电子商务综合辅导：电子商务及其安全技术电子商务师考试

[摘要] 电子商务的安全性是影响其成败的一个关键因素。本文讨论了电子商务应用中所存在的问题，继而对电子商务的安全性技术进行了分析，提出了一些相应措施。 [关键词] 网络安全交易安全安全技术安全措施 一、引言 电子商务的发展前景十分诱人，而其安全问题也变得越来越突出，如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和用户都十分关心的话题。 二、电子商务存在的安全问题 1.计算机网络安全 (1)潜在的安全隐患。未进行操作系统相关安全配置。不论采用什么操作系统，在缺省安装的条件下都会存在一些安全问题，只有专门针对操作系统安全性进行相关的和严格的安全配置，才能达到一定的安全程度。 (2)未进行CGI程序代码审计。网站或软件供应商专门开发的一些CGI程序，很多存在严重的CGI问题，对于电子商务站点来说，会出现恶意攻击者冒用他人账号进行网上购物等严重后果。 (3)安全产品使用不当。由于一些网络安全设备本身的问题或使用问题，这些产品并没有起到应有的作用。很多厂商的产品对配置人员的技术背景要求很高，超出对普通网管人员的技术要求，就算是厂家在最初给用户做了正确的安装、配置，但系统改动，在改动相关安全产品的设置时，很容易产生许多安全问题。 (4)缺少严格的网络安全管理制度 网络安全最重要的还是要思想上高度重视，网站或局域网内部的安全需要用完备的安全制度来保障。建立和实施严密的计算机网络

安全制度与策略是真正实现网络安全的基础。 2.商务交易安全 (1)窃取信息。由于未采用加密措施，信息在网络上以明文形式传送，入侵者在数据包经过的网关或路由器上可以截获传送的信息。通过多次窃取和分析，可以找到信息的规律和格式，进而得到传输信息的内容，造成网上传输信息泄密。 (2)篡改信息。当入侵者掌握了信息的格式和规律后，通过各种技术手段和方法，将网络上传送的信息数据在中途修改，然后再发向目的地。 (3)假冒。由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。 (4)恶意破坏。由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入网络内部，其后果是非常严重的。 三、电子商务安全技术 1.加密技术 (1)对称加密/对称密钥加密/专用密钥加密 该方法对信息的加密和解密都使用相同的密钥。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。如果进行通信的贸易方能够确保专用密钥在密钥交换阶段未曾泄露，那么机密性和报文完整性就可以通过对称加密方法加密机密信息和通过随报文一起发送报文摘要或报文散列值来实现。 (2)非对称加密/公开密钥加密 这种加密体系中，密钥被分解为一对。这对密钥中的任何一把都可作为公开密钥通过非保密方式向他人公开，而另一把则作为专用密钥加以保存。公开密钥用于对机密性的加密，专用密钥则用于对加密信息的解密。专用密钥只能由生成密钥对的贸易方掌握，公开密钥可广泛发布，但它只对应于生成该密钥的贸易方。 (3)数字摘要 该方

法亦称安全Hash编码法或MD5。采用单向Hash函数将需加密的明文“ 摘要 ”成一串128bit的密文，即数字指纹，它有固定的长度，且不同的明文摘要成密文，其结果总是不同的，而同样的明文其摘要必定一致。这摘要便可成为验证明文是否是“ 真身 ”的“ 指纹 ”了。 (4)数字签名 信息是由签名者发送的.信息在传输过程中未曾作过任何修改。这样数字签名就可用来防止电子信息因易被修改而有人作伪；或冒用别人名义发送信息；或发出（收到）信件后又加以否认等情况发生。 (5)数字时间戳 它是一个经加密后形成的凭证文档，包括三个部分：需加时间戳的文件的摘要.DTS收到文件的日期和时间.DTS的数字签名。 (6)数字凭证 数字凭证又称为数字证书，是用电子手段来证实一个用户的身份和对网络资源的访问的权限。在网上的电子交易中，如双方出示了各自的数字凭证，并用它来进行交易操作，那么双方都可不必为对方身份的真伪担心。它包含：凭证拥有者的姓名. 凭证拥有者的公共密钥.公共密钥的有效期.颁发数字凭证的单位.数字凭证的序列号.颁发数字凭证单位的数字签名。 数字凭证有三种类型：个人凭证，企业（服务器）凭证， 软件（开发者）凭证。 2.Internet电子邮件的安全协议 (1)PEM：是增强Internet电子邮件隐秘性的标准草案，它在Internet电子邮件的标准格式上增加了加密、鉴别和密钥管理的功能，允许使用公开密钥和专用密钥的加密方式，并能够支持多种加密工具。对于每个电子邮件报文可以在报文头中规定特定的加密算法、数字鉴别算法、散列功能等安全措施。 (2)S/MIME：是在RFC1521所描述的多功能Internet电子邮件扩充报文基础上添加数字签名和加密技术的一种协议，目的是在MIME上定义安全服务措施

的实施方式。 (3)PEM-MIME：是将PEM和MIME两者的特性进行了结合。 3.Internet主要的安全协议 (1)SSL:是向基于TCP/IP的客户/服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息机密性等安全措施。该协议通过在应用程序进行数据交换前交换SSL初始握手信息来实现有关安全特性的审查。在SSL握手信息中采用了DES、MD5等加密技术来实现机密性和数据完整性，并采用X.509的数字证书实现鉴别。 (2)S-HTTP：是对HTTP扩充安全特性、增加了报文的安全性，它是基于SSL技术的。该协议向WWW的应用提供完整性、鉴别、不可抵赖性及机密性等安全措施。 (3)STT： STT将认证和解密在浏览器中分离开，用以提高安全控制能力。 (4)SET：主要文件是SET业务描述、SET程序员指南和SET协议描述。SET 1.0版已经公布并可应用于任何银行支付服务。它涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数据认证、数据签名等。 SET规范明确的主要目标是保障付款安全，确定应用之互通性，并使全球市场接受。 