第 5 章　电子商务安全

知识点

- 电子商务安全的基本概念
- 电子商务交易中的安全技术

难点

- 电子商务安全及其重要性
- 电子商务安全解决方案

要求

熟练掌握以下内容：

- 电子商务安全的主要问题和主要威胁
- 电子商务安全及其重要性
- 电子商务交易中的安全技术
- 数字证书与认证中心
- 电子商务的安全协议与安全解决方案

了解以下内容：

- 电子商务安全的主要问题

5.1　电子商务安全概述

随着电子商务的飞速发展，电子商务的规模、范围和地域的扩大以及参与人数的增加，其安全问题已成为人们关注的焦点，成为制约电子商务发展的主要环节。电子商务是建立在网络基础上的，Internet 网络的开放性，使电子商务活动面临着种种威胁，由此提出了相应的安全控制要求。

电子商务安全问题涉及的范围非常广，包括商家、客户等实体的安全，涉及国家法律、诚信体系等各个方面。

5.1.1　电子商务安全的主要问题

电子商务安全是指企业信息的安全和客户交易的安全，是网上交易各方相互信任的基础。电子商务的安全主要包括以下几个方面的问题。

1. 电子商务各环节的安全

对电子商务活动的环节进行分析，如果能保证电子商务活动各个环节的安全，就能保证整个电子商务活动的安全。

电子商务活动的主要环节包括：建立电子商务网站，客户上网浏览选择，客户下订单、支付，商家对客户订单的确认、处理，商家向客户发货、售后服务等。这些环节中的安全问题包括：信息

的准确、不被篡改，商家及客户身份的认证，客户敏感信息不被泄漏、盗用等。

2. 电子商务安全措施

电子商务安全措施主要分为物理安全措施和逻辑安全措施。

（1）物理安全措施。物理安全措施是采用物理设备实现安全的措施。例如，警铃、保卫人员、防火门、防盗门及保险柜等。

（2）逻辑安全措施。逻辑安全措施是采用非物理设备实现安全的措施。例如，加密、数字签名、数字时间戳、电子商务安全协议等。

3. 电子商务安全核心

电子商务安全的核心主要包括：保密性、完整性、即需性、有效性、真实性、可靠性和不可抵赖性等方面。

（1）保密性。保密性是指敏感信息在存储、传输和处理过程中，不被窃取和泄漏。电子商务安全的一大威胁就是敏感的商业信息或个人信息（包括信用卡号、密码等信息）被泄漏。要保证信息的保密性，就要防止黑客侵入系统，对商务机密要进行加密处理，再进行网络传输。

（2）完整性。完整性包括信息在存储中不被篡改和破坏，以及在传输过程中收到的信息和原发送信息的一致性。保证信息的完整性就要防止数据的丢失、重复及保证传送次序的一致。信息的完整性要求系统能够识别信息是否被篡改或破坏，决定贸易各方的交易能否顺利完成，甚至造成纠纷。保证各种数据的完整性是电子商务应用的基础。

（3）即需性。即需性是指在客户需要商业信息或服务时，能及时获得、保证不被拒绝。参与电子交易各方能否及时进行数据交换，关系到电子商务的正常运行。例如，一个网上股票交易系统如果不能将股市行情及时通报给股民，这样的系统不会有人使用；如果客户要求的服务被拒绝，同样会失去客户。

（4）有效性。有效性是指在开展电子商务时，要保证电子单证和电子交易信息的有效。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交易的有效性。接收方必须能证实接收的数据是原发送方发出的；原发送方也必须保证只有指定的接收方才能接收。

（5）真实性。真实性是指参与交易双方的身份是确实存在的，不是假冒的。例如，甲、乙两公司进行网上交易，交易双方必须确认对方身份是否真实，商家要排除客户不是骗子：客户要确认商家不是假店、有信誉，才能建立彼此信任的交易关系。另外，还要能识别是否有第三方在假冒交易对象。

（6）可靠性。可靠性是指计算机及网络系统的软、硬件工作的可靠性，是否会因为计算机故障或意外原因（如停电）造成信息丢失、失效或混乱。提高系统可靠性的主要措施是选择质量好、可靠性高的硬件和软件产品，同时考虑系统配置的冗余和备份，还要配置良好的备用电源和防雷设施，系统维护人员要经常对系统进行保养和维护，不可带故障运行等。

（7）不可抵赖性。不可抵赖性是指交易双方的交易行为具有不能否认的特点，包括对自己的行为和行为发生的时间不可抵赖。电子商务交易双方不是面对面的交易，双方都无法按照传统方式确认对方的身份，电子商务中的身份认证就显得尤为重要。通过进行身份认证及数字签名可以避免交易行为的抵赖，通过数字时间戳可以避免对行为发生时间的抵赖。

4. 电子商务安全策略

为了能有效地保证电子商务的安全，应该制定切实可行的安全策略。安全策略主要内容包括：①认证，对交易各方的身份确认；②访问控制，限制不同的人具有不同的访问权限；③保密，对于敏感信息及商业秘密信息限制读取的范围；④数据完整性，限制对数据的修改权限；⑤审计，对操

作的人、事及时间进行记录和审查；⑥法律，用法律手段解决出现的安全问题，保护交易双方的合法权益；⑦管理制度，提高管理者素质，防范来自内部的攻击。

5.1.2 电子商务安全及其重要性

1. 电子商务安全现状

在 Internet 上进行交易面对着风险，同样在现实中也有类似的风险，例如，信用卡信息被盗用的风险等。因此，无论是在网络虚拟世界，还是在现实世界，都要面对信用卡信息被盗用的风险。

在防不胜防的破坏性活动面前，谁也无法预测计算机信息系统将会受到怎样的挑战。一方面，没有统一的信息安全标准、密码算法和协议，在安全和效率之间难以两全；另一方面，大多数管理者对网络安全不甚了解，存在着管理漏洞。另外，信息犯罪属于跨国界的高技术犯罪，要用现有的法律进行有效的防范十分困难，无形中增加了解决电子商务安全问题的难度。

2. 电子商务安全的重要性

电子商务交易的安全一直是媒体的热门话题，大多数媒体的报道都对网上交易的安全性持怀疑态度，认为 Internet 是一个开放式的网络结构，在上面传递的个人信用信息很可能被网络黑客窃取、盗用。如果在网上购物，每次在输入信用卡号时都担心信用卡信息是否会被他人盗取，这种交易环境能让人安心使用吗？

相对于面对面的常规交易，人们对网上交易的安全性信心不足，主要原因有：①进行交易时消费者和商家不在同一个地方；②消费者和商家的网上交易可以非同步进行；③个人信用信息在传递过程中可能被他人偷窃、盗用；④网络商店的真伪不好辨别，或网上商店、商务网站可能被黑客利用等。

因此，在运用电子商务模式进行交易时，电子商务的交易安全就成为关键所在，也是电子商务得以顺利推行的保障。要想营造一种可以信赖的安全环境，解决电子交易的安全、保密问题至关重要。

3. 电子商务安全隐患

Internet 在给人们带来方便的同时，也把人们引入了安全陷阱。据报道，2004 年春季，美国一位网络高手利用在新闻组中查到的技术，窃取了 8 万个信用卡的账号和密码，并标价 126 万美元出售，在全球引起了巨大震动。而互联网站遭到黑客袭击的消息更是不绝于耳，据《今日美国》报道，对 560 多家企业、大学和政府机构的调查表明，85%的网站曾受黑客的袭击，经济损失累计在一亿美元以上。另有资料显示，企业计算机受到侵害的比例逐年上升，从 1999 年的 49%上升到 2012 年的 85%。为什么电子商务会遇到如此之多的安全问题？一种解释认为，Internet 起初设计并不是用于商业目的，而是为了方便信息资源共享。所以，Internet 的 TCP/IP 协议及源代码的开放与共享在当时是合情合理的。但要在网上进行安全要求较高的电子商务活动，信息资源共享的做法难免暴露出许多安全问题。

开展电子商务面临的安全隐患主要有：①中断系统，破坏系统的有效性；②窃听信息，破坏系统的保密性；③篡改信息，破坏系统的完整性；④伪造信息，破坏系统的可靠性和真实性；⑤对交易行为进行抵赖，要求系统具备审查能力。

5.1.3 电子商务安全的主要威胁

黑客对网络进行的大多数攻击和破坏，是利用网络自身的漏洞进行的，主要的攻击表现在以下几方面。

1. 侵入系统

未授权人（黑客）通过非法手段侵入到系统内部，实现对系统资源的占用，或对用户信息的窃取、篡改和非法使用。黑客利用网上的漏洞和缺陷，进行修改网页、非法进入主机、窃取信息等破坏活动。入侵者不仅可以轻易盗取系统资源，还可能在系统中注入木马等病毒，破坏系统的正常工作。

2. 监听扫描

监听扫描是指通过某种软件对网络主机进行信息扫描或信息监视，提取重要信息，通过分析，获得有价值的数据。

3. 拒绝服务

拒绝服务是一种破坏性的攻击，是指一个用户采取某种手段故意占用大量的网络资源，使系统没有剩余资源为其他用户提供服务的攻击。随着因特网的发展，拒绝服务攻击成为网络安全的重要威胁。

4. 身份仿冒

计算机系统一般采用身份认证方式进行保护，对系统用户的身份进行仿冒是常见的一种攻击方式。用于用户身份认证的密码，在登录时是以明文的方式在网络上进行传输的，因此，很容易在网络上被截获，黑客可以对用户的身份进行仿冒，使身份认证机制失效。

