电子商务交易过程中的网络安全技术电子商务师考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_645578.htm 本文分析了电子商务首要的安全要素，以及将面临的一系列安全问题,并从网络平台和数据传输两个方面完整地介绍了一些相关的安全技术,通过它们来消除电子商务活动中的安全隐患。 一、引言 随着信息技术和计算机网络的迅猛发展，基于Internet的电子商务也随之而生，并在近年来获得了巨大的发展。电子商务作为一种全新的商业应用形式，改变了传统商务的运作模式，极大地提高了商务效率，降低了交易的成本。然而，由于互联网开放性的特点，安全问题也自始至终制约着电子商务的发展。因此，建立一个安全可靠的电子商务应用环境，已经成为影响到电子商务发展的关键性课题。 二、电子商务面临的安全问题 1.信息泄漏。在电子商务中主要表现为商业机密的泄露，包括两个方面:一是交易双方进行交易的内容被第三方窃取；二是交易一方提供给另一方使用的文件被第三方非法使用。 2.信息被篡改。电子的交易信息在网络上传输的过程中，可能被他人非法修改、删除或被多次使用，这样就使信息失去了真实性和完整性。 3.身份识别。身份识别在电子商务中涉及两个方面的问题：一是如果不进行身份识别，第三方就有可能假冒交易一方的身份，破坏交易、败坏被假冒一方的信誉或盗取交易成果；二是不可抵赖性，交易双方对自己的行为应负有一定的责任，信息发送者和接受者都不能对此予以否认。进行身份识别就是防止电子商务活动中的假冒行为和交易被否认的行为。 4.信息破坏。一是网络传输的可靠

性，网络的硬件或软件可能会出现问题而导致交易信息丢失与谬误；二是恶意破坏，计算机网络本身遭到一些恶意程序的破坏，例如病毒破坏、黑客入侵等。 三、电子商务的安全要素 1.有效性。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此，要对一切潜在的威胁加以控制和预防，以保证贸易数据在确定的时刻和地点是有效的。 2.机密性。电子商务是建立在一个较为开放的网络环境上的，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。解决数据机密性的一般方法是采用加密手段。 3.完整性。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方的差异。此外，数据传输过程中的丢失、重复或传送的次序差异也会导致贸易各方的不同。因此，要预防对随意生成、修改和删除，同时要防止数据传送过程中的丢失和重复并保证传送次序的统一。 4.不可抵赖性。电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是进行交易所期望的贸易方这一问题则是保证电子商务顺利进行的关键。在交易进行时，交易各方必须附带含有自身特征、无法由别人复制的信息，以保证交易后发生纠纷时有所对证。 四、电子商务采用的主要安全技术手段 1.防火墙技术。防火墙就是在网络边界上建立相应的网络通信监控系统，用来保障计算机网络的安全，它是一种控制技术，既可以是一种软件产品，又可以制作或嵌入到某种硬件产品中。所有来自Internet的传输信息或发出的信息都必须经过防火墙。这样，防火墙就起到了保护诸如电子邮件、文件传输、远程登录、在特定的系统间进行信息交

换等安全的作用。实现防火墙技术的主要途径有：分组过滤和代理服务。分组过滤：这是一种基于路由器的防火墙。它是在网间的路由器中按网络安全策略设置一张访问表或黑名单，即借助数据分组中的IP地址确定什么类型的信息允许通过防火墙，什么类型的信息不允许通过。防火墙的职责就是根据访问表(或黑名单)对进出路由器的分组进行检查和过滤。这种防火墙简单易行，但不能完全有效地防范非法攻击。目前，80%的防火墙都是采用这种技术。代理服务：是一种基于代理服务的防火墙，它的安全性高，增加了身份认证与审计跟踪功能，但速度较慢。所谓审计跟踪是对网络系统资源的使用情况提供一个完备的记录，以便对网络进行完全监督和控制。通过不断收集与积累有关出入网络的完全事件记录，并有选择地对其中的一些进行审计跟踪，发现可能的非法行为并提供有力的证据，然后以秘密的方式向网上的防火墙发出有关信息如黑名单等。防火墙虽然能对外部网络的功击实施有效的防护，但对网络内部信息传输的安全却无能为力，实现电子商务的安全还需要一些保障动态安全的技术。2.数据加密技术。在电子商务中，数据加密技术是其他安全技术的基础，也是最主要的安全措施，贸易方可根据需要在信息交换的阶段使用。目前，加密技术分为两类，即对称加密和非对称加密。 (1)对称加密。对称加密又称为私钥加密。发送方用密钥加密明文，传送给接收方，接收方用同一密钥解密。其特点是加密和解密使用的是同一个密钥。使用对称加密方法将简化加密的处理，每个贸易方都不必彼此研究和交换专用的加密算法，而是采用相同的加密算法并只交换共享的专用密钥。比较著名的对称加密算法是：美国国家标准

