电子商务员考试辅导：电子商务安全技术电子商务师考试
 随着Internet的发展，电子商务已经逐渐成为人们进行商务活动的新模式。越来越多的人通 过Internet进行商务活动。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。 电子商务的一个重要技术特征是利用IT技术来传输和处理商业信息。因此，电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。采集者退散 * 计算机网络安全的内容包括：计算机网络设备安全、计算机网络系统安全、数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全性为目标。 * 商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，如何保障电子商务过程的顺利进行。即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。 计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起。没有商务交易安全保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。 计算机网络安全 1.计算机网络的潜在安全隐患 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。千万不要以为操作系统缺省安装后，再配上很强的密码系统就算作安全了。网络软件的漏洞和“后门”是进行网络攻击的首选目标。 未进行CGI程序代码审计 如果是通用的CGI问题，防范起来还稍微容易一些，但是对于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。 拒绝服务（DoS，Denial of Service）攻击 随着电子商务的兴起，对网站的实时性要求越来越高，DoS或DDoS对网站的威胁越来越大。以网络瘫痪为目标的袭击效果比任何传统的恐怖主义和战争方式都来得更强烈，破坏性更大，造成危害的速度更快，范围也更广，而袭击者本身的风险却非常小，甚至可以在袭击开始前就已经消失得无影无踪，使对方没有实行报复打击的可能。今年2月美国“雅虎”、“亚马逊”受攻击事件就证明了这一点。 安全产品使用不当 虽然不少网站采用了一些网络安全设备，但由于安全产品本身的问题或使用问题，这些产品并没有起到应有的作用。很多安全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，但一旦系统改动，需要改动相关安全产品的设置时，很容易产生许多安全问题。 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.计算机网络安全体系 一个全方位的计算机网络安全体系结构包含网络的物理安全、访问控制安全、系统安全

、用户安全、信息加密、安全传输和管理安全等。充分利用各种先进的主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、安全审计技术、安全管理技术、系统漏洞检测技术、黑客跟踪技术，在攻击者和受保护的资源间建立多道严密的安全防线，极大地增加了恶意攻击的难度，并增加了审核信息的数量，利用这些审核信息可以跟踪入侵者。 在实施网络安全防范措施时：* 首先要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；* 其次要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，并及时加以修补；* 从路由器到用户各级建立完善的访问控制措施，安装防火墙，加强授权管理和认证；* 利用RAID5等数据存储技术加强数据备份和恢复措施；* 对敏感的设备和数据要建立必要的物理或逻辑隔离措施；* 对在公共网络上传输的敏感信息要进行强度的数据加密；* 安装防病毒软件，加强内部网的整体防病毒措施；* 建立详细的安全审计日志，以便检测并跟踪入侵攻击等。 网络安全技术是伴随着网络的诞生而出现的，但直到80年代末才引起关注，90年代在国外获得了飞速的发展。近几年频繁出现的安全事故引起了各国计算机安全界的高度重视，计算机网络安全技术也因此出现了日新月异的变化。安全核心系统、VPN安全隧道、身份认证、网络底层数据加密和网络入侵主动监测等越来越高深复杂的安全技术极大地从不同层次加强了计算机网络的整体安全性。安全核心系统在实现一个完整或较完整的安全体系的同时也能与传统网络协议保持一致。它以密码核心系统为基础，支持不同类型的安全硬件产品，屏蔽安全硬件以变化对上层应用的影响

，实现多种网络安全协议，并在此之上提供各种安全的计算机网络应用。 互联网已经日渐融入到人类社会的各个方面中，网络防护与网络攻击之间的斗争也将更加激烈。这就对网络安全技术提出了更高的要求。未来的网络安全技术将会涉及到计算机网络的各个层次中，但围绕电子商务安全的防护技术将在未来几年中成为重点，如身份认证、授权检查、数据安全、通信安全等将对电子商务安全产生决定性影响。 商务交易安全 当许多传统的商务方式应用在Internet上时，便会带来许多源于安全方面的问题，如传统的贷款和借款卡支付/保证方案及数据保护方法、电子数据交换系统、对日常信息安全的管理等。电子商务的大规模使用虽然只有几年时间，但不少公司都已经推出了相应的软、硬件产品。由于电子商务的形式多种多样，涉及的安全问题各不相同，但在Internet上的电子商务交易过程中，最核心和最关键的问题就是交易的安全性。一般来说商务安全中普遍存在着以下几种安全隐患：窃取信息 由于未采用加密措施，数据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。 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。这种方法并不新鲜，在路由器或网关上都可以做此类工作。 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。 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。 因此，电子商务的安全交易主要保证以下四个方面：信息保密性 交易中的商务信息均有保密的要求。如信用卡的账号和用户名等不能被他人知悉，因此在信息传播中一般均有加密的要求。 交易者身份的确定性 网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先要能确认对方的身份，对商家要考虑客户端不能是骗子，而客户也会担心网上的商店不是一个玩弄欺诈的黑店。因此能方便而可靠地确认对方身份是交易的前提。 不可否认性 由于商情的千变万化，交易一旦达成是不能被否认的。否则必然会损害一方的利益。因此电子交易通信过程的各个环节都必须是不可否认的。 不可修改性 交易的文件是不可被修改的，否则也必然会损害一方的商业利益。因此电子交易文件也要能做到不可修改，以保障商务交易的严肃和公正。 电子商务交易中的安全措施 在早期的电子交易中，曾采用过一些简易的安全措施，包括：* 部分告知（Partial Order）：即在网上交易中将最关键的数据如信用卡号码及成交数额等略去，然后再用电话告之，以防泄密。* 另行确认（Order Confirmation）：即当在网上传输交易信息后，再用电子邮件对交易做确认，才认为有效。 此外还有其它一些方法，这些方法均有一定的局限性，且操作麻烦，不能实现真正的安全可靠性。 近年来，针对电子交易安全的要求，IT业界与金融行业一起，推出不少有效的安全交易标准和技术。 主要的协议标准有：* 安全超文本传输协议（S－HTTP）：依靠密钥对的加密，保障Web站点间的交易信息传输的安全性。* 安全套接层协议（SSL）：由Netscape公司提出的安全交易协议，提供加密、认证服务和

报文的完整性。SSL被用于Netscape Communicator和Microsoft IE浏览器，以完成需要的安全交易操作。 * 安全交易技术协议（STT，Secure Transaction Technology）：由Microsoft公司提出，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。Microsoft在Internet Explorer中采用这一技术。 * 安全电子交易协议（SET，Secure Electronic Transaction） 1996年6月，由IBM、MasterCard International、Visa International、Microsoft、Netscape、GTE、VeriSign、SAIC、Terisa就共同制定的标准SET发布公告，并于1997年5月底发布了SET Specification Version 1.0，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 2.0预计今年发布，它增加了一些附加的交易要求。这个版本是向后兼容的，因此符合SET 1.0的软件并不必要跟着升级，除非它需要新的交易要求。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。 所有这些安全交易标准中，SET标准以推广利用信用卡支付网上交易，而广受各界瞩目，它将成为网上交易安全通信协议的工业标准，有望进一步推动Internet电子商务市场。相关链接：电子商务主要的安全技术 