5. 信息重发

信息重发攻击方式，就是攻击者在截获网络上相关信息后，再将这些信息发向有关的服务器，实现破坏的目的。

6. 病毒攻击

病毒是能够破坏计算机系统正常工作，具有传染性的一段程序。因特网的快速发展使病毒传播速度大大加快，病毒侵入网络，破坏资源，成为电子商务的又一重要安全威胁。

5.2　电子商务交易中的安全技术

目前使用最多的安全防护技术主要有：防火墙技术、信息加密技术和数字证书等。

5.2.1　防火墙技术

1. 防火墙的作用

电子商务系统包括企业内部网和外部网，内部网在加强企业内部管理、方便企业内部信息交流，提高工作效率等方面起着重要的作用。但是 Intranet 与 Internet 连接以后，如果不加限制，Internet 上的每一个用户都可以访问企业内部网，使黑客能够轻而易举地侵入企业内部网，非法访问、破坏企业的内部信息资源。因此，在企业内部网与外部网之间设置一道安全屏障是非常重要的。

防火墙（Firewall）是指由软件和硬件设备结合而成，在 Intranet 和 Internet 之间构筑的一道屏障（相当于家庭的防盗门），是一个用于加强内部网络与公共网络之间安全防范的系统。只有允许的通信信息才能通过防火墙，起到内部网与外部网的隔离作用，可以限制外部用户对内部网络的访问和内部用户对外部的通信。它控制所有内部网与外部网之间的数据流通，防止企业内部信息流入 Internet；同时控制外部有害信息流入 Intranet。防火墙还能执行安全策略，记录可疑事件。

2. 防火墙的类型

常用的防火墙主要可分为包过滤型和应用网关型两种。

（1）包过滤型。包过滤型可以动态检查通过防火墙的 TCP/IP 报文头中的报文类型、源 IP 地址、目标 IP 地址、源端口号等信息，与预先保存的清单进行对照，按预定的安全策略决定哪些报文可以通过、哪些报文不可以通过防火墙。包过滤型可以在路由器上增加功能，成本较低。

（2）应用网关型。应用网关型使用代理技术，在内部网与外部网之间建立一个单独的子网，该子网有一个代理主机，通过路由器和网关分别与内、外网连接，代理主机对外部和内部用户的网络服务请求进行认证，对于合法用户的服务请求，代理服务主机将内部网与外部网连通，自己作为通信的中介，外部用户只能获得经过代理的内部网服务，这种机制可以保护内部网络资源不受侵害。

3. 防火墙的安全策略

防火墙的安全策略有两种。

（1）凡是没有被列为允许访问的服务都被禁止。这是安全性高于一切的策略，要确定所有需要提供服务的客户的安全特性。在这个策略下，会有很多安全的用户和信息因未被列入允许服务清单而被拒之门外，使网络的应用范围和效率降低。

（2）凡是没有被列为禁止访问的服务都被允许。这种策略只需确定那些不安全的客户和服务，禁止他们的访问。网络的灵活性得到保留，但容易出现漏网之鱼，使安全风险增大，所以网络管理员必须随时发现要禁止访问的客户和服务，增添到安全策略中去。

5.2.2 信息加密技术

保证电子商务安全和口令安全的一个重要手段就是信息加密。信息加密技术是研究数据加密、解密及变换的科学，涉及数学、计算机科学、电子与通信诸多学科。核心思想是：既然网络本身不安全可靠，那么就要对重要的信息进行加密处理，确保其安全性。加密算法能将信息进行伪装，使任何未经授权的人都无法了解其内容。

1. 信息加密技术概述

（1）明文、密文、加密与解密算法

在信息加密系统中，要加密的信息称为明文（Plaintext），明文经过变换加密后的形式称为密文（Ciphertext）。将明文转变为密文的过程称为加密（Enciphering），由加密算法实现。将密文还原成明文的过程称为解密（Deciphering），由解密算法实现。对明文进行加密时采用的一组规则称为加密算法，对密文进行解密时采用的一组规则称为解密算法。

（2）加密技术

数据加密技术要求只有指定的用户，才能接触密码进行数据的加密或还原，这需要给数据发送方和接收方一些特殊的信息用于加密或解密，即密钥。密钥是加密和解密所需的一串数字，是指加密算法中参与变换的参数，是从大量的随机数中选取的。

具体的加密方法有两种：一种是硬件加密，其效率和安全性非常高，但硬件设备有专用性，成本高、不通用；另一种是软件加密，其优点是灵活、方便、实用、成本低，安全性不如硬件高。

根据明文转换的情况，将加密技术分为替代密码加密和换位密码加密。替代密码加密就是隐藏明文，将明文中的字符替换成另外的字符，接收方对密文进行逆替换就能恢复出明文。换位密码加密是不隐藏明文中的字符，只是将明文中字符的顺序打乱，达到保密的效果。

（3）对称密钥算法与非对称密钥算法

根据加密和解密过程是否使用相同的密钥，加密算法分为对称密钥算法和非对称密钥算法两种。对称算法是指加密和解密的过程使用同一个密钥，其特点是运算速度快。常见的对称算法有 DES（Data Encryption Standard）算法等。非对称算法虽然运算速度慢，但是在需要身份认证的信

息系统应用中，具有不可替代的作用。非对称加密算法中有两个密钥，一个称为公钥，一个称为私钥。在加密时，公钥用于加密，私钥用于解密。这种算法比较复杂，如 RSA（Rivest Shamir and Adleman）算法等。非对称加密算法已广泛应用于因特网的数据加密传送和数字签名。

网络黑客会千方百计地破获密钥，为了使黑客难以破获密钥，就要增加密钥的长度，使黑客无法破解密钥。当密钥长度超过 100 位（bit）时，即使是使用当代高速计算机，也需要几十年才能破译密钥。因此，现在采用的密钥都在 128 位以上。

2. 对称加密技术

（1）对称密钥加密法

对称密钥加密法又称单钥加密，即加密和解密使用的是同一个密钥，即使不相同，也可以由一个密钥推导出另一个密钥。通信双方必须相互交换彼此的密钥，当需要给对方发送信息时，用密钥进行加密，而对方在接收到数据后，再用密钥进行解密。

对称加密算法的使用大大简化了加密的处理方式，贸易双方采用相同的加密算法，不必彼此研究和交换专用的加密算法，只需交换共享的专用密钥即可。在和对方交换信息时，还需要有一种非常安全的方法传输各自的解密密钥，否则，解密密钥一旦被泄漏，加密也就失去了作用，任何拥有密钥的人都可以解读加密的信息。对称密钥加密法算法常见的有：DES 加密算法，IDEA 加密算法，ESS 加密算法等。

美国国家标准局为了能在政府各部门间进行信息传递，保证数据的安全，自 1971 年开始研究数据密码的标准化，1973 年开始征集满足下列条件的密码方式。

1）密码的规定明确而严谨。

2）能通过破译密钥所需时间与计算量来表示它的安全性。

3）安全性只依赖于密钥的安全性，不依赖于算法的安全性。

征集的结果是采用了 IBM 公司提出的研制方案，这种方案于 1975 年研制成功，是一种采用多次换位与代替相结合的处理方法。美国国家标准局于 1977 年 1 月 5 日正式将其确定为美国的统一数据加密标准 DES。近 40 年 DES 算法得到了广泛的应用。

（2）对称加密技术的缺陷

对称加密技术使用 DES 算法，发送方和接收方有相同的密钥，密钥的长度一般为 64 位或 56 位。这种加密方法虽然解决了信息的保密问题，但是又引出了新的问题：如何将密钥传送给接收方？因此，对称加密技术在实际应用中有以下问题。

1）密钥传输的安全性。在首次通信前，双方必须通过除网络以外的安全途径传递密钥。

2）密钥的保管复杂。当通信对象增多时，需要相应数量的密钥。例如一个拥有 100 个贸易伙伴的企业，必须要有 100 个密钥，这就使密钥管理和使用的难度增大。如果企业对所有的合作者使用同一个密钥，他们就能相互读取别人的信件，这样就无密可保了。

3）无身份鉴别。对称密钥加密无法验证消息的发送方和接收方的身份，因此，没有办法进行身份鉴别。用户 A 和用户 B 拥有相同的密钥，而算法是公开的，这样他们都可以创建和加密一个信息，然后声称密文是对方发送的。要实现身份的鉴别，解决方法是采用公开密钥，这是一种非对称的加密方法。

3. 非对称加密技术

为了克服对称加密技术密钥管理和分发上存在的问题，产生了非对称加密技术。

（1）非对称密钥加密法

非对称密钥加密法，又称双钥加密法，其思想是由 W.Diffie 和 Hellman 在 1976 年提出的，于

1978 年由 Rivest、Shamir 和 Adleman 三人，在麻省理工学院研究发明的，因此，称为 RSA 算法。RSA 算法是公开密钥密码体制中一种比较成熟的算法。非对称密钥技术中的密钥都是成对的，即有一对互补的钥匙，一个称为公钥（Public Key），另一个称为私钥（Private Key），其中公钥是公开的，这个公开的密钥可以保存在服务器上供大家下载，私钥需要使用者自己保留使用。公钥和私钥之间具有紧密联系，用公钥加密的信息只能用相应的私钥解密，反之亦然。要想由一个密钥推知另一个密钥，在算法上是不可能的。