局提出的DES(DataEncryption Standard，数据加密标准)。对称加密方式存在的一个问题是无法鉴别贸易发起方或贸易最终方。因为贸易双方共享同一把专用密钥，贸易双方的任何信息都是通过这把密钥加密后传送给对方的。 (2)非对称加密。非对称加密又称为公钥加密。公钥加密法是在对数据加解密时，使用不同的密钥，通信双方各具有两把密钥，即一把公钥和一把密钥。公钥对外界公开，私钥自己保管，用公钥加密的信息，只能用对应的私钥解密。同样地，用私钥加密的数据只能用对应的公钥解密。RSA(即Rivest，ShamirAdleman)算法是非对称加密领域内最为著名的算法。贸易方利用该方案实现机密信息交换的基本过程是：贸易方甲生成一对密钥并将其中的一把作为公开密钥向其他贸易方公开，得到该公开密钥的贸易方乙使用该密钥对机密信息进行加密后再发送给贸易方甲；贸易方甲再用自己保存的另一把私有密钥对加密后的信息进行解密。贸易方甲只能用其私有密钥解密由其公开密钥加密后的任何信息。为了充分发挥对称和非对称加密体制各自的优点，在实际应用中通常将这两种加密体制结合在一起使用，比如：利用DES来加密信息，而采用RSA来传递对称加密体制中的密钥。 3.数字签名技术。仅有加密技术还不足以保证商务信息传递的安全，在确保信息完整性方面，数字签名技术占据着不可替代的位置。目前数字签名的应用主要有数字摘要、数字签名和数字时间戳技术。 (1)数字摘要。数字摘要是对一条原始信息进行单向哈希(Hash)函数变换运算得到的一个长度一定的摘要信息。该摘要与原始信息一一对应，即不同的原始信息必然得到一个不同的摘要。若信息的完整性遭到破坏，信息就无法通过原始摘要信息的验

证，成为无效信息，信息接收者便可以选择不再信任该信息。(2)数字签名。数字签名实际上是运用公私钥加密技术使信息具有不可抵赖性，其具体过程为：文件的发送方从文件中生成一个数字摘要，用自己的私钥对这个数字摘要进行加密，从而形成数字签名。这个被加密的数字签名文件作为附件和原始文件一起发送给接收者。接收方收到信息后就用发送方的公开密钥对摘要进行解密，如果解出了正确的摘要，即该摘要可以确认原始文件没有被更改过。那么说明这个信息确实为发送者发出的。于是实现了对原始文件的鉴别和不可抵赖性。(3)数字时间戳。数字时间戳技术或DTS是对数字文件或交易信息进行日期签署的一项第三方服务。本质上数字时间戳技术与数字签名技术如出一辙。加盖数字时间戳后的信息不能进行伪造、篡改和抵赖，并为信息提供了可靠的时间信息以备查用。 五、小结 本文分析了目前电子商务领域所使用的安全技术：防火墙技术，数据加密技术，数字签名技术，以及安全协议，指出了它们使用范围及其优缺点。但必须强调说明的是，电子商务的安全运行，仅从技术角度防范是远远不够的，还必须完善电子商务立法，以规范飞速发展的电子商务现实中存在的各类问题，从而引导和促进我国电子商务快速健康发展。 