电子商务的加密技术及安全模型设计分析电子商务师考试
 一、现有电子商务体系及安全问题 电子商务是以网络为平台，以信息技术为手段，以经济效益为中心的现代化商业运转模式，目标是实现商务活动的网络化、自动化与智能化，电子商务改变了企业的经营理念、管理方式和支付手段。网络营销、网上采购和电子支付成为企业经营的必要环节，极大地缩短了企业生产周期，降低了生产成本，增强了企业对市场的反应能力。它是基于C/S(即客户端和服务器Client/Server)模式下的交易模型，分为服务器端和客户端。客户端所下的订单通过网络进行传输，在服务器端进行信息确认后进行交易，再由物流系统进行配货。 这个体系由个人用户系统、网络系统、服务端系统及物流系统组成。物流系统是实物运输，所以是安全的。其他几个部分都存在着不安全的因素。作为服务端的服务商(如银行系统),投入了大量的资金和人力，应用了先进的技术(如防火墙、访问控制、入侵检测及漏洞评估等)以保障电子商务的安全。一直以来服务器端的安全都得到了足够的重视,随着电子商务的迅速发展与日益完善,服务器端不安全的可能性越来越小。 根据CCNIC一年一度的中国互联网发展统计报告,电子商务中的安全事件包括用户的主机被植入木马,账号和密码被窃取.冒充用户进行交易.由于用户的错误操作导致的安全问题.由于用户自身安全意识的不足,在交易过程中被假冒、欺骗(如假网站)、传输过程中信息被窃取、篡改、伪造等等。可以看到,在上述的安全威胁中,窃听、陷门和特洛伊木马、病

毒等威胁及诸如存在于数据链路层网络和服务器端的安全威胁,都是针对客户端和数据传输过程的。 二、数据加密技术 数据加密是所有数据安全技术的核心,在计算机网络环境下很难做到对敏感性数据的隔离,较现实的方法是设法做到即使攻击者获得了数据,但仍无法理解其包含的意义,以便达到保密的目的。所谓加密就是通过密码算法对数据进行转化,使之成为不拥有正确密钥的任何人都无法读懂的报文。而这些以无法读懂的形式出现的数据一般被称为密文。为了读懂报文,密文必须重新转变为它的最初形式明文,而含有用来以数学方式转换报文的双重密码就是密钥。在这种情况下即使一则信息被截获并阅读,这则信息也是毫无利用价值的。而实现这种转化的算法标准,据不完全统计,到现在为止已经有近200多种。 按照国际上通行的惯例,将这近200种方法按照双方收发的密钥是否相同的标准划分为两大类:一种是私钥加密算法(也称对称加密算法),其特征是收、发双方使用相同的密钥,即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有:美国的DES及其各种变形,比如3DES、GDES、NewDES和DES的前身Lucifer.欧洲的IDEA.日本的FEALN、LOKI91、Skip2jack、RC4、RC5，以及以替换密码和轮换密码为代表的古典密码等。另外一种是公钥加密算法(也叫非对称加密算法)。其特征是收、发双方使用的密钥互不相同,而且几乎不可能从加密密钥推导解密密钥。比较著名的公钥密码算法有:RSA、背包密码、McEliece密码、DiffeHellman、Rabin、OngFiatShamir、零知识协议、椭圆曲线(ECC)、EIGamal算法等。 加密技术是电子商务安全的基础,对称加密算法与非对称加密算法(如应用最广泛的DES、RSA、MD5几种加密算法)各有优缺点,通常结

合起来使用(即日益广泛使用的混合密码体制),以期同时获得公钥加密体制的安全优点和私钥加密体制的速度优势。 私钥加密体制和公钥加密体制的结合使用不但可以简化私钥加密体制中的密钥管理,而且能够做到对应每个明文使用一个不同的密钥(即一次一钥).由于每个密钥仅仅使用一次,即使在某一次数据传输中密钥不慎泄露,它也只影响本次交换的信息,对保障电子商务的健康发展起着越来越关键的作用。 三、个人用户终端采取的安全措施 在电子商务中,客户终端一直以来都是安全的薄弱环节。从统计的数据来看,大约有85%的电子商务安全事件都是由于终端用户的安全问题引起的,针对用户终端的不安全性，使用如下措施来加强安全性: (1)使用SSL(安全套接层)解决WEB终端的安全套接：使用户通过WEB的数据是经过加密的,如MD5用于防止篡改或伪造报文,MD5结合DES或RSA确保信息的完整性(即真伪)等。 (2)软件键盘措施:用户使用鼠标点击软件键盘对应的按键,屏蔽了一些记录用户敲击真实键盘信息的软件。 (3)验证码措施:由系统自动生成随机伪序列,每一次的验证码不相同,可以防止重放攻击。 (4)确认体制:需要用户进行确认,这种确认可以是不同于网络的安全通道。 四、附有用户特征信息的服务器反向链接安全体系 由于终端用户引起的安全问题,并不属于电子商务中加密算法的范围,虽然采取了上述措施,以及严密的加密算法，但也不可能把用户的失误操作屏蔽掉,而终端机的安全问题也是最容易被病毒、漏洞、黑客等威胁入侵的,从而成为电子商务中最不安全的因素。这说明,需要一种更新的体制来提高客户端的安全性。在不增加用户复杂度的前提下提升安全性能,我们需要一种能够防止终端用户失误操作而导致的安全问题,这就是基于现

行加密体系的附有用户特征信息的服务器反向链接安全体系。 此方案加强了用户终端的安全性能,可以避免木马、病毒、系统漏洞、假冒网站等威胁。服务器反向链接所建立的简易操作平台应实现的功能:一是对用户透明结合了用户特征的加密过程.二是在用户终端,随机建立进程ID,防止病毒或木马对指定进程的分析和攻击.三是拒绝其他进程(除服务所需要)对其进行数据修改等操作。 这里所提到的用户特征信息,是用户自己定义的惟一的数据组合,它可以是数字、字符、逻辑等信息,用于在建立用户账户时,电子商务系统按照一定的逻辑存储在服务器端(我们假设服务器绝对安全,值得信赖)。在用户使用电子签名进行操作时,服务器端会以用户的电子签名进行身份的合法性验证,以便取出并生成随机的一次性信息进行下一步操作。这种数据只能与服务器反向链接所建立起来的应用层之间才能识别和利用。由于这种链接具有加密性和随机性,可以对操作系统漏洞、病毒、木马、假网站，以及恶意攻击免疫,这些威胁事实上对固定不变的应用程序更具有威胁性。由于该模型是由客户端请求,服务器端响应并协商参数,提供给客户端简易操作平台,再由客户端运行,服务器端全程控制的机制,所以所涉及的数学逻辑都在服务器存储并控制,这既可以防止因客户端的不安全导致的对电子商务安全的威胁,又便于集中升级和维护。在以往的交易过程中,当用户请求交易时,会向交易平台或银行系统发送交易请求,服务器响应并返回操作界面,但用户并不知道此交易界面是不是正常的,或者并不知道自己的主机是不是在正常的安全模式下面(如中木马、病毒、键盘记录器等),所以此时交易是非常危险的,账户信息很容易被窃取。 假设服务器是足够安全的,并且这种机制是不可复制

的,如果是服务器的反向链接形成的交易平台,木马、病毒、键盘记录器等威胁并不可能对这样随机产生的并且没有任何特征可言的进程或程序实行实时监控和记录,因为木马、病毒、键盘记录器等一般只记录它预先定义好的敏感信息,这就最大限度地保护了用户的交易安全。而且这种反向链接机制,可以确保用户所进行的操作都是正规的银行或交易平台里进行的。