通信时，发送方用接收方的公钥将明文进行加密，然后通过网络传送给接收方，接收方用自己的私钥将密文解密，除了私钥拥有者以外，没有任何人能将其解密，即使是发送方也是如此。如果密文在网络传输过程中被第三方截获，其得到的只是加密后的信息，没有私钥就无法解密还原。这样既解决了信息保密问题，又克服了对称加密中密钥管理与分发传递的问题。非对称密钥算法常见的有 RSA 算法和 Hash 函数法等。

（2）非对称加密技术的优缺点

非对称密钥加密法的主要优点如下。

1）降低密钥传递风险。公开密钥可以通过服务器等方式轻易地发布，企业无需给每一个合作者发送一个公开密钥拷贝，他们可以从企业的密钥服务器上方便地获得。企业要做的就是保管好自己的私有密钥，不要被他人窃取。企业的合作者用公开密钥加密明文，给企业发送信息，这样只有拥有私有密钥的企业才能解密阅读。

2）识别私有密钥使用者的身份。用非对称密钥加密可以鉴别出信息的发送方，基本思想是：用户 A 的公开密钥是能解开某条密文的唯一密钥，因此，可以判定这条密文只能是用户 A 用其私有密钥加密后发送的，这样就鉴别出这条信息只能是由用户 A 发送的。

非对称密钥加密法的主要缺点是：加密、解密速度慢，耗用资源大等。

（3）对称密钥加密法与非对称密钥加密法的比较

与对称密钥加密法相比，利用非对称密钥加密法进行安全通信，首先，通信双方不需要事先通过保密信道交换密钥；其次，密钥持有量大大减少。在 N 个用户之间进行通信，每个用户只需持有自己的私钥，公钥可以放在公共数据库中，供其他用户取用。这样，通信只需拥有 N 对密钥，就可以满足相互之间进行安全通信的需求。实际上，出于安全方面的考虑，每个用户可以持有多个密钥，分别用于数字签名、加密等用途。即使如此，与使用对称密钥加密法时需要 N×N/2 个不同的密钥相比，需要的密钥数量还是显著地减少。

一般情况下，实用的加密解密方案都将对称密钥加密法和非对称密钥加密法进行了综合运用，发挥它们各自的特点。

5.2.3 信息加密技术的应用

要实现完全的电子商务必须具有在线支付的功能，保证在线支付的安全是实现在线支付的关键。安全电子交易协议 SET 是已经被广泛接受的一种因特网信用卡标准化支付机制。SET 使用了多种密钥技术达到安全性的要求，主要采用对称数字加密技术、公开密钥加密技术和散列函数的方法。

综合应用这些数据加密技术产生了信息摘要、数字签名、数字时间戳、数字信封和数字证书等多种应用。

1. 信息摘要

信息摘要是 Ron Rivest 在 20 世纪 70 年代发明的一种单向加密算法，其加密结果是不能解密的。将需要加密的明文直接“摘要”成一串 128bit 的密文，这一串密文又称为数字指纹（Finger Print）。

信息摘要具有固定的长度，而且不同的明文摘要成的密文，是绝对不相同的，但相同的明文其摘要一定是相同的。因此，信息摘要成为验证明文的数字“指纹”，可以通过“指纹”鉴别明文的真伪。数字摘要方法解决了信息的完整性问题。

信息摘要过程：①对明文使用 Hash 算法得到信息摘要；②将信息摘要与明文一起发送；③接收方对接收到的明文用 Hash 算法生成一个信息摘要；④将接收方产生的信息摘要与发送方发来的信息摘要进行对比，若两者相同，表示明文在传输过程中没有被篡改，否则说明原文被篡改过。

2. 数字签名

数字签名又称电子加密（Digital Signature），是非对称加密技术的一种应用，主要采用 RSA 算法、DSS 算法和 Hash 算法，其中使用最广泛的是 RSA 算法。RSA 数字签名采用公开密钥算法，生成一对公钥和私钥，发送信息时用私人密钥加密信息（即数字签名），信息接收方用信息发送方的公钥对数字签名进行解密，验证发送方身份。

数字签名机制提供了一种鉴别方法，普遍用于银行、电子贸易等，可以解决以下问题。

（1）伪造。防止接收方伪造一份文件，声称这是发送方发送的。

（2）抵赖。防止发送方或接收方事后不承认自己曾经发送或接收过文件。

（3）冒充。防止网上的用户冒充另一个用户来发送、接收文件。

（4）篡改。防止接收方对收到的文件进行局部的篡改。

要说明的是，数字签名与手写签名不同，会随着文本的变化而变化，与文本信息是不可分割的，而手写签名是附加在文本之后的，与文本信息是分离的。

数字签名过程：①发送方用自己的私钥对信息摘要加密；②发送方将加密后的信息摘要与原文一起发送；③接收方用发送方的公钥对收到的加密摘要进行解密；④接收方对收到的原文用 Hash 算法进行信息摘要；⑤将解密后的摘要与计算得到的摘要进行对比，相同说明信息完整且发送方身份是真实的，否则说明信息被篡改过或不是该发送方发送的。

由于发送方的私钥是自己严密管理的，他人无法仿冒，同时发送方也不能否认用自己的私钥加密发送的信息，所以数字签名解决了信息的完整性和不可否认性问题。

数字签名与密钥加密不同，密钥加密是发送方用接收方的公钥加密，接收方用自己的私钥解密，是多对一的关系，表明任何一个拥有公司公钥的人都可以向该公司发送密文，但只有该公司才能解密，其他人不能解密；而数字签名是发送方用自己的私钥对摘要进行加密，接收方用发送方的公钥对数字签名解密，是一对多的关系，表明公司的任何一个贸易伙伴都可以验证数字签名的真伪性。

3. 数字时间戳

在交易文件中，时间是十分重要的信息。在书面合同中，文件签署的日期和签名一样是十分重要的防止文件被伪造和篡改的关键性内容。在电子交易中，同样需要对交易文件的日期和时间信息采取安全措施，数字时间戳能提供电子文件发表时间的安全保护。

数字时间戳（Digital Time Stamp，DTS）是由专门机构提供的电子商务安全服务项目，用于证明信息的发送时间。数字时间戳是一个经加密后形成的证书文件，包含 3 个部分：①需要加数字时间戳的文件的摘要；②数字时间戳服务机构收到文件的日期和时间；③数字时间戳服务机构的数字签名。

数字时间戳产生的过程为：需要数字时间戳的用户先将文件用 Hash 算法加密得到数字摘要，然后将数字摘要发送到提供数字时间戳服务的专门 DTS 机构；DTS 机构对原摘要加上时间以后，用自己的私钥加密（即数字签名）再发还给原用户，获得数字时间戳的用户就可以将它再发送给自

己的商业伙伴证明信息的发送时间。

由于数字时间戳是由认证中心（Certificate Authority，CA）——数字时间戳服务机构加上的，作为收到文件的时间依据，因此，时间戳还可以扩展到作为科学发明、专利等事物的时间认证上。

4. 数字信封

数字信封（Digital Envelop）就是对所传送的密钥用非对称加密技术中的公钥进行加密形成的，是双方传送对称数字加密技术的密钥时应用的技术。就像人们把不希望别人看到的东西放到信封里交给对方一样，传送对称加密技术的密钥时，将密钥放到“数字信封”里。对方收到数字信封后，再用自己的私钥解密，从而获得对称加密技术的密钥。

数字信封可以解决密钥的分发问题。在密钥分发过程中，还存在接收方如何确认数字信封不是伪造的问题。解决这个问题需要由各方都信任的第三方机构——认证中心对数字信封的有效性进行认证，确定发送数字信封的发送方的真实身份。认证中心通过发放数字证书证明数字证书拥有者的身份。

5.2.4 数字证书

1. 数字证书概述

在电子交易中，假如交易的甲方从网上得到了乙方的公钥，他会想这个公钥是否真是乙方的，是否会有他人假冒乙方在网上发布公钥？甲方不能直接通过网上向乙方询问，因为假冒者可能会截获询问而再次假冒乙方发回确认信息。为了确认网上交易双方的真实身份，需要借助第三方颁发的数字证书进行身份确认。

数字证书又称数字凭证（Digital Certificate/Digital ID），是用电子手段证实用户的身份和对特定网络资源的访问权限，是由权威机构发行的。包含拥有者的公开密钥、详细个人资料的信息摘要以及签发机构的数字签名。在网上电子交易中，如果双方出示了各自的数字证书，并用它来进行交易操作，那么双方都不必为对方身份的真伪担心。数字证书可广泛用于电子邮件、电子商务、电子基金转移等各种用途。

数字证书是由权威公正的第三方机构（认证中心）签发的。以数字证书为核心的加密技术，可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性、签名信息的不可否认性，保证网络应用的安全性。

数字证书采用公、私钥密码体制，每个用户有一把仅为本人所掌握的私钥，用它进行信息解密和数字签名；同时拥有一把公钥，用于信息加密和签名验证。要发送保密文件时，发送方使用接收方的公钥对数据进行加密，接收方使用自己的私钥进行解密。这样，信息就可以安全无误地传输了，即使被第三方截获，由于没有相应的私钥，也无法进行解密。

