电子商务综合辅导：电子商务的应用与安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/264/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_264026.htm 伴随着Internet的蓬勃发展，电子商务正以自身高效、低成本的优势，逐步成为新兴的经营模式和理念，其涉及的领域从银行、外贸、证券市场到贴近我们每个人的日常购物。首先我们看看电子商务应用的具体例子。 在过去十年中，新加坡通过“ 国家IT计划 ”进行了IT方面的基础建设。在1989年，新加坡就是世界上第一个100%实现ISDN的国家。通过IT的基础设施，新加坡实施了一系列著名的电子商务系统。TradeNet应用于贸易，连接18个与贸易文件有关的政府部门、港口和民航。商家通过TradeNet全天候将电子报关单传送到贸易发展委员会的主机，在15分钟内即可得到报关批复。据估计，TradeNet可以每年为新加坡节约10亿美元。 美国的Security First Network Bank1995年成为当时世界上唯一的网上银行。营业之初，该银行有4000个帐号，开户条件是超过100美元的存款、地址及社会安全号码。在欧盟银行的网上业务中，世界各地的用户可以使用各种币种的银行服务。法国、澳大利亚、巴西、美国也都出现了提供全面Internet服务的银行。据估计传统银行的费用比率为60%，而网上银行是15%～20%。IT行业的一些著名企业也参与到网上银行中，IBM Global Network早已开始处理大量的电子商务信息，IBM还同美国和加拿大的17家主要银行组成Integrion金融网络，该网络拥有六千万家庭用户，占据了北美银行个人用户市场的一半，其功能也从资金的转移和支付，逐步涵盖贷款申请、股票期货交易等领域

。Integrion的用户可以使用任何Internet浏览软件或个人理财软件访问网络，使用非常方便。 在证券领域，美国的NASDAQ完全采用计算机系统竞价和进行实时交易，现已成为仅次于纽约证交所的世界第二大证券市场。 这些让我们感到了电子商务的波澜壮阔之势，一场生活和技术的重大变革正在我们身边发生。电子商务的优势是明显的，但是其进一步的发展则面临以下的一些问题： 1.易用性。从键盘、软件到触摸式输入已经简化了电子商务的应用。今后电子商务客户端的输入方式更注重人的直觉，并具备自然语言识别、手写输入、虚拟现实和各语种的同步翻译等功能。 2.网络技术。网络技术要实现多种设备、软件的无缝连接，通讯技术将多种通讯工具与计算机实现连接；路由器等网络设备要支持更大容量的数据在更短时间内实现通讯，成本则大大降低；用户只要使用简单的点击操作就可安全地进行交易。 3.设备处理能力。智能卡、网络访问设备的处理能力要极大地提高。智能卡不仅要有存储个人信息的能力，还要有PC的一些功能，如下载电子货币；网络访问设备将可以访问远程服务器上的应用软件。 4.应用工具。应用工具要根据个人的喜好，收集过滤Internet的信息，提供最好的商务参考。数据挖掘工具和模型要更快、更准确地处理大量的数据，为用户寻找新的商机。 5.中小型企业的参与。当今的电子商务包含的范围还主要是大银行和企业，中小企业是被排斥在外的。积极将中小企业包容进来，扩大电子商务的应用范围是很重要的。 电子商务的安全性 任何在Internet上开展业务的机构都必须采取积极的步骤，确保系统有足够的安全措施防止机密信息泄露和非法侵入所造成的损失。但Internet本身就是基于开放

思想设计并逐步发展起来的。要想在Internet上实现绝对安全是困难的。Internet上实现电子商务面临的风险主要来自机密关键数据安全及电子交易安全两方面，具体到技术细节包含以下四个方面。 1.数据的私有性和安全性 如果不采用特别的保护措施，包括电子邮件等在Internet中开放传输的数据都可能被第三者监视和阅读。考虑到巨大的传输量和难以计数的传输途径，想任意窃听一组数据传输是不可能，但是一些设置在Web服务器的黑客程序却可以查找和收集特定类型的数据。这些数据包括信用卡、存款的帐号和相应的口令。同时因为Internet的开放性设计，数据私有性和安全性还包括数据传输之外的问题，例如连入Internet的数据存储网络驱动器的安全性，所以任何存储在Web服务器上的数据必须采取保护措施。 2.数据的完整性 由于Internet的开放体系，如果具备了特定的知识和工具完全可以更改传输中的数据。同时要采取适当的存取访问控制，以保证数据存取系统的安全。在电子商务中务必保存数据最初的格式和内容。 3.认证 电子商务的具体实现中，首先要确认当前的通讯、交易和存取要求是合法的。例如Internet中的计算机系统的身份是其由IP地址确认的。黑客通过IP欺骗，使用虚假的IP地址，从而达到隐瞒自己身份盗用他人身份的目的。在日常电子邮件的使用中可以很容易地发匿名邮件，或者使用不真实的邮件用户名。因此，在电子商务中必须建立严格的身份认证机制以确保参加交易各方的身份真实有效。 4.不可否认性 不可否认主要包含数据的原始记录和发送记录，确认数据已经完成发送和接收，防止接收用户更改原始记录，防止用户在已经收到数据以后否认收到数据，并拖延自己的下一步工作。为了保证交易过

