

电子商务安全问题 及其解决方案

李玉海 桂学勤

摘要: 本文分析了电子商务中存在的的核心安全问题,并特别提出诚信安全问题,同时对当前解决电子商务安全的技术进行了分析,包括SSL协议和SET协议的特点及其应用中的一些局限。最后,提出了通过支付中介解决电子商务安全特别是诚信安全的方案。

关键词: 电子商务安全; 诚信安全; 支付中介

电子商务是利用Internet进行的各项商务活动,主要包括非支付型业务和支付型业务,非支付型业务指广告、售后服务等业务,支付型业务指交易、支付等业务。

电子商务改变了传统的买卖双方面对面的交流方式,它通过网络使企业面对整个世界,电子商务的规模正在逐年迅速增长,它带来的商机是巨大而深远的。由于电子商务所依托的Internet的全球性和开放性,电子商务的影响也是全面的,它不仅在微观上影响企业的经营行为和消费者的消费行为,而且在宏观上影响到国际贸易关系和国家未来竞争力。因此电子商务引起包括我国在内

的许多国家政府部门的高度重视,纷纷出台了有关政策和举措推动电子商务的发展。

确保有效开展电子商务活动,关键是要保证电子商务系统的安全性,也就是要保证基于Internet的电子商务环境的安全和电子商务交易过程的安全。如何确保电子商务环境的安全和电子商务交易过程的安全,为客户在网上从事商务活动提供信心保证,是决定电子商务系统成败的关键,是电子商务健康全面发展的保障。

1. 电子商务环境安全问题

电子商务环境安全包括计算机系统安全、数据安全、网络安全和应用安全。^[1]

1.1 计算机安全

计算机是一种硬件设备,硬件设备难免出现故障,一旦出现,将会影响电子商务系统的运行。特别是计算机的硬盘,一旦损坏,数据就会丢失,损失就无法挽回,需要对计算机硬件和数据进行备份。计算机系统安全主要

是考虑提高用于电子商务系统的计算机硬件可靠性和稳定性。

1.2 网络安全

网络是用户进行数据交换,信息传递的主要途径。通过网络,用户可以访问网络中不同的计算机系统。网络安全主要是考虑限制用户对用于电子商务系统的计算机的访问权限,防止未授权的用户对系统的访问以及越权访问。

1.3 数据安全

在网络上传递的数据如果不采用任何安全措施,就会受到各种各样的攻击,如数据被截获,甚至数据被恶意篡改和破坏。数据安全主要是考虑防止数据被截获或截获后被破译,以及防止数据被恶意篡改和破坏。

1.4 应用安全

在网络环境下,计算机病毒猖獗,如果不加防范,就容易导致应用软件被病毒感染,程序被非法入侵和破坏,系统的功能受到限制。更严重的是导致系统不能正常工作,数据和信息丢失。应用安全主要是考虑防止应用软件被各种病毒非法入侵和破坏。

2. 电子商务交易安全问题

电子商务交易过程中,商家要发布产品信息,确认订购信息,收货款;客户要获取产品信息,传递订购信息,支付货款。买卖双方都存在安全问题,其中主要包括交易信息安全、支付安全和诚信安全。

2.1 交易信息安全

交易信息包括商家的产品信息和订单确认信息、客户的订单信息。交易信息具有机密性,不能被篡改。交易信息安全主要是防止交易信息被截获或截获后被破译,以及防止数据被恶意篡改和破坏。

2.2 支付安全

支付信息主要是客户的银行帐号、交易金额、以及个人识别码(PIN)和电子货币信息。支付过程中必须保证这些信息的安全。同时,对商家来说,可能存在虚假定单,假冒者以客户名义订购货物,而要求客户付款;对客户来说,可能存在欺骗性网站,盗取客户敏感信息,导致资金被窃取。如何保证客户支付信息安全以及买卖双方身份的真实性,是支付安全主要考虑的问题。

2.3 诚信安全

当电子商务的交易信息和支付信息有了安全保障,也不能让买卖双方放心从事网上交易。我们知道电子商务

的在线支付形式有电子现金、电子支票、信用卡支付。但是采用这几种方式,都要求客户先付款,商家再发货。这样客户的付款以后,会担心收不到货物或者收到劣质的货物。如果是先发货,然后付款,那么商家会担心客户是否会付款。因此,诚信安全也是影响电子商务支付型业务快速发展的关键问题。