用户用自己的私钥对信息进行处理，由于私钥仅为本人所有，所以能生成别人无法仿造的数字签名。由于数字签名与信息的内容相关，因此，一份经过签名的文件如有改动，就会导致数字签名的验证失败，这样就可以保证文件的完整性。

数字证书可用于发送电子邮件、访问网站、网上证券交易、网上采购招标、网上办公、网上保险、网上税务、网上签约和网上银行等安全电子事务处理和安全电子交易活动。

2. 数字证书的内容

数字证书的格式和内容，由 CCITT X.509 国际标准规定，包含的主要内容有：①证书拥有者的姓名；②证书拥有者的公钥；③公钥的有效期；④颁发数字证书的单位；⑤数字证书的序列号；⑥颁发数字证书单位的数字签名。

数字证书的内容可以在 IE 浏览器中查看，查看方法是：在 IE 窗口中，依次选择“工具”→“Internet 选项”菜单项，打开“Internet 属性”对话框，如图 5-1 所示。在“Internet 属性”对话框中选择“内容”选项卡，单击“证书”按钮，进入证书选择窗口，如图 5-2 所示。在其中选择一种证书类别，再在证书列表中选择一个证书，例如，在图 5-2 中选择“受信任的根证书颁发机构”选项卡中的“AddTrust External CA Root”，单击“查看”按钮，可查看所选证书的内容，如图 5-3 所示。

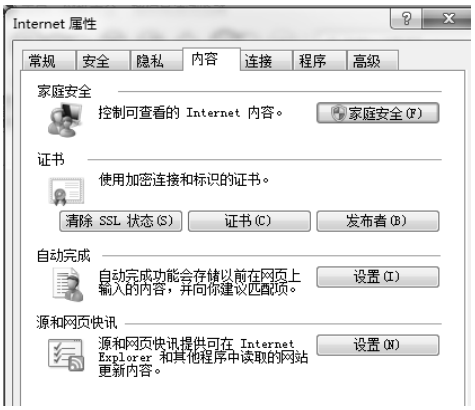

图 5-1　“Internet 属性”对话框

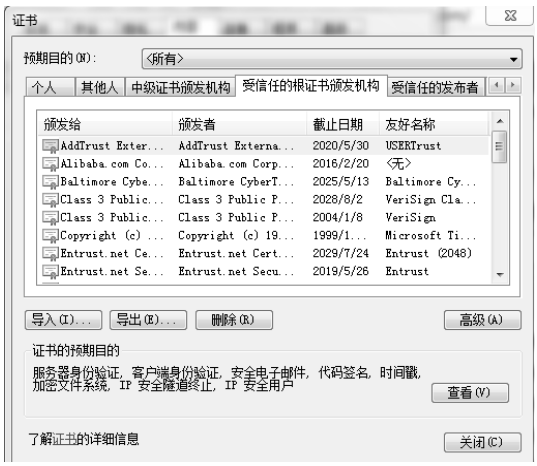

图 5-2　证书选择窗口

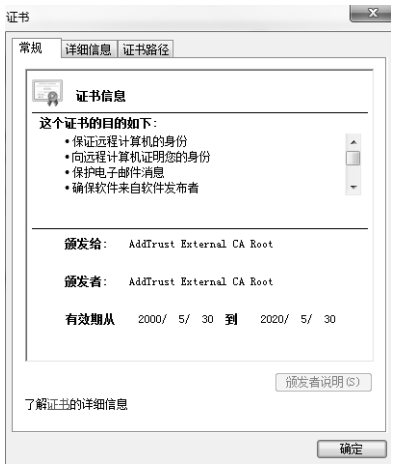

图 5-3　证书查看窗口

3. 数字证书的作用

数字证书的主要作用有：①证实在电子商务或信息交换中参与者的身份；②授权交易，如信用卡支付；③授权接入重要信息库，代替口令或其他传统的进入方式；④提供经过因特网发送信息的不可抵赖性的证据；⑤验证通过因特网交换的信息的完整性。

数字证书是实现电子商务的必要条件，是参与网上电子交易的通行证，因此它本身的可信任程度就更加重要。

4. 数字证书的类型

数字证书主要有以下三种类型。

（1）个人数字证书（Personal Digital ID）

个人数字证书为某一用户提供证书，帮助个人在网上进行安全交易操作。个人数字证书通常

可以安装在客户端的 Web 浏览器内，通过安全的电子邮件进行交易操作。

1）个人安全电子邮件证书。个人安全电子邮件证书可以确保邮件的真实性和保密性。申请后一般是安装在用户的浏览器中。用户可以利用它来发送签名或加密的电子邮件。

2）个人身份证书。个人身份证书是用来表明和验证个人在网络上身份的证书，确保网上交易和操作的安全性和可靠性。个人身份证书可以用于网上炒股、网上理财、网上保险、网上缴费、网上购物、网上办公等，通常存储在 U 盘或 IC 卡中。

（2）企业（服务器）证书（Server ID）

企业证书通常是指网上的某个 Web 服务器的证书，拥有 Web 服务器的企业可以对具有证书能力的网站进行安全的电子交易。具有证书的 Web 服务器会自动地将其与客户端 Web 浏览器通信的信息内容加密。

1）客户端数字证书。主要用于单位安全电子事务处理。具体应用如安全电子邮件传送、网上公文传送、网上签约、网上招标投标、网上办公系统等。

2）服务器数字证书。主要用于网站交易服务器，需要和网站的 IP 地址、域名绑定，保证网站的真实性和不被人仿冒。目的是保证客户和服务器之间进行交易、支付时，双方身份的真实性、安全性和可信任度等。

（3）软件数字证书（Software Digital ID）

软件数字证书又称代码数字证书，代表软件开发者身份，用于对软件开发者开发的软件进行数字签名，证明软件的合法性。通常为在 Internet 中下载的正版软件提供证书，使用户在下载软件时能获得相应的信息。

这三类数字证书的前两类是常用的凭证，大多数认证中心都能提供，第三类证书用于特殊场合，认证中心一般不提供，由专门机构审理。

5. 数字证书的申请

（1）个人数字证书的申请

个人数字证书的申请可以在用户浏览器上进行，分为两个级别。第一级数字证书仅仅提供个人电子邮件地址的认证，个人获得一级数字证书后，认证中心将邮件地址证书列于公共目录中。第二级数字证书提供对个人姓名、身份等信息的认证，获得二级数字证书后，认证中心也会将认证信息列入公共目录。

当一个人申请数字证书之后，认证中心对申请者的电子邮件地址、个人身份及信用卡号等信息进行核实，通常这个过程需要 3～5 天，核实后即向申请人颁发数字证书。颁发数字证书时由认证中心发给用户一个确认邮件，在邮件中通知用户有关证书中的信息，同时将该证书安装在用户的 Web 浏览器或电子邮件系统中。

个人在其 Web 浏览器上安装了数字证书后，可以在浏览器中设置以下 3 种状态。

1）普通发送。不使用数字证书。

2）签发文件。在发送信息的同时，系统会自动将信息和发送方的数字签名一起发送给对方，但用此方法发送的信息本身并未加密。

3）加密文件，除了拥有上面签发文件功能外，在发送时还会自动用接收方的公钥加密信息，并会注明此信息是加密的。

（2）服务器数字证书的申请

与个人数字证书不同，服务器数字证书将帮助企业建立一个在虚拟交易环境中的信任度。在网上虚拟交易环境中，人们无法和商家面对面接触，因而需要依靠数字证书进行信任度确认。

申请服务器数字证书要比申请个人数字证书复杂，验证要比个人身份的验证复杂。企业需要把调查表文件填写好后，用电传或电子邮件发送到认证中心，调查文件的内容包括：①企业或组织的情况介绍；②合作伙伴的情况；③营业执照与纳税证明等。

当企业的服务器证书生效后，就能用验证后的身份与外界通信，数字证书依据与之绑定的一对密钥表示其确定性。用该对密钥进行加密，可以保证该服务器的身份。当一个经认证的客户与一个经认证的服务器进行通信时，客户端的软件会自动验证服务器端的数字证书，而服务器绑定的这对密钥又被用于加密一个会话密钥。会话密钥用于对服务器和客户机的会话进行加密。每个服务器和客户机的会话均会使用不同的会话密钥，每个会话密钥只有 12～24 小时的有效期，因此，要在被认证的服务器和客户机通信时进行信息窃听是十分困难的。

（3）数字证书的申请步骤

不同类型的数字证书的申请步骤略有不同，一般都有以下步骤。

1）下载并安装 CA 的根证书。为了建立数字证书的申请人与 CA 的信任关系，保证申请证书时信息传输的安全性，在申请数字证书前，客户端计算机要下载并安装 CA 的根证书。

2）填交证书申请表。不需身份验证的申请表可在线填写后提交。需要个人或单位身份验证的，下载申请表，填写后连同身份证明材料一起送达 CA。

3）CA 进行身份审核。

4）下载或领取证书。

普通证书，可以用身份审核通过后得到的序列号和密码，从网上下载证书；使用特殊介质（如 U 盘、IC 卡）存储的证书，需要到 CA 领取。

5.2.5　认证中心

认证中心（Certificate Authority，CA）作为电子商务的神经中枢是保证网上电子交易安全的一个不可缺少和无法替代的机构，在电子交易中承担网上认证服务、签发数字证书、确认用户身份等工作，是具有权威性和公正性的第三方服务机构，是实现网上交易和网上支付的安全保障。

