殊的数学函数单向陷门函数，即从一个方向求值是容易的，但其逆向计算却很困难，从而在实际上成为不可能。除了密钥加密技术外，还有数据加密技术。一是链路加密技术。链路加密是对通信线路加密；二是节点加密技术。节点加密是指对存储在节点内的文件和数据库信息

进行的加密保护。 3.数字签名技术。数字签名(Digital Signature)技术是将摘要用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要。在电子商务安全保密系统中，数字签名技术有着特别重要的地位，在电子商务安全服务中的源鉴别、完整性服务、不可否认服务中都要用到数字签名技术。 在书面文件上签名是确认文件的一种手段，其作用有两点，一是因为自己的签名难以否认，从而确认文件已签署这一事实；二是因为签名不易仿冒，从而确定了文件是真的这一事实。数字签名与书面签名有相同相通之处，也能确认两点，一是信息是由签名者发送的，二是信息自签发后到收到为止未曾做过任何修改。这样，数字签名就可用来防止：电子信息因易于修改而有人作伪；冒用别人名义发送信息；发出(收到)信件后又加以否认。 广泛应用的数字签名方法有RSA签名、DSS签名和Hash签名三种。RSA的最大方便是没有密钥分配问题。公开密钥加密使用两个不同的密钥，其中一个是公开的，另一个是保密的。公开密钥可以保存在系统目录内、未加密的电子邮件信息中、电话黄页上或公告牌里，网上的任何用户都可获得公开密钥。保密密钥是用户专用的，由用户本身持有，它可以对公开密钥加密的信息解密。DSS数字签名是由美国政府颁布实施的，主要用于跟美国做生意的公司。它只是一个签名系统，而且美国不提倡使用任何削弱政府窃听能力的加密软件。Hash签名是最主要的数字签名方法，跟单独签名的RSA数字签名不同，它是将数字签名和要发送的信息捆在一起，所以更适合电子商务。 4.数字时间戳技术。在电子商务交易的文件中，时间是十分重要的信息，是证明文件有效

性的主要内容。在签名时加上一个时间标记，即有数字时间戳(Digita Timestamp)的数字签名方案：验证签名的人或以确认签名是来自该小组，却不知道是小组中的哪一个人签署的。指定批准人签名的真实性，其他任何人除了得到该指定人或签名者本人的帮助，否则不能验证签名。 时间戳(Time-Stamp)是一个经加密后形成的凭证文档，包括三个部分。一是需加时间戳的文件的摘要(Digest)，二是DTS收到文件的日期与时间，三是DIS数字签名。 时间戳产生的过程是：用户首先将需要加时间的文件用HASH编码加密形成摘要，然后将该摘要发送到DTS，DTS在加入了收到文件摘要的日期和时间信息后再对该文件加密(数字签名)，然后送回用户。书面签署文件的时间是由签署人自己写上的，数字时间则不然，它是由认证单位DIS来加的，以DIS收到文件的时间为依据。 