3. 电子商务安全问题的对应安全技术

保证电子商务的安全,也就是要保证基于Internet的电子商务环境的安全和电子商务交易的安全。针对电子商务的安全问题,需要有相应的安全技术加以解决。对于电子商务环境安全问题,主要是通过数据备份和灾难恢复技术、防火墙技术、数据加密解密技术和防病毒技术加以解决,这里不作详细介绍。对于电子商务交易安全问题,采用以下技术加以解决。

3.1 数据加密技术

由于交易信息在传输过程中有可能遭到侵犯者的窃听而失去机密性,加密技术是电子商务采取的主要保密安全措施,是最常用的保密安全手段。加密技术也就是利用技术手段把重要的数据变为乱码(加密)传送,到达目的地后再用相同或不同的手段还原(解密)。加密包括两个元素:算法和密钥。密钥和算法对加密同等重要。密钥加

密技术的密码体制分为对称密钥体制和公共密钥体制两种。相应地,对数据加密的技术分为两类,即对称加密和非对称加密。对称加密以数据加密标准(DES, Data Encryption Standard)算法为典型代表,非对称加密通常以RSA(Rivest Shamir Adleman)算法为代表。

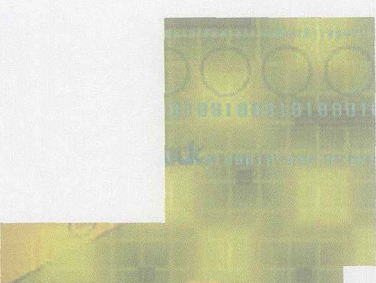
3.2 数字签名

对信息进行加密只解决了信息保密问题,而防止他人对传输的信息进行篡改或破坏,保证信息的完整性,以及保证信息发送者对发送信息的不可抵赖性,需要采用其它的手段,这一手段就是数字签名。在电子商务系统中,数字签名技术有着特别重要的地位,数据签名技术能够保证:信息除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;发送方对于自己发送的信息不能抵赖[2]。

目前的数字签名是建立在公共密钥体制基础上,它是公用密钥加密技术的另一类应用。数字签名与书面文件签名有相同之处,采用数字签名,也能确认以下两点:信息是由签名者发送的;信息自签发后到收到为止未曾作过任何修改。应用广泛的数字签名方法主要有三种,即:RSA签名、DSS签名和Hash签名。这三种算法可单独使用,也可综合在一起使用[3]。

3.3 数字信封

数字签名也是建立在公共密钥体



制基础上,它也是公用密钥加密技术的另一类应用。所谓数字信封是指信息发送方用信息接收方的公开密钥将一个会话密钥加密,形成一个数字信封,然后发送给接收方,只有指定的接收方才能使用自己的秘密密钥打开数字信封,获取其中的对称密钥,并使用对称密钥解读发送方传送过来的信息。

3.4 数字证书

在公共密钥体制中,私钥只有信息发送者知道,而与之匹配的公钥是公开的,它能保证传输信息的机密性,但没有解决公钥的分发方式。数字签名保证了信息是由签名者发送的以及信息自签发后到收到为止未曾作过任何修改,但不能保证签名者身份的真实性。因此需要有一种措施来管理公钥分发,保证公钥以及与公钥有关的实体身份信息的真实性。这一措施就是数字证书。数字证书是一般由具有权威性、可信任性的第三方机构即认证机构(Certificate Authority, CA)所颁发。数字证书是公共密钥体制中的密钥管理媒介,并将公钥和实体身份信息绑定在一起,并包含认证机构的数字签名。数字证书在电子商务中用于公钥的分发、传递,证明电子商务实体身份与公钥相匹配[4]。

以上安全技术、加密技术是电子商务交易安全的基础技术,用于对信息的加密,保证信息的机密性。数字签名和数字信封技术应用了加密技术,建

立在公共密钥体制基础上。数字签名用于对信息进行数字签名,保证信息的完整性和不可抵赖性。数字信封用于对信息进行封装,保证信息只有指定的接收者才能看到。电子证书是对加密技术和数字签名进行支持的技术,用于管理公钥分发,保证公钥以及与公钥有关的实体身份信息的真实性。因此,电子证书必须由权威的和可信赖的第三方签发。

4. 电子商务安全的网络实现技术

电子商务的安全技术是解决电子商务安全的技术手段,需要在电子商务系统所在的网络环境中实现,这些安全技术手段是通过网络安全协议实现。目前网络安全协议包括安全套接层协议(Secure Sockets Layer, SSL)和安全电子交易协议(Secure Electronic Transaction, SET)。

4.1 安全套接层协议(SSL)

SSL(Secure Socket Layer)是由Netscape设计的一种开放协议,主要目的是在两个通信应用程序之间提供机密性和数据完整性。它为基于TCP/IP的客户机/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。SSL协议在应用层收发数据前,协商加密算法、连接密钥并认证通信双方,从而为应用层