1. 认证中心的概念

认证中心是颁发数字证书的第三方权威机构，在电子商务交易过程中，商家、客户、银行的身份都要由认证中心认证。

数字证书的申请者在生成自己的密码密钥后，可以把公钥和身份信息送到认证中心认证。认证通过后，认证中心将签核过的认证放到认证数据库中，供其他人查询和下载，交易双方都能在认证中心取得对方的认证，证明公钥和身份的相关性。认证中心除了签发认证之外，还要负责维护认证的安全性与完整性，万一交易过程发生纠纷，认证中心应按照他和客户之间的协议，负责举证的责任，将双方的注册信息和认证送交司法机构裁决。

2. 认证中心的主要功能

认证中心的主要功能是受理数字证书的申请、签发及对数字证书的管理。认证中心通过运用对称和非对称数字加密技术建立起一套严密的身份认证系统，可以保证信息除了发送方和接收方外不被其他人窃取，信息在传输过程中不被篡改，发送方能够通过数字证书确认接收方的身份，发送方对于自己发送的信息不能抵赖。认证中心主要有以下 5 种基本功能。

（1）证书核发

认证中心接收、验证用户（包括下级认证中心和最终用户）的数字证书的申请，核实申请人的各项资料是否真实，根据核实情况决定是否颁发数字证书。如果认证中心接受该数字证书的申请，

将进一步确定给用户颁发何种类型的证书。新证书用认证中心的私钥数字签名以后，发送到目录服务器供用户下载和查询。为了保证信息的准确性和完整性，发给用户的所有信息都要使用认证中心的数字签名。

（2）证书更新

认证中心定期更新所有用户的证书或根据用户的请求更新用户的证书，保证认证中心保留最新、最有效的证书信息。

（3）证书查询

证书查询分为两类：一类是证书申请的查询，认证中心根据用户的查询请求返回当前用户证书申请的处理过程；另一类是用户证书的查询，这类查询由目录服务器完成，目录服务器根据用户的请求返回适当的证书信息。

（4）证书作废

有两种情况需要把证书作废。一种情况是用户的私钥泄漏，用户提出证书作废。此时用户需要向认证中心提出证书作废申请，认证中心根据用户的申请确定是否将该证书作废；另一种情况是证书已经过了有效期，认证中心自动将该证书作废。认证中心通过维护证书作废列表完成证书作废的功能。

（5）证书归档

证书具有一定的有效期，证书过了有效期之后自动作废。但是不能将作废的证书简单地丢弃，因为有时客户可能需要验证以前的某个交易过程中产生的数字签名，这时客户就需要查询作废的证书。因此认证中心必须具备管理作废证书和作废私钥的功能。

3. 认证中心的树型验证结构

在交易双方通信时，通过认证中心签发的数字证书证实对方的身份，如果对签发证书的认证中心的身份有怀疑，可以向签发该证书的 CA 机构验证该认证中心证书的身份有效性，这样逐级认证，一直到公认的权威认证中心，形成一种树型验证结构，最权威的认证中心称为根 CA。例如，某商家的证书是由湖北省电子商务认证中心（HBECA）签发的，而 HBECA 的证书又是由中国南方电子商务中心（Southern Electronic Business Center Class CA）签发的，等等。

4. 认证中心是身份认证的机构

在电子交易中为了保证交易的安全性、公正性，身份认证的工作是由第三方机构完成的，认证中心就是这样的服务机构。认证中心通过对电子商务各参与方发放并管理数字证书，确认各方的身份，通过其注册机构核实证书申请者的身份。

5. 认证中心是对公钥进行公证的机构

交易中的各种证书大部分是非对称密钥体制的一种密钥管理媒介，例如，数字时间戳服务和数字证书，都是权威性的电子文档，是网络环境的身份证，用于证明某一主体（如人、服务器等）的身份及其公钥的合法性。在使用公钥体制的网络环境中，必须向公钥的用户证明公钥的真实合法性。因此，在公钥体制环境中，必须有一个可信的机构对某个主体的公钥进行公证，证明主体的身份及其公钥的匹配关系，认证中心正是这种机构。

6. 国内外认证中心简介

只有建立一个安全、高效的 CA 体系，才能保证网上交易的顺利进行，使电子商务健康有序地发展。我国已经建立了一些大型的认证中心，如中国金融认证中心、上海市电子商务证书管理中心等。许多省市也建立了本地的电子商务认证中心，如海南、湖北、重庆及河南等。它们将对我国的认证体系的建设起到巨大的推动作用。

（1）国内常见的 CA 中心

国内常见的认证中心如下。

1）中国金融认证中心（www.cfca.com.cn），支持网上银行、网上证券交易、网上购物以及安全电子文件传递等应用。

2）中国电子邮政安全证书管理中心（www.chinapost.com.cn），发放并管理参与网上交易各方所需的安全数字证书。

3）中国数字认证网（www.ca365.com），为交易双方提供数字认证、数字签名、CA 认证、CA 证书、数字证书等服务。

4）北京数字证书认证中心（www.bjca.org.cn），为网上电子政务和电子商务活动提供数字证书服务。

5）上海 CA 认证中心（www.sheca.com），是发放数字证书的机构，保证电子商务和网上交易的安全。

6）天津 CA 认证中心（www.tj-ca.net），提供网上身份认证、数字签名、电子公证、安全电子邮件等服务。

7）广东省电子商务认证中心（www.cnca.net），提供电子商务认证、安全产品和解决方案，制作、颁发、管理数字证书。

8）湖北省电子商务认证中心（www.hbca.org.cn），提供电子商务安全认证。

9）海南省电子商务认证中心（www.hndca.com/CA/），电子商务数字证书制作、颁发和管理。

（2）国外常见的 CA 中心

在 Internet 上提供认证服务的，常见的国外 CA 有：VeriSign、Certisign Certificadora Digital Ltd、GTE CyberTrust、Thawte 等。

5.3　电子商务的安全协议

通过电子支付安全地完成电子交易过程，是人们在选择网上交易时，首先要考虑到的问题。虽然电子支付的安全问题还没有一个公认、成熟的解决方法，但是人们还是不断地通过各种途径进行大量的探索，安全套接层协议和安全电子交易协议就是这种探索的重要结果，已经广泛地应用于国际、国内的电子支付过程中。

5.3.1　安全套接层协议

安全套接层协议（Secure Sockets Layer，SSL）最初是由 Netscape Communication 公司设计开发的，主要用于提高应用系统间的数据的安全性。

1. 安全套接层协议提供的服务

安全套接层协议主要提供以下三方面的服务。

1）认证用户和服务器。用户和服务器都有各自的识别号，这些识别号由公钥进行编号，为了验证用户是否合法，安全套接层协议要求在握手交换数据时进行数字认证，以此确保用户的合法性，使信息能够发送到正确的客户机和服务器上。

2）加密和隐藏传输的数据。安全套接层协议采用的加密技术既有对称密钥加密，也有非对称密钥加密。具体要看客户机与服务器进行数据交换之前，交换初始握手信息中包含的是哪种。

3）维护数据的完整性。安全套接层协议采用 Hash 函数和机密共享的方法提供数据完整性服

务，建立客户机与服务器之间的安全通道，确保数据在传输过程中不被篡改。

2. 安全套接层协议的运行步骤

安全套接层协议运行的主要步骤有：①接通。客户通过网络向服务商连接，服务商回应。②密码交换。客户与服务商之间交换双方认可的密码，一般选用 RSA 密码算法。③会话密码。客户与服务商之间产生彼此交谈的会话密码。④验证。检验服务商取得的密码。⑤客户认证。验证客户的可信度。⑥结束。客户与服务商之间相互交换信息结束。

安全套接层协议是最早应用于电子商务的网络安全协议，运行的基本特点是商家对客户信息保密的承诺。商家认证客户是必要的，但整个过程中缺少了客户对商家的认证。在电子商务的开始阶段，参与电子商务的公司都是一些大公司，信誉度较高，这个问题没有引起人们足够的重视。随着参与电子商务的厂商迅速增加，对厂商的认证问题越来越突出，安全套接层协议的缺点完全暴露出来，所以目前安全套接层协议正在逐渐地被安全电子交易协议（SET 协议）取代。

5.3.2 安全电子交易协议

在 Internet 上开展电子商务，关键是如何保证买卖双方传输数据的安全。为了克服安全套接层协议的缺点，两大信用卡组织 Visa 和 Master Card，联合开发了安全电子交易协议（Secure Electronic Transactions，SET）。SET 是一个为在 Internet 上进行在线交易而设立的、开放的、以电子货币为基础的电子付款系统规范。安全电子交易协议在保留对客户信用卡认证的前提下，又增加了对商家身份的认证，这对需要支付货币的交易是至关重要的。由于设计合理，安全电子交易协议得到了 IBM、HP、Microsoft、Netscape、GTE 等大公司的支持，并已经获得了 IETF 标准的认可。

安全电子交易协议是一种以信用卡为基础的、在 Internet 上交易的付款协议，是授权业务信息传输的安全标准，采用 RSA 密码算法，利用公钥体系对通信双方进行认证，用 DES 等标准加密算法对信息加密传输，用 Hash 算法鉴别传输的信息有无篡改。

