

保障电子商务安全的三种技术

安全问题是电子商务推广过程中最大的障碍。目前，电子商务过程中主要采用的技术有加密技术、认证技术和安全认证协议。这些技术是如何应用的？在下面的内容中将会具体介绍。

加密技术

加密技术是一种主动的信息安全防范措施，其原理是利用一定的加密算法，将明文转换为无意义的密文，阻止非法用户理解原始数据，从而确保数据的保密性。明文变为密文的过程称为加密，由密文还原为明文的过程称为解密，加密和解密的规则称为密码算法。在加密和解密的过程中，由加密者和解密者使用的加解密可变参数叫做密钥。

目前，获得广泛应用的两种加密技术是对称密钥加密体制和非对称密钥加密体制。它们的主要区别在于所使用的加密和解密的密码是否相同。

1. 对称密钥加密体制

对称密钥加密，又称私钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据。它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。

使用对称加密技术将简化加密的处理，每个参与方都不必彼此研究和交换专用设备的加密算法，而是采用相同的加密算法并只交换共享的专用密钥。如果进行通信的双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使用对称加密方法对机密信息进行加密以及通过随报文一起发送报文摘要或报文散列值来实现。

2. 非对称密钥加密体制

非对称密钥加密系统，又称公钥密钥加密。它需要使用一对密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。

在非对称加密体系中，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（加密密钥）通过非保密方式向他人公开，而另一把则作为私用密钥（解密密钥）加以保存。私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。

该方案实现信息交换的过程是：贸易方甲生成一对密钥并将其中的一把作为公开密钥向其他贸易方公开；得到该公开密钥的贸易方乙使用该密钥对信息进行加密后再发送给贸易方甲；贸易方甲再用自己保存的另一把专用密钥对加密信息进行解密。

认证技术

安全认证的主要作用是进行信息认证。信息认证的为目的为：（1）确认信息发送者的身份；2）验证信息的完整性，即确认信息在传送或存储过程中未被篡改过。下面从安全认证技术和安全认证机构两个方面来做介绍。

1. 常用的安全认证技

安全认证技术主要有数字摘要、数字信封、数字签名、数字时间戳、数字证书等。

（1） 数字摘要

数字摘要是采用单向 Hash 函数对文件中若干重要元素进行某种变换运算得到固定长度的摘要码，并在传输信息时将之加入文件一同送给接收方，接收方收到文件后，用相同的方法进行变换运算，若得到的结果与发送来的摘要码相同，则可断定文件未被篡改，反之亦然。

（2） 数字信封

数字信封是用加密技术来保证只有规定的特定收信人才能阅读信的内容。在数字信封中，信息发送方采用对称密钥来加密信息，然后将此对称密钥用接收方的公开密钥来加密（这部分称为数字信封）之后，将它和信息一起发送给接收方，接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开信息。这种技术的安全性相当高。

（3） 数字签名

日常生活中，通常用对某一文档进行签名来保证文档的真实有效性，防止其抵赖。在网络环境中，可以用电子数字签名作为模拟。

把 Hash 函数和公钥算法结合起来，可以在提供数据完整性的同时保证数据的真实性。完整性保证传输的数据没有被修改，而真实性则保证是由确定的合法者产生的 Hash，而不是由其他人假冒。而把这两种机制结合起来就可以产生数字签名。

（4） 数字时间戳

在书面合同中，文件签署的日期和签名一样均是防止文件被伪造和篡改的关键性内容。而在电子交易中，同样需对交易文件的日期和时间信息采取安全措施，而数字时间戳服务就能提供电子文件发表时间的安全保护。数字时间戳服务

（DTS）是网络安全服务项目，由专门的机构提供。时间戳是一个经加密后形成的凭证文档，它包括三个部分：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。

（5） 数字证书

在交易支付过程中，参与各方必须利用认证中心签发的数字证书来证明各自的身份。所谓数字证书，就是用电子手段来证实一个用户的身份及用户对网络资源的访问权限。

数字证书是用来惟一确认安全电子商务交易双方身份的工具。由于它由证书管理中心做了数字签名，因此任何第三方都无法修改证书的内容。任何信用卡持有人只有申请到相应的数字证书，才能参加安全电子商务的网上交易。数字证书一般有四种类型：客户证书、商家证书、网关证书及 CA 系统证书。

2. 安全认证机构

电子商务授权机构（CA）也称为电子商务认证中心（Certificate Authority）。在电子交易中，无论是数字时间戳服务还是数字证书的发放，都不是靠交易双方自己能完成的，而需要有一个具有权威性和公正性的第三方来完成。

认证中心（CA）就是承担网上安全交易认证服务，能签发数字证书，并能确认用户身份的服务机构。认证中心通常是企业性的服务机构，主要任务是受理数字证书的申请、签发及对数字证书的管理。

安全认证协议

目前电子商务中有两种安全认证协议被广泛使用，即安全套接层 SSL（Secure Sockets Layer）协议和安全电子交易 SET（Secure Electronic Transaction）协议。

1. 安全套接层（SSL）协议

安全套接层协议是由 Netscape 公司 1994 年设计开发的安全协议，主要用于提高应用程序之间的数据的安全系数。SSL 协议的概念可以被概括为：它是一个保证任何安装了安全套接层的客户和服务器间事务安全的协议，该协议向基于 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。目的是为用户提供 Internet 和企业内联网的安全通信服务。

SSL 采用了公开密钥和专有密钥两种加密：在建立连接过程中采用公开密钥；在会话过程中使用专有密钥。加密的类型和强度则在两端之间建立连接的过程中判断决定。它保证了客户和服务器间事务的安全性。

2. 安全电子交易（SET）协议

安全电子交易是一个通过开放网络进行安全资金支付的技术标准，由 VISA 和 MasterCard 组织共同制定，于 1997 年联合推出。由于它得到了 IBM、HP、Microsoft 等很多大公司的支持，已成为事实上的工业标准，目前已获得 IETF 标准的认可。这是一个为 Internet 上进行在线交易而设立的一个开放的、以电子货币为基础的电子付款规范。

SET 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，这对于需要支付货币的交易来讲是至关重要的。SET 将建立一种能在 Internet 上安全使用银行卡购物的标准。安全电子交易规范是一种为基于信用卡而进行的电子交易提供安全措施的规则，是一种能广泛应用于 Internet 上的安全电子付款协议，它能够将普遍应用的信用卡的使用场所从目前的商店扩展到消费者家里，扩展到消费者个人计算机中。