程的可操作性，必须采取可靠的方法确保交易过程的真实性，保证参加电子交易的各方承认交易过程的合法性。简言之，在Internet上实现电子商务面临的任务：(1)私有性，即保证只有发送者和接收者可以接触到信息；(2)完整性，即信息在传输过程中未经任何改动；(3)身份认证，即接收方可以确信信息来自发信者，而不是第三者冒名发送，发送方可以确信接收方的身份是真实的，而不至于发往与交易无关的第三方；(4)不可否认性，在交易数据发送完成以后，双方都不能否认自己曾经发出或接收过信息。在我们把银行的内部网络接入Internet以后，相应地增加了许多可以访问银行内部网络的节点。从理论上讲从世界各个地方都可以实现对银行内部网络的访问，这对银行计算机网络的数据和系统的安全性提出了更高的要求。这些要求我们采取严密的访问控制，禁止非法访问。电子商务中威胁计算机网络安全的因素有：破坏、更改或者盗窃数据；公开机密信息；计算机系统崩溃；公共形象(如主页)被污损等等。造成这些损失的因素有：黑客，公司内部职员，电子商务软件中的Bug，商业间谍等。电子商务面临的上述问题主要是由对系统的非法入侵造成的。首先是网络黑客，他们通过发现Web服务器、操作系统或者主页部件在配置方面的漏洞，攻击网络系统。其次是内部入侵，这主要是由企业IT部门的员工造成的，保护网络的物理安全(如主控机房)及严格的口令管理制度是防范该类问题的关键。还有恶意代码(如计算机病毒)，它们在企业的传播会给电子商务系统造成严重的损失。另外值得关注的是计算机系统本身的问题，例如由于电源造成的系统宕机，以及广域网络的通讯，这些都会直接造成服务的突然中止，影响电子商

务的形象。我们还应关注系统管理方面的问题，有时电子商务出现的问题既非黑客也非系统本身的毛病，而是源于对敏感数据处理不善或者是安全系统(如防火墙)的不正确配置。用户的身份认证是计算机系统安全的基础工作，数字签名加密等技术在这里可以充分起到作用。 电子商务系统的保护方法主要有以下几种。 1.用户识别文件和口令 许多互联网研究机构都将私有性和保密性列为电子商务的首要问题。用户识别文件和口令在Internet之前的大型主机时代，就已经是安全的有效实现方法。在电子商务中，可以采用限制错误登录的次数、跟踪错误访问的办法，保护用户识别文件和口令的安全。 2.数据加密 因为开放的Internet本身并不提供安全的传输路径，所以在电子商务中必须采用数据加密，保证帐户和交易数据的安全。超文本安全传输协议S-HTTP和安全套接层协议SSL是在Web端与浏览器端实现加密的应用技术，这两种技术使得数据对于没有密钥的人是毫无用处的，并且易于在商业领域应用。 3.认证授权和数字认证 CA是认证授权中心(Certificate Authority)的简称，它和数字认证(Digital Certificate)一起在电子商务的身份认证、不可否认性、数据私有加密钥管理方面起着主要的作用。CA是交易双方都信任的第三方机构，由它来证明参加交易各方的身份。在交易过程中CA将自己的数字签名附在所有的传送消息和公共密钥上。数字认证指的是附有CA签名的消息。参加交易方都必须信任CA，CA在交易前确认所有各方的身份，可见CA的主要任务在于管理而不是技术。CA在电子商务中，起着法律仲裁的作用，其工作相当于确定用户的数字签名能否得到法律的认可。但是只有在CA拥有了仲裁权以后，这种认证才有法律效

应。在电子商务的发展过程中，CA的重要作用正在日益显现。 认证中心与加密技术相结合产生了一种完全适合电子商务的加密技术安全电子交易SET。安全套接层SSL加密方法仅仅是实现了传输加密和数据完整性，相当于在两台计算机之间建立一个安全的通道。而电子商务的要求则更高一点，例如用户通过与商家连网，进行支付和交易时，商家不应该知道用户的帐户等信息，显然SSL协议不能防止商家的欺诈。另外SSL协议也不保证交易各方身份的真实性和不可否认性。SET的架构是通过几个成员所共同组成的，各个成员可以很好地模拟实际电子商务操作的角色，这些成员分别是电子钱包(Electronic Wallet)、商户服务器(Merchant Server)、支付网关(Payment Gateway)和认证中心(Certification Authority)。SET通过认证中心和认证签名确认交易各方的真实身份，利用数字签名保证交易的不可否认性。SET的技术特点还有： 1.对订单信息和支付信息进行双重签名，这样商家只能得到订单信息，银行只知道支付信息； 2.采用信息摘要技术保证了交易的完整性； 3.采用公钥体系和密钥体系结合进行加密，而SSL只采用了公钥体系。\ 图1 与SSL相比，SET是在应用层上实现了数据的加密和完整性。SET的应用模式如图1所示。 SET的购物模式如图2所示。 图2 SET已经成为国际公认的Internet电子商务的安全标准，非常详细地反映了电子交易各方之间存在的各种关系。目前，一些厂商有专门的软件产品与SET的各个角色相对应。 4.虚拟专用网（VPN） 虚拟专用网是利用Internet公用网络，通过隧道协议和安全方法传输企业专用数据的技术。虚拟专用网在传送数据前将其加密，在接收端进行解密，它的特点是不仅加密数据，而且加密接收双方的