1. 安全电子交易协议运行的目标

安全电子交易协议要达到的目标主要有以下 5 个。

1）保证在 Internet 上传输信息的安全性，防止信息被黑客或内部人员窃取。

2）保证电子商务参与者的信息相互隔离。每个客户的信息在加密打包后，通过商家传输到银行，商家不能直接看到客户的账户和密码。

3）解决多方认证的问题，不仅要对消费者的信用卡认证，还要对在线商店的信誉度认证，同时还有消费者、在线商店与银行之间的认证。

4）保证网上交易的实时性，使所有的支付过程都是在线的。

5）效仿 EDI 贸易形式，规范协议和信息格式，促使不同厂家开发的软件具有兼容性和互操作功能，并且可以运行在不同的硬件和操作系统平台上。

2. 安全电子交易协议涉及的对象

安全电子交易协议主要涉及的对象如下。

1）消费者。包括个人消费者和团体消费者，按照在线商店的要求填写订货单，通过银行发行的信用卡进行付费。

2）在线商店。提供商品或服务，具备相应电子货币使用的条件。

3）收单银行。通过支付网关处理消费者和在线商店之间的交易付款过程。

4）电子货币发行公司，以及兼有电子货币发行功能的银行。负责处理电子货币的审核和支付工作。

5）认证中心（CA）。负责确认交易双方的身份，对厂商的信誉度和消费者的支付手段和支付能力进行认证。

3. 安全电子交易协议涉及的范围

安全电子交易协议涉及的技术范围有：①加密算法的应用（如 RSA 和 DES）；②证书信息和对象格式；③交易信息和对象格式；④认可信息和对象格式；⑤划账信息和对象格式；⑥对话实体之间消息的传输协议。

4. 安全电子交易协议的交易流程

根据安全电子交易协议的工作原理，安全电子交易的流程主要有以下 7 步。

1）消费者利用自己的 PC 通过 Internet 选定所要购买的物品，在计算机上输入订货单。订货单内容主要包括：网店名称、购买物品名称及数量、交货时间及地点等信息。

2）通过电子商务服务器与有关在线商店联系，在线商店作出应答，告诉消费者所填写的订货单的货物单价、应付货款、交货方式等信息是否准确，是否有变化。

3）消费者选择付款方式，确认订单，签发付款指令，此时安全电子交易协议介入。

4）在安全电子交易协议中，消费者必须对订单和付款指令进行数字签名，使用双重签名技术，保证商家看不到消费者的账号等信息。

5）在线商店接收订单后，向消费者所在银行请求支付认可。信息通过支付网关到收单银行，再到电子货币发行公司确认，批准交易后，返回确认信息给在线商店。

6）在线商店发送订单确认信息给消费者，消费者的终端软件可以记录交易日志，以备将来查询。

7）在线商店发送货物或提供服务，通知收单银行将货款从消费者的账号转到商店的账号，或请求发卡银行进行支付。

从第 3）步开始安全电子交易协议起作用，一直到第 7）步。在处理过程中，有关通信协议、请求信息的格式、数据类型的定义等，安全电子交易协议都有明确的规定。在线操作的每一步，消费者、网店、支付网关等都要通过 CA 进行通信主体身份的验证，确保通信的对方不是冒名顶替。也可以简单地认为，安全电子交易协议规定充分发挥了认证中心的作用，确保在开放的网络上参与电子商务各方提供信息的真实性和保密性。

5. 安全电子交易协议的缺陷

安全电子交易协议也不是完美无缺的，还存在以下问题和缺陷。

1）协议没有说明收单银行给在线商店付款前，是否必须收到消费者的货物接受证书，否则的话，在线商店提供的货物不符合质量标准，消费者提出疑义或要求退货，很难明确责任由谁来承担。

2）协议没有担保“非拒绝行为”，这意味着在线商店无法证明订单是不是由签署证书的消费者发出的。

3）安全电子交易协议技术规范没有提及在事务处理完成后，如何安全地保存或销毁此类证据，是否应当将数据保存在消费者、在线商店或收单银行的计算机里。这种漏洞可能使这些数据在以后会受到潜在的攻击。

4）安全电子交易协议大部分的操作依赖 CA 认证中心的认证，但是安全电子交易协议又无法确认认证中心是否被攻击、被假冒，也无法确认认证中心的密钥是否已经泄漏或被修改。

总之，安全电子交易协议提供了网上交易的安全保障体系，但是在实际交易活动中仍可能出现各种非法的侵权行为，因此，不断地分析可能出现的问题和漏洞，对其进行修正和改进，是电子商务安全永远研究的课题。

5.3.3 其他安全协议

1. 安全超文本传输协议（S-HTTP）

安全超文本传输协议（S-HTTP）基于提供保密、认证、完整性和不可否认等服务，保证在Web上的文本安全。

由于Internet的开放性造成了在网络中传输信息的公开性，为了保证信息在网络传输过程的安全，需要进行信息加密。S-HTTP实际上是使服务器支持SSL协议，客户只有通过认证中心（CA）进行身份认证后，才能登录该网站，并且在网络中传输的所有数据都要通过随机产生的密钥加密。

2. 安全交易技术协议（STT）

Microsoft公司提出，STT将认证和解密在浏览器中分开，可以提高安全控制能力。另外，还有国际通用的电子商务标准UN/EDIFACT，国际商会制定的UNCID等安全协议。

5.3.4 使用SET协议的过程

使用SET协议的过程分为发送方和接收方两种。

1. 发送方使用SET协议

使用SET协议发送信息时，发送方对发送的明文进行Hash函数的运算，产生数字摘要，再使用自己的私钥对数字摘要进行数字签名。然后将明文、数字摘要、数字签名以及发送方的CA证书一起，用发送方的对称密钥加密，形成密文。同时用接收方的公钥对发送方的对称密钥加密，形成数字信封，发送方将密文及数字信封一起发送给接收方。

2. 接收方使用SET协议

接收方收到信息后，先用自己的私钥对数字信封解密，得到对称密钥（解密文的密钥）；用该密钥对密文解密后，得到明文、数字签名和发送方的CA证书。再用发送方的公开密钥对数字签名解密得到数字摘要。再对收到的明文用Hash函数进行运算，得到新的摘要，与从数字签名得到的摘要进行比较，如果一致，说明明文未被篡改。

在国内的电子商城或网上超市进行购物，要求用户使用信用卡或电子钱包软件，因此，一些商业银行和商家已经使用了支持SET的电子支付。

5.4 电子商务安全解决方案

在这里阐述的电子商务安全主要涉及：电子商务系统的服务器、客户机和电子通信信道等的安全保护。

5.4.1 电子商务服务器的保护

服务器是电子商务系统的核心部件之一，特别是电子商务数据服务器中保存着大量企业营销数据和客户信息。服务器一旦出问题将导致整个电子商务系统的瘫痪，所以保证电子商务服务器的安全是整个电子商务系统安全的基本要求。

1. 对电子商务服务器的安全威胁

电子商务服务器的主要功能是向不同客户提供不同的服务，这些服务主要使用超文本传输协议进行。对服务器安全构成威胁的主要有：WWW 服务程序；任何有数据的后台程序，如数据库和数据库服务器；服务器的公用网关接口（CGI）程序等。

（1）WWW 服务程序的安全威胁

WWW 服务程序的安全威胁主要来自以下几个方面。

1）WWW 服务程序的安全漏洞。WWW 服务程序越复杂，包含错误代码的概率越高，出现安全漏洞的概率也越高。

2）权限设置带来的安全威胁。设置权限是为了对敏感数据的保护，如果权限设置不当反而会适得其反。大多数计算机上运行的 WWW 服务程序可在不同权限下运行，WWW 服务程序如果以高权限状态运行，黑客有可能利用 WWW 服务器的高权限执行高权限的指令，构成对服务器的安全威胁。

3）目录显示带来的安全威胁。如果服务器所有文件夹的内容浏览者都能看到，会破坏其保密性。因此，WWW 服务程序应更改目录显示的默认设置，限制用户浏览文件夹的内容。

4）对用户名和口令的安全威胁。某些服务器要求用户在访问安全区域中每个页面时都要输入用户名和口令。当用户访问同一 WWW 服务器上受保护域内多个页面时，用户名和口令有可能泄漏。因为 WWW 无法记忆在上一事件中发生过什么，记录用户名和口令最方便的方式，是将用户的保密信息存在用户计算机上的 Cookies 里。当服务器请求用户计算机发出 Cookies 信息进行确认时，WWW 服务器不能保证安全地传输 Cookies 里的信息，此时有可能泄密信息。

5）FTP 程序带来的安全威胁。FTP 程序会对 WWW 服务程序带来安全威胁。如果对 FTP 用户浏览的文件夹不进行保护，有可能发生未经授权的信息泄漏。例如，某企业员工利用 FTP 客户机程序登录到业务伙伴的计算机后，如果对方没有保护措施，就可以打开并显示对方 WWW 服务程序上其他文件夹的内容，甚至下载所看到的任何信息。

6）Cookies 的安全威胁。WWW 服务程序上最敏感的文件之一就是存放用户名和口令的文件 Cookies，如果此文件没有得到保护，任何人就都能以他人身份进入敏感区域，黑客就会得到用户名和口令信息。

（2）数据库安全的威胁

电子商务系统的数据库都是存放在专用的数据库服务器中，不同的服务器可以对不同的用户设置不同的权限。一般一个电子商务系统至少需要一个数据库保存不同类型的信息，这些信息包括 4 个方面：①用户的身份认证信息；②用户的授权信息；③商业信息；④商业交易信息。