提供了安全的传输通道;在该通道上可透明加载任何高层应用协议以保证应用层数据传输的安全性。

但是,SSL是一个面向连接的协议,在涉及多方的电子交易中,只能提供交易中客户与服务器间的双方认证,而电子商务往往是用户、网站、银行三家协作完成,SSL协议并不能协调各方的安全传输和信任关系。在客户直接在线支付的电子商务系统中,由于有银行参与,按照SSL协议,客户购买的信息首先发到商家,商家再将信息转发银行,银行验证客户信息的合法性后,通知商家付款成功,商家再通知客户购买成功,并将商品寄送客户。SSL协议运行的基点是商家对客户信息保密的承诺。在整个过程中我们也可以注意到,商家通过银行对客户身份进行认证,但客户没有对商家身份进行认证,SSL协议有利于商家而不利于客户。但是,SSL协议独立于应用层协议,且被大部分的浏览器和Web服务器所内置,便于在电子商务交易中应用。因此目前大部分电子商务系统仍然使用SSL协议。

4.2 安全电子交易协议(SET)

在电子商务系统中,保证买卖双方传输数据的安全成为电子商务的重要问题。为了克服SSL安全协议的缺点,满足电子交易持续不断地增加的安全要求,两大国际信用卡组织(VISA

和 Master Card) 联合 Microsoft、IBM 等共同制定了安全电子交易 (Secure Electronic Transactions, SET) 协议。这是一个为在线交易设立的以信用卡为基础的电子付款规范, SET 系统在对客户信用卡认证的前提下, 又增加了对商家身份的认证。SET 主要使用电子认证技术, 其认证过程使用 RSA 和 DES 算法, 因此, 可以为电子商务提供很强的安全保护。SET 规格充分发挥了认证中心的作用, 在信息传递过程中使用了数字证书、加密技术, 数字签名, 数字信封等技术, 保证了传递信息的机密性, 数据的完整性和不可抵赖性。

在电子商务交易过程中, 使用 SET 协议, 客户在交易过程中提供两组信息, 一组是向商家提供的订购信息, 一组是向银行提供的支付信息, SET 协议使用数字信封和数字签名技术保证商家并不知道客户的银行支付帐号有关的信息, 同时银行也不知道具体的订购内容, 保证客户资料信息的安全。

虽然 SET 协议规范了客户、商店、支付网关、收单银行、发卡银行资料传送与身分识别以及电子签名等等机制, 安全性大大提高。但 SET 的缺点也很多, 最大的问题是使用麻烦, 客户要使用 SET 协议进行电子商务交易, 需要在电脑上安装电子钱包软件, 且要向发行申请认证, 还要记得钱包密码。而且换一台电脑又不能进行交易, 除非这个

客户比较懂电脑可以把档案带着走。这对大部分的客户来说是一个障碍。也导致 SET 在实际应用中较少使用。

5. 电子商务交易形式和诚信安全解决方案

5.1 电子商务的交易形式

在一般的电子商务系统中, 不论是采用 SSL 还是 SET 协议, 一般都要求客户先付款, 商家再发货。这样, 客户就会担心收不到货物或者收到不符合质量标准的货物。电子商务的诚信安全没有得到解决。根据电子商务系统是否解决诚信安全问题, 可以把电子商务交易分为以下两种形式:

(1) 客户直接与商家在线支付的电子商务交易

客户直接与商家在线支付的电子商务交易, 它的交易过程如下:

① 客户利用已有的计算机通过 Internet 选定物品, 并下电子订单;

② 商家接受定单后做出应答, 告诉消费者的订单的相关情况;

③ 客户选择在线付款方式, 确认订单, 签发付款指令;

④ 付款信息经过商业银行确认后, 商家得到客户付款;

⑤ 商家通知客户购买成功, 并发送货物。

这种交易形式是真正意义上在线支付, 但没有解决诚信安全问题。客户

还没有收到货物, 客户的资金就到了商家的账户。这种交易形式需要商家有足够的诚信, 只有当客户感到交易环境足够安全, 诚信基本不成为问题时, 才会放心的通过采用这种方式进行网上交易。

目前, 诚信度较高的大公司的 B2C 模式的电子商务系统一般采用是这种支付形式的进行电子商务交易。一般只有那些相互熟悉、了解对方诚信的客户和商家使用直接在线支付的交易形式。这一定程度限制了电子商务的发展。

(2) 客户通过支付中介与商家在线支付的电子商务交易

客户通过支付中介与商家在线支付的电子商务交易, 它的交易过程如下:

① 客户利用已有的计算机通过 Internet 选定物品, 并下电子订单;

② 商家做出应答, 告诉消费者的订单的相关情况, 并接受订单;

③ 消费者选择通过支付中介付款方式, 并付款给支付中介;

④ 商家接到支付中介到款通知后发送货物, 并提交发货信息;

⑤ 客户收货满意后, 同意付款给商家;

⑥ 商家收到货款。

这种交易方式客户不是直接付款给商家, 而是先付款给支付中介, 由支付中介代为安全保管。客户收货满意

后,才通知支付中介支付货款给商家,因此客户可以放心的付款。商家在确认支付中介已收到货款后才发货,因此,可以放心的发货。

目前,C2C模式的电子商务系统一般采用这种支付形式的进行电子商务交易。如阿里巴巴网站使用的支付保、易趣网站使用的安付通,就是保证网上安全交易的支付中介。采用支付中介的网上交易做到了“货到付款”与“款到发货”,解决了诚信安全问题,支付中介在交易过程中充当值得信赖的第三方并且控制付款流程,提高了网上交易的安全,有了它,买卖双方就可以放心的通过支付中介进行网上交易了。

5.2 电子商务诚信安全解决方案

安全的电子商务系统不仅要解决交易安全,还需要解决诚信安全,而不能依赖人们对商家的信赖。因此,具有完整的安全解决方案的电子商务系统不仅需要前面介绍的安全技术来解决交易信息安全、支付安全,而且必须引入支付中介来解决诚信安全问题。这里要说明的是支付中介不是一种安全技术,而是一种解决诚信安全的机制。支付中介不但负责资金的安全,同时保证商品的质量。因此,必须由权威的、可信赖的

第三方承担。

引入支付中介的电子商务系统,做到了“货到付款”与“款到发货”,解决了诚信安全问题。同时通过支付中介对客户和商家进行认证,解决了SSL协议中客户对商家身份没有进行认证的问题。因此在引入了支付中介的电子商务系统中一般采用SSL协议保证交易信息安全和支付安全。电子商务诚信安全解决方案如下图(图1):

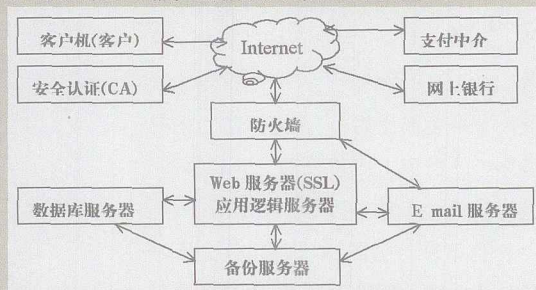


图1 电子商务诚信安全解决方案

下面以典型的支付中介,阿里巴巴网站使用的支付保(支付宝是阿里巴巴公司创办的,用于解决网上安全支付问题)为例,说明使用支付中介的电子商务系统的交易过程:客户注册一个支付宝账户,利用开通的网上银行给支付宝账户充值,然后用支付宝账户在网上购物并网上支付,您的货款会先付款给支付宝,商家收到您支付的信息后给您发货,客户收到商品后在支付宝确认,支付宝收到您确认收货信息后,给商家付款。

采用支付中介的电子商务系统的

交易和支付信息流如下图(图2):

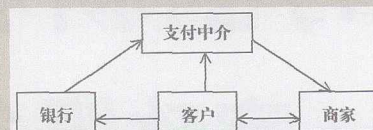


图2 支付中介的电子商务系统的交易和支付信息流

最后必须说明的是,采用支付中介的电子商务交易不是真正意义的在线支付,支付中介只是用于解决诚信安全的机制。电子商务交易的信息安全、支付安全仍然需要加密技术、数字签名和数字证书等技术的支持。支付中介本身也是信息系统,它也需要利用以上安全技术保证自身的安全。■

参考文献:

- [1] 刘军,季常煦,曾洁琼. 电子商务系统规划与设计. 北京.人民邮电出版社. 2002
- [2] 纪志凤,丁鹏. 电子商务系统安全与数字签名技术. 经济师. 2005, 8.
- [3] 中国烟台网. 第四章电子商务的技术要求[EB/OL]. <http://www.chinayantai.net/sw/shangwu5.htm>. 2006-6-10
- [4] 胡伟雄. 电子商务安全认证系统. 武汉. 华中师范大学出版社. 2005

李玉海 华中师范大学信息管理系
湖北 武汉 43007
桂学勤 咸宁学院计算机系
湖北 咸宁 437100