关于电子支付安全技术的研究

赵 敏(沈阳理工大学)

【摘 要】本文主要阐述电子支付安全技术,首先从电子支付安全问题入手,介绍了常见的电子支付的安全隐患,而后详细介绍了数据加密、防火墙、支付网关、数字签名技术等电子支付安全技术,从而促进电子商务的支付安全和快速发展。

【关键词】电子支付;信息泄露;数据加密;防火墙;支付网关
【中图分类号】TP393.0 【文献标识码】A 【文章编号】1006-4222(2017)02-0116-01

1 概 述

随着科学技术水平的不断提升，电子商务成为一种非常流行的新模式,带动了我国国民经济的快速发展,与电子商务配套的服务则是电子支付，通过互联网操作完成电子商务网站的资金支付过程,银行网银、第三方支付等也都随着电子商务的快速发展如火如荼地开展起来。表象的繁荣景象下电子支付安全问题却一直令人担忧，尤其是行业相关的安全规范和法律法规都未随之发展和完善起来，这些都为不法分子造成了可乘之机,也为电子支付的过程带来了安全威胁,如何对电子支付进行安全防护是非常值得关注的问题。所以对于电子支付安全技术的研究,对提升支付安全度,促进电子商务快速发展来说具有非常重要的现实意义。

2 电子支付安全面临的问题

目前的法律法规在电子支付过程中的相关义务和权利定义不清晰,网络消费和服务权益的规则不完善,客户信息和隐私数据的保护不彻底等种种原因造成了我国电子支付安全问题层出不穷,电子支付过程面临着各种安全问题,网络侵权行为时有发生。互联网恶意攻击者可以轻松地获取到客户的邮件信息、付款信息、账户信息、支付信息等,并且很容易造成客户隐私数据甚至是商业机密的泄露。其次,在互联网的恶意攻击下,卖方信息很容易造成泄露或复制,从而使用钓鱼网站等来假冒真正的卖方来实现个人的恶意行为,如资金欺骗、恶意竞争等,甚至可以开展商业间谍活动来盗取商业机密。对于买方来说,个人信息很容易造成泄露,从而被非法分子利用来做其他的欺骗行为,同时也会造成其他更多的破坏行为。

3 关于电子支付安全技术的研究

3.1 数据加密技术

数据加密技术是常见对数据信息安全保护技术，可以对明文数据信息开展有效的保护。目前,数据加密包括了非对称加密和对称加密两部分，二者在本质上的区别在于对密钥的管理上和数据加密方式上，而目前比较流行的电子支付数据加密技术为非对称加密技术。非对称加密技术又称为公开密钥加密,通过提供公开密钥和私有密钥的方式,来配合数据加密算法对敏感信息进行数据加密和解密处理，公开密钥和私有密钥的不对称,而算法处理上需要的时间比较长,但是对于数据加密的效果非常好，所以在数据安全尤其是电子支付安全方面非常符合敏感数据的加密要求，有时候为了满足更高的数据安全要求,在数据发送过程中,会采用对称加密和非对称加密对数据进行多重加密过程,从而有效保障数据的安全。

3.2 防火墙技术

防火墙技术属于典型的边界安全技术，尝尝会在网络边界将受保护的网络或服务器等设备与外部网络进行隔离,通过防火墙自身的数据筛选和过滤功能来保障被保护网络和服务器的安全,这对于黑客或病毒入侵、非法访问等具有非常好的保护效果。防火墙技术的本质是对数据的过滤和访问请求的控制，常见的通过过滤型防火墙通过在路由器设置访问控制列表，将网络报文中的源 IP 和目标 IP 地址以及数据访问行为进行筛选和过滤，根据预设的规则来转发或丢弃相关的数据包,从而实现电子支付的安全。防火墙技术也可以通过构建病毒防火墙来实现对病毒程序的过滤，通过对数据的过滤来有效保障病毒程度的入侵和扩散，从而保障被保护网络的安全,实现电子支付的信息安全。当然,防火墙技术的引入,一定程度上降低了网络的性能，但是大大提升了网络电子支付过程中的数据信息安全,对于电子支付领域来说非常重要。

3.3 支付网关技术

支付网关技术又称为 GT,是 Payment Gateway 的全称,其主要功能是实现对敏感数据的加解密处理。在银行或支付系统中的数据在互联网络进行传输时，支付网关首先会对其根据相关的加密算法进行加密，而后封装处理生成网络传输报文,而支付系统接收到电商系统发出的数据后,支付网关会先对其进行解析,而后根据相应的解密算法对其进行解密,从而生成银行或支付系统所需要的数据，通过在互联网络中对传输支付报文进行有效的加密、解密和报文封装、解析工作,有效地保障了电子支付的安全。当然,支付网关的引入会在性能上对支付系统造成瓶颈，网关配置过低可能会限制大并发量负载下的电子支付的效率。

3.4 数字签名技术

数字签名技术是保障电子支付信息有效性的技术，由于数字签名很难被伪造,所以在电子支付过程中被广泛应用。数字签名技术与常规的签名一样,在电子支付信息发送之前,在整个数据链中假如一个数字标签,即为数字签名,在支付系统或电商系统接收到相应的支付信息后，会对数字签名进行验证,如果验证通过则说明数据报文信息是有效的,如果验证失败则说明该报文信息无效，而后会丢弃该报文并进行相应的处理。数字签名技术有效地保障了电子支付的安全,在形式上也多种多样,如哈希签名、RSA 签名等,这些签名技术可以单独使用也可以多种组合使用，有效地提升了电子支付过程中的数据信息安全。

4 总 结

通过电子支付安全技术来保障电子支付的资金安全和信息安全,是从根本上为电子支付提供安全保障,有效保障支付过程中的数据安全,通过数据加密技术、防火墙技术、支付网关技术、数字签名技术等,有效地提升电子支付数据信息的安全,从而有效地提升电子商务活动的安全性。

参考文献

[1]徐可塑.电子支付安全技术探究[J].电子测试,2014(06).
[2]姜魁武.浅析电子支付的安全问题及解决策略[J].行政事业资产与财务,2013(04).

收稿日期:2017-1-4