电子商务系统的用户可能是客户或潜在客户、员工和合作伙伴。用户的身份认证信息一般包括：用户名、口令、用户的公钥和一些数字证书，授权信息包括访问服务器所需要的所有控制信息。对于数据库的安全威胁主要是某些电子商务系统将 WWW 服务器和数据库服务器共用一台计算机系统，同时对数据库又没有安全措施，完全依赖 WWW 服务器的安全措施。这样，一旦 WWW 服务器的安全被黑客破坏，数据库的安全也就被破坏了。

（3）公用网关接口的安全

公用网关接口（CGI）可以实现从 WWW 服务程序到另一个程序的信息传输。CGI 和接收传输数据的程序为网页提供了活动内容，例如，网页上有一个列表框，要访问者填入某些信息，当访问者提交后，CGI 处理信息将结果放到网页上发给用户的浏览器。CGI 是可执行的程序，允许客户在服务器上运行程序，这势必造成安全威胁。所以在使用 CGI 之前必须做好以下安全保障工作。

1）CGI 必须处于特定的、直接置于管理员的管理目录中，程序编写必须由管理员进行。

2）对 CGI 程序的使用要加以限制。

①不要轻易使用从网上得到的 Script 脚本，限制 CGI 程序对本机文件的读写。

②限制 CGI 程序使用本机程序。

③不允许以特权身份运行 CGI 程序。

④规定 CGI 程序必须检测用户的输入。

3）对于尚处在开发过程的 CGI，一定要对服务器的地址保密，防止程序被泄漏。

4）在 CGI 中，不要用相对路径执行程序，如果必须使用相对路径，应该在执行前设置环境变量。

5）调用 CGI 有两种方法，它们各有利弊。

①通过接口调用。此时 CGI 只能以某个用户的 ID 运行，不会对系统造成致命的破坏。但攻击者可以通过程序删除该用户的文件或者给该用户设置木马。

②以 Server 的 user ID 调用。使用此方法时管理员很难定位。

2. 电子商务服务器安全的解决方案

典型的电子商务服务器包括 WWW 服务器、FTP 服务器、E-Mail 服务器和远程登录服务器等，对电子商务服务器的安全解决方案如下。

（1）访问控制和认证

访问控制是指控制访问电子商务服务器的访问者和访问内容。认证是指验证期望访问的人的身份。

服务器可以通过可信赖的认证中心发放的证书进行认证，对于内部网络的客户机还可以通过回叫系统核对用户名和客户机地址。可以通过用户名、口令以及授予不同的权限进行访问控制。

对访问者使用的证书要注意与认证中心核对其真伪，是否是过期或作废证书。对用户名和口令要注意妥善保存，用户名可以用明文形式存储，口令要用加密格式存储。

WWW 服务器一般是以访问控制表的方式限制用户对文件的访问权限。每个文件都有自己的访问控制列表，在访问控制列表中列出有权访问文件的用户名清单。大多数操作系统都有用户名和口令认证系统。

（2）防火墙

将电子商务服务器放在防火墙内，增加对电子商务服务器的安全保护。

（3）其他防护措施

1）限制在 Web 服务器上开账户，定期删除长时间不用的用户。

2）对 Web 服务器上的账户，在口令长度及定期更新方面作出要求，防止被盗用。

3）尽量使 ftp、mail 及数据库等服务器与 Web 服务器分开，无关的应用尽量少设置。

4）定期查看服务器中的日志，分析可疑事件。

5）合理设置权限和属性，对于关键性文件如配置文件，只允许管理员有写的权利。

6）可以通过程序，限制许可访问的用户 IP 地址或域名。

7）禁止使用从网上下载的工具软件，防止其在程序中设下陷阱。

5.4.2 电子商务客户机的保护

客户机是客户与电子商务企业之间联系的主要工具，如果其安全受到威胁或破坏，可能会出现无法交易或遭到欺诈。

1. 对电子商务客户机的安全威胁

电子商务客户机以浏览器方式运行客户机软件。浏览器采用静态页面时是以 WWW 标准页面描述语言 HTML 编制的，其作用只是显示内容并提供与其他页面的链接。在浏览器页面增加了动态内容后，使浏览器页面生动活泼，同时也带来了对客户机的安全威胁。

（1）动态内容对客户机的安全威胁

动态内容是指在页面上嵌入的对用户透明的程序，嵌有动态内容的页面可显示动态图像、下载和播放音乐等。动态内容有多种形式，包括 Java 应用程序、ActiveX 控件、JavaScript、VBScript 及 WWW 浏览器插件等。动态内容中的某些形式是不能在计算机上直接执行的，只能在另一个程序中执行，许多动态内容程序必须由用户去执行。如小应用程序会随用户所看到的页面自动下载下来，再在用户的计算机上启动运行。电子商务中使用的动态内容涉及将客户选中的商品放入购物车、计算费用总额等。动态内容扩展了 HTML 的功能，为页面带来了生机。

在 WWW 页面里加入动态内容虽然丰富了页面，但却对电子商务客户机带来了安全威胁。黑客可以将有破坏性的页面放入无害的页面中，或随着无害的页面下载到客户机上，一旦运行就可能进行破坏活动。这些破坏活动可能是盗取 Cookie 中的用户名、口令及信用卡号等个人敏感信息，也可能是改变或删除客户机上的信息，还有可能将破坏信息传到服务器，带来更大范围的安全威胁。

（2）Java 应用程序和 JavaScript 对客户机的安全威胁

1）Java 应用程序。Java 是 Sun 公司开发的一种高级程序设计语言，是一种真正面向对象的程序设计语言，已得到广泛的应用。Java 应用程序是用 Java 语言编写的、可实现各种各样的客户端应用的程序。这些应用程序可随页面下载，只要浏览器兼容 Java，就可以在客户机上运行。Java 应用程序在 Netscape 公司的 Navigator 浏览器上和 Microsoft 公司的 Internet Explorer 浏览器上都可以运行。

Java 应用程序经下载就可以运行，这意味着黑客如果在其中放置了破坏性的代码，能够很容易在客户机运行和进行破坏。

2）JavaScript。JavaScript 是网景公司（Netscape）开发的一种脚本语言，支持页面设计者创建动态网页。当用户下载一个嵌有 JavaScript 代码的页面时，此代码就在客户机上运行。JavaScript 与 Java 不同，JavaScript 程序不能自行启动，必须由用户启动。因此，有恶意行为的程序会用各种伪装诱惑用户去启动它进行破坏。

（3）ActiveX 控件对客户机的安全威胁

ActiveX 是一个对象（称作控件），包含页面设计者放在页面执行特定任务的程序。ActiveX 构件源于许多程序设计语言，例如 C++或 Visual Basic 等，但与 Java 或 JavaScript 代码不同的是，ActiveX 控件只能在安装有 Windows 操作系统的计算机上运行，并且只能在支持 ActiveX 控件的浏览器上运行。程序设计人员将 ActiveX 代码封装在 ActiveX 信封里，编译控件把它放到页面上，当浏览器下载了嵌有 ActiveX 控件的页面时，就可以在客户机上运行。

ActiveX 控件一旦下载到客户机上，能像其他程序一样运行，访问包括操作系统代码在内的所有系统资源。因此，有恶意的 ActiveX 能破坏保密性、完整性和即需性。

（4）浏览器插件和电子邮件的附件对客户机的安全威胁

浏览器插件是增强浏览器功能的程序，可以完成浏览器不能处理的页面。插件通常是有益的，用于执行如播放音乐片段、显示电影片段或动画图形等特殊任务。电子邮件不仅能发送文本文件，还可以在附件中放入音频、视频或图形、图像等多媒体内容。

黑客可以将有恶意的指令嵌入到浏览器插件的音频、视频等片段中，随着这些插件的运行执行这些有恶意的指令，起到破坏的作用。同样黑客也可以将有恶意的程序或指令隐藏在电子邮件的附件中，当用户打开附件时，许多形式的附件会同时运行，此时有破坏性的程序或指令也被运行了。例如，在 Microsoft Office 中出现的宏病毒，经常被黑客用来嵌入到电子邮件的附件中。

（5）特洛伊木马

只要动态内容启动，就存在这样一个问题：由于动态内容模块是嵌在 WWW 页面里的，对浏览页面的用户完全透明，企图破坏客户机的黑客将破坏性的动态页面放进无害的 WWW 页面中。这种技术称作特洛伊木马，它可立即运行并进行破坏活动。特洛伊木马是隐藏在程序或页面里并且掩盖了真实目的的一种程序，可以窃取计算机上的保密信息，并将这些信息传给它的 WWW 服务器，构成对保密性的侵害。特洛伊木马还可以改变或删除客户机上的信息，构成对完整性的侵害。

2. 客户机安全的保护措施

针对各种活动给客户机安全带来的威胁，可以采取以下措施避免或减少对客户机安全的威胁。

（1）设置 Java 运行程序安全区

设置 Java 运行程序安全区是根据安全模式定义的规则，限制 Java 应用程序的活动，保护客户机不受 Java 应用程序的威胁。对于不可信的 Java 应用（尚未证明是安全的 Java 应用程序），在 Java 运行程序安全区限制的范围内运行时，不能访问系统中安全规定范围之外的程序代码。例如，遵守运行程序安全区规则的 Java 应用程序，不能执行对文件的输入、输出或删除等操作，防止了破坏保密性和完整性的安全威胁。但是 ActiveX 控件不受 Java 运行程序安全区的限制。

