文章编号：2096-1472(2018)-08-30-03
DOI:10.19644/j.cnki.issn2096-1472.2018.08.009

计算机网络安全技术在电子商务中的应用

赵 炎
(江苏省宿迁经贸高等职业技术学校，江苏 宿迁 223600)

摘 要：近年来，在计算机网络的深入推进下，电子商务在使人们的日常生活中，得到了较为广泛的运用，也给人们带来了很多的便利性，电子商务中的买卖双方都处在一个虚拟的网络空间当中来完成双方之间的交易。因此，计算机网络安全技术的高低对买卖双方交易的隐私有着最直接的影响。确保用户交易和隐私安全，对于在电子商务中进行交易的买卖双方具有非常重要的作用。因此，完善计算机网络安全技术在电子商务中的应用，大大提高电子商务的安全性，为电子商务的健康、可持续发展提供更有力的技术保障，具有极其深远的意义。

关键词：电子商务；计算机；网络安全技术fb90019
中图分类号：TP393.08 **文献标识码**：A

Application of Computer Network Security Technology in Electronic Commerce

ZHAO Yan
(*Jiangsu Suqian Higher Vocational and Technical School of Economy and Trade*,*Suqian* 223600,*China*)

Abstract: With the advancement of computer network technology in recent years,electronic commerce has become more widely used in people's daily life,bringing a lot of convenience.Since buyers and sellers in e-commerce conduct transactions in virtual network space,the computer network security technology directly influences the security and privacy of both buyers and sellers.It is very important for both buyers and sellers to ensure the security of the transaction and privacy in e-commerce.To this end,the improvement of network security technology can increase significantly the security of e-commerce,providing more powerful technical safeguard for the healthy and sustainable development of e-commerce.

Keywords:e-commerce;computer;network security technology

1 引言(Introduction)

随着信息技术的不断发展，电子商务的到来，在很大程度上打破国家和地区之间的区域限制，促使生产开始向无形化转变，即网络化和全球化。电子商务是一把双刃剑，有利有弊端。众所周知计算机和网络技术是电子商务发展的载体。在新形势下，全球电子商务日新月异发展，与此同时，各种计算机病毒让人防不胜防，木马千变万化，黑客层出不穷导致安全问题成为的现阶段电子商务当中，最重要的是事情，故而，我们如何采取行之有效地措施，进一步确保电子商务的可别性、保密性、完整性、不可伪造性是当前亟待解决的问题。

2 分析计算机网络技术同电子商务之间的关系(Analyze the relationship between computer network technology and e-commerce)

2.1 计算机网络技术是电子商务的运行基础

从广义上来看，电子商务其实就是建立在计算机网络基础上的一种商务活动，在这项以网络为基础的活动当中，包含各个方面的行为，比如，商务和服务的消费者、提供者等，而虚拟交易就是电子商务的实质，一旦电子商务脱离了计算机网络技术，就丧失了其存在于发展的空间[1]。

2.2 计算机技术是促进电子商务发展和革新主要动力

通过计算机网络技术可以整合和管理电子商务数据库，并运用先进的算法来实现对数据库的安全保护和数据加密，从而有效促进商务活动的顺利进行；此外，交易双方还能通过计算机网络技术进行在线交流，例如在电子商务网站中设置即时聊天软件等。企业也可以利用计算机网络技术最大化地实现企业、消费者，以及相关供应商和企业的合作伙伴之间的切实有效地进行沟通，进一步促使企业通过电子业务共享等功能，切实有效地让企业业务流程的电子化，与此同时，电子业务化，并同生产管理系统互相配合，通过有机的配合，最大化提升企业的各个环节的工作效率。

3 电子商务活动中的计算机网络安全隐患分析(Analysis of computer network security risks in e-commerce activities)

3.1 数据信息安全隐患

研究发现，如果在电子商务的具体运行过程当中，缺乏相关对相关网络数据的加密保护处理，而是使用明文方式来传送

相关网络数据，非常容易出现网络数据在在传送的过程当中对黑客被截获的情况，从而造成用户信息被盗取或篡改的情况，一部分攻击者还会通过冒充用户以虚假信息进行诈骗，对合法用户的权益造成严重经济损失，后果无法估量[2]。

3.2 网络边界安全隐患

网络和外部数据是电子系统运行的基础，倘若在具体的运行过程当中，没有采取相关措施对其进行保护很可能会给攻击者留下可以利用的漏洞，使其获得访问系统的权限，为系统的安全性留下隐患。研究发现，现阶段我们最为常见的网络攻击手段一共有几种，Dos/DDos、欺骗类攻击、控制类攻击、探测类攻击和漏洞类攻击。

让系统无法正常运行是Dos/DDos的主要目的，让系统资源耗尽，让服务器系统的相关服务崩溃，以及使其网络连接出现堵塞情况，最终导致系统无法正常的运行。且最为典型的Dos/DDos主要是，死亡之ping、LAND和同步洪流等。欺骗类攻击，这种网络攻击手段，利用各种不同的方式和不良手段，伪造假各种信息，目的主要是为了制造假象，欺骗客户最终进行攻击。此网络攻击手段，最为常见且典型的主要是IP地址欺骗、DNS欺骗等。控制类攻击这种攻击手段，通过一些手段，掌握了计算机控制权，在获取了相关权利之后，在进行进攻。通常情况下，木马攻击、为缓冲区溢出攻击，是我们日常生活最为常见的。另外，就是探测类攻击，从字面上理解，这种形式主要是通过对相关目标的收集和整理，找出计算机网络系统当中，所隐藏的一系列问题，进而对系统进行进攻。最后一种类型漏洞类攻击，这种攻击行为，针对计算机网络系统当中存在的各种漏洞，实施攻击行为，随着社会的不断发展，当前网络攻击行开始变的多样化且针对性强。