网络地址。同时VPN的用户验证方法也提供了更高一级的远程访问安全性。 5.路由器和防火墙 路由器是在Internet上确定数据包下一个网络传输地址的网络设备，可能是专用的硬件设备，也可能是一个软件。防火墙是企业专用网和Internet公共网的连接点，控制来往的数据流，对受到的攻击进行登录、报告和报警。如果路由器和防火墙配置得当，可以有效防范非法用户。 6.病毒防范 很多潜在的恶意代码可以直接从Internet下载，并在网络上快速传播。 7.备份和错误恢复 备份可以减轻任何一种系统错误带来的损失。硬件备份包括RAID与磁盘系统、不间断电源、服务器阵列和恢复技术。 8.系统的物理安全 9.实施规划和方法 技术上先进的系统如果不能采用严格的实施规划，也无法发挥应有的效力。实施规划是在整个企业范围内，对内、外部用户访问数据文件进行限制，确定企业计算机系统的拓朴结构及关键数据的放置。在企业级的系统中，从硬件到软件，从操作系统到数据库，涉及各种各样的系统。应用的复杂性也在不断增加，问题也越来越多。如不同操作系统之间的资源共享，公共密钥的集中管理等。对于这种情况可以采取管理器/代理器的结构对系统安全进行统一管理。其中代理器是运行在不同平台上的软件引擎，不同的引擎将它负责的安全信息传输到管理器上。管理器收集代理器传来的信息，并进行汇总，然后与管理员的指令初稿相比较，检查安全状况。在这种模式下，只要更改系统的配置要求就可以适应系统结构、规模的变化，从而实现了系统安全的统一管理。 电子商务的影响 电子商务在改变我们生活方式的同时，也会改变我们的一些观念，例如货币的表现形式，怎样衡量企业的资产。在电子商务时代，企

业的价值不仅体现在它的资产上，而且更多地体现在它所联系的客户群的多少，它的影响力有多大。企业的智力资源和信息是其财富的核心。从事电子商务的企业会在客户方面投入大量精力，以维持良久稳定的关系，企业对客户的要求要做出即时的反应。可见在电子商务时代，在技术进步的背后是人力的更大支出。 在谈到在电子商务方面我们应该采取哪些对策时，首先要明确电子商务是政府行为还是企业行为。新加坡政府制定了“ 国家IT计划 ”，在电子商务方面的投入大约是20亿美元，今后还会增加，这显然是政府行为。美国政府提出了“ 下一代互联网计划 ”以领导基础设施的改进工作。在电子商务的具体实施方面，则主要是通过如IBM等IT行业的龙头企业，通过其技术推广和市场活动进行，因此美国在电子商务方面是政府行为和企业行为相结合，更多是企业行为。而企业行为之所以能够起到主导作用，主要是因为这些企业有着强大的技术创新能力和雄厚的资金支持。同时在IT行业同传统产业如银行业的联合中，避免了重复建设和不兼容等问题。在我国的IT行业中还没有技术、资金如此强大的企业，所以以IT行业为主导的电子商务建设模式难以适用于国内。在我国的电子商务发展过程中，应更多的是政府行为。 当前在WTO内部，美国和欧盟的主要矛盾就是电子商务问题，美国试图以自己在电子商务领域的竞争优势获得经济利益。最近欧盟的专业部门还就美国在线和时代华纳的合并专门开会研究对策。现在美国和欧盟在电子商务领域的争执，可能就是不久的将来我国和WTO中发达国家的讨论焦点。银行作为电子商务的核心部门，受到电子商务的影响最大，在加入WTO后，金融业要逐步地开放，我国银行业如何面

临这些挑战和机遇是应引起高度重视的。根据我国的金融体制，可以考虑把银行业作为实现电子商务的切入点。 电子商务的法律和规划工作，例如规范电子商务中各个环节的行为，网上银行的监管工作如何实施等，应及时进行，以免被动。 在技术方面，加快开发自己的电子商务软件是首要任务。由于美国在密钥体制上对中国限制出口56位以上的软件，因此我们的开发可以在应用层上进行。同时欧洲一些软件公司，如德国BROKAT公司的相应产品值得注意。 100Test 下载频道开通，各类考试题目直接下载。详细请访问
www.100test.com