（2）充分利用浏览器软件自身具有的安全措施

常用的浏览器有 Microsoft 公司的 Internet Explorer 和 Netscape 公司的 Navigator。

1）Internet Explorer。Microsoft 公司在 IE 浏览器内部对客户机的保护主要有以下 3 条。

①可以对基于 ActiveX 和 Java 的活动内容做出反应，验证下载活动内容的身份。

②可以检查 ActiveX 控件里的签名以及签名是否被修改。

③可以按照下载文件的来源指定不同的安全设置，采取不同的处理方式。

Microsoft Internet Explorer 将因特网分成 4 个区（Internet 区、本地 Intranet 区、受信任的站点区和受限制的站点区），将安全级别也分为 4 级（低、中低、中和高）。区及安全级别的设置可以在“Internet 属性”/“Internet 选项”对话框中完成。

2）Navigator。Netscape 公司的 Navigator 在浏览器内部对客户机的保护主要有以下 3 条。

①可以控制是否允许将活动内容下载到客户机上。

②在允许下载 Java 程序和 JavaScript 控件时，向用户发出警告信息，指出下载的内容是否有签名并允许用户查看证书。

③可以选择对 Cookie 的 3 种处理方式（无条件接受所有 Cookie、只接受要发回服务器的 Cookie 或完全不接受 Cookie）。

（3）妥善处理 Cookie

Cookie 一般存储在客户机上，保存有发布 Cookie 的网站名、用户在网站上浏览的网页、用户的用户名和口令、用户的信用卡号以及用户的地址等信息。使用 Cookie 的目的是用户在下一次访问该网站时不用重复输入上述信息。为了避免黑客利用 Cookie 进行破坏，可以对 Cookie 采取的措施有：设置 Cookie 的有效期或在浏览器中设置对 Cookie 的控制。

1）Internet Explorer 对 Cookie 的控制。对 Windows 操作系统，可以在“Internet 属性”对话框的“隐私”选项卡中，设置对 Cookie 的控制。对 Cookie 的设置分为以下 6 个级别。

①阻止所有 Cookie：选择该级别的设置，将阻止来自所有网站的 Cookie，客户机上的现有 Cookie 不能被网站读取。

②高：选择该级别的设置，将阻止没有合同隐私策略的 Cookie，阻止使用个人标识信息而没有用户使用许可的 Cookie。

③中高：选择该级别的设置，将阻止没有合同隐私策略的第三方 Cookie，阻止使用个人标识信息而没有用户明确使用许可的第三方 Cookie，阻止使用个人标识信息而没有隐含许可的第一方 Cookie。

④中：选择该级别的设置，将阻止没有合同隐私策略的第三方 Cookie，阻止使用个人标识信息而没有用户隐含许可的第三方 Cookie，限制使用个人标识信息而没有隐含许可的第一方 Cookie。

⑤低：选择该级别，设置将限制没有合同隐私策略的第三方 Cookie，限制使用个人可标识信息而没有隐含许可的第一方 Cookie。

⑥接受所有 Cookie：选择该级别的设置，将允许所有 Cookie 保存到用户的客户机，客户机上所有的 Cookie 都允许创建它们的计算机读取。

Cookie 级别的设置可以通过鼠标拖动左侧的滚动条进行。

2）Navigator 对 Cookie 的控制。在 Netscape 公司的 Navigator 浏览器中，对 Cookie 的控制设置是在参数选择（Preferences）对话框中进行的，有 3 种设置，分别是无条件接受所有 Cookie、只接受要发回服务器的 Cookie 和完全不允许 Cookie。

（4）使用防病毒软件和防火墙软件

防病毒软件是一种不可缺少的防护措施，可以保护客户机不受已经下载到客户机上的病毒的攻击。防火墙软件可以作为一道客户机与网络之间的屏障，保护客户机不受网上黑客的攻击。

5.4.3　电子商务通信信道的安全保护

因特网是电子商务系统的基础，电子商务的各类信息依赖因特网进行传输。因特网构建之初没有考虑安全问题，发展到现在其安全状况仍然没有改善。信息在因特网上传输，从源节点到目标节点的路径中间可能要经过多个节点和多条链路，在一次信息传输过程中，不同的数据帧经由不同的路径。这些都给通信信道的安全保障带来了困难。

1. 对通信信道的安全威胁

对通信信道的安全威胁是多方的，构成了对保密性、完整性和即需性的安全威胁。

（1）利用“探测程序”窃取信息

在因特网上通过“探测程序”记录某个节点（计算机或路由器）的信息已经不是什么难事。在电子商务交易过程中，用户的注册信息（姓名、通信地址、信用卡号、电子邮件等个人或者公司信息）在电子邮件的传输过程中，有可能被“探测程序”窃取。

（2）对他人网站的破坏

所谓破坏他人网站就是对不属于自己的网站进行恶意的修改，添加一些非公司本意的信息，是破坏完整性的典型实例，这种行为相当于破坏他人的实际财物。

（3）电子伪装

电子伪装也是一个破坏网站完整性的例子。所谓电子伪装是在网络上，某人伪装成他人或者某个网站伪装成另外一个网站。当用户访问伪装的网站时就会泄漏个人信息，这样，黑客不仅能获得访问者的信息，还有可能修改访问者的信息后再发送给被伪装者或被伪装的网站，造成不可估计的损失。

（4）破坏即需性

破坏即需性的目的是破坏计算机的正常运行或使计算机拒绝服务。黑客利用大量无用的垃圾信息充斥欲对其进行即需性破坏的计算机，使正常的访问变慢或无法进行，还有可能将信息截获使计算机不能获得信息而造成“拒绝”服务。

（5）访问者使用不当给黑客可乘之机

有时访问者使用不当也会给黑客造成可乘之机。例如，当访问者访问某网站并填写了一个调查表提交后，由于速度慢，在还没有完成提交时就转去访问另一个网站，此时另一个网站就能记录前一个网站的 URL 地址并能够搜集到访问者在调查表中填写的信息。

2. 通信信道安全的保护措施

通信信道的安全保护意味着保证通信的保密性、信息的完整性和通信信道的可用性。

（1）加密

要防止通信信道的窃听是一件非常困难的事（路径的不确定、需要经过多个节点及多条链路等），甚至是不可能的事。因此采取对传输的敏感信息加密的方法，使信息即使被窃听也无法知道所传输信息的真正含义。

（2）安全协议

采用安全协议进行两台计算机间的连接和信息的传输，是保护通信信道安全的必要措施。具体的安全协议是支持两台计算机间的安全连接的安全套接层协议（SSL）和支持安全信息传输的安全 HTTP 协议。

1）安全套接层协议

安全套接层协议（SSL）是由 Netscape 公司推出的一种安全通信协议。SSL 协议要求在建立连接时交换的握手数据中进行数字认证，确保用户和服务器的合法性。在握手信息中采用了加密技术，保证其机密性和数据的完整性。

2）安全 HTTP 协议

安全 HTTP 协议（S-HTTP）是 HTTP 协议的扩展，提供了多种安全功能，包括客户机和服务器的认证、加密以及请求/响应的不可否认等。使用安全 HTTP 协议，客户机和服务器可以指定某个安全功能是“必需”、“可选”还是“拒绝”。客户机和服务器可以单独使用 S-HTTP。如果用户决定使用 S-HTTP 协议，只需在浏览器的 URL 地址栏中输入 URL 地址时，将“HTTP”改写为“S-HTTP”即可。

（3）使用可靠的传输控制协议

传输控制协议（TCP）是面向连接的可靠传输控制协议。在进行传输前首先通过 3 次握手建立起可靠连接，然后再进行信息的传输。对于网络质量不能保证完全满足要求或所传输的信息要求正确率高的情况，应该使用传输控制协议，而不要使用用户数据传输协议（UDP）。因为 UDP 是一种无连接的传输协议，不能完全保证数据的可靠传输。

小　结

电子商务安全要素包括信息的保密性、完整性、不可修改性，收发信息者的身份确定、不可否认，以及系统的可靠性与审查能力。本章介绍的都是电子商务安全的基本内容，主要介绍了电子商务安全现状、电子商务安全隐患、防火墙的作用、数据加密技术、数字摘要、数字签名、数字时间戳、认证技术与数字证书、安全套接层协议（SSL）、安全电子交易协议（SET）和其他安全协议等。通过本章的学习，对电子商务安全要有比较明确、详细的了解，掌握电子商务安全的保障技术，为电子商务活动提供安全保障。

习　题

1．简述电子商务活动中存在哪些安全威胁。
2．电子商务的安全性需求有哪几方面
3．简述对称加密和非对称加密的优缺点。
4．对称加密和非对称加密有哪些异同点？
5．简述数字签名的作用。
6．简述数字签名的形成过程。
7．什么是数字证书？
8．数字证书包括哪些内容？
9．试述数字证书的作用。
10．上网申请一份个人数字证书（或试用证书）。
11．简述认证中心的功能。
12．常用的电子商务安全交易协议有哪些？
13．简述 SSL 协议的作用。
14．简述 SET 协议的作用。
15．试述 SSL 安全协议和 SET 安全协议的区别。
16．简述 SET 协议的工作过程。
17．试述对电子商务系统的保护措施。
18．为什么说安全问题是电子商务能够健康发展的核心问题？