3.3 电子商务服务器和网站安全隐患

通过研究发现，很大一部分电子商务网站设计网站的时候，并没有立足整个系统的来考虑网络的安全性，这样一来，导致网络存在各种问题，如跨站注入漏洞、上泄露传漏洞等，在很大程度上就让攻击者有机可乘，进人电子商务网站，泄露用户的交易信息，造成极大地经济损失。如果电子商务网站服务器系统存在的大量的漏洞，就会让病毒有机可乘，对系统进行攻击，轻者损害经济利益，重者客户资料全部丢失。另一方面，倘若用户权限或者是账号的密码设置过于简单，就会让入侵者跨站注入漏洞、上泄露传漏洞，以及SQL注入安全漏洞等，这样一来，就让攻击者有机可乘，出现信息的泄漏或者是让服务器系统的崩溃等各种安全隐患[3]。

3.4 用户计算机安全隐患

众所周知，商家和客户之间的交易操作，都是通过网络来进行的，由于用户可以随时随地家中、办公室，以及网吧使用计算机来进行交易，一旦计算机存在木马和病毒，可能会导致出现泄露广大客户登录和交易信息，造成非常严重的损失[4]。

4 计算机网络安全技术在电子商务中的应用 (Application of computer network security technology in electronic commerce)

4.1 数据加密技术

随着信息技术的不断发展，加密技术是电子商务中不可或缺的一门关键技术，计算机研究人员，将这种技术分为两种：第一，对称加密；第二，非对称加密。

我们说到的第一种技术就是对称加密，这种技术主要是使用的对称密码编码技术，其主要是就是在文件的加密和解密中，用一样的密钥，计算机网络研究人员对其冠名称之为对称加密算法，这种的数据加密技术具体流程如图1所示，对称加密发送方使用加密算法用密钥K加密需要发送的明文，通过有效地处理之后，将相应的加密文件通过网络为对方传输过去，收到加密文件的接受方，使用密钥K对相关信息做解密做处理，这样做的目的就是获取发送方的明文，规避相关信息被盗取。

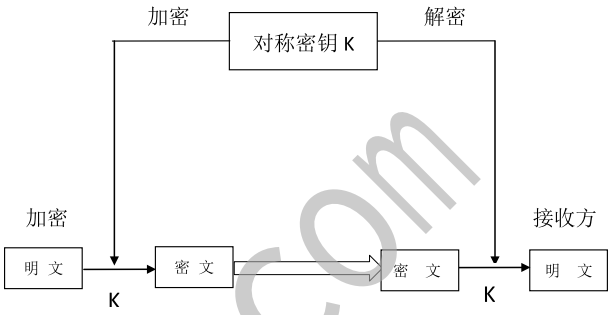

图1 对称加密算法流程图

Fig.1 Flow chart of symmetric encryption algorithm

非对称加密算法有公开密钥和私有密钥两个密钥，二者共同完成有关数据信息加密或是解密工作，想要处理好加密和解密过程是必须要两把完全不相同的密钥。故而，计算机研究人员将这两种过程为非对称加密算法，被我们熟知或最具有代表性的就是RSA算法。具体流程如图2所示，发送方利用密钥将其发来的明文进行加密处理，从而使其形成密文，并通过网络将其密文传输送达接收方。受到密文的接受方，利用密钥使用解密算法进行解密，进而有效地获取明文信息。

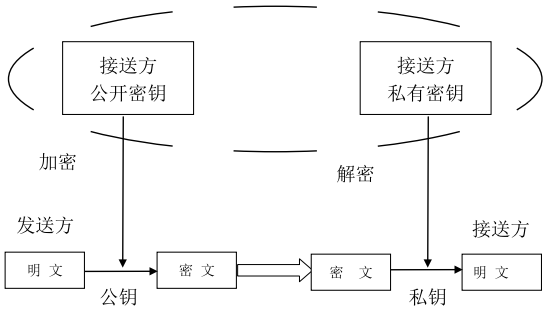

图2 非对称加密算法流程图

Fig.2 Flow chart of asymmetric encryption algorithm

由于两种算法各自具有优势，非对称加密算法密钥管理简单，能最大化的实现验证和数字签字，对称加密算法密钥较短，整理快捷简单破译难度大。因此，在具体的应用过程中，可以有效地将二者有机结合在一起。

4.2 认证技术

4.2.1 数字签名

数字签名还可以叫它电子签名，这种认证技术在认证身份、不可否认性、数据的完整性和匿名性等方面有着非常终重要的应用价值。数字摘要与非对称加密技术就是数字签名的联合应用。一个128Uit的报文摘要生成，是通过报文发送方从报文文本中得来的，且对这个散列值进行加密是用自己专用密钥进行的，发送方的数字签名由此形成；接收报文一方所收到的数字签名，就是通过报文的附件和报文进行发送的；其中

128BI位的散列值，是报文接收方通过接收到的原始报文中计算出的，报文附加的数字签名需要用发送方的公开密钥进行解密。相同的两个报文摘要，则表示该数字签名是发送方的，对原始报文的鉴别和不可抵赖性可以通过数字签名得以实现。具体情况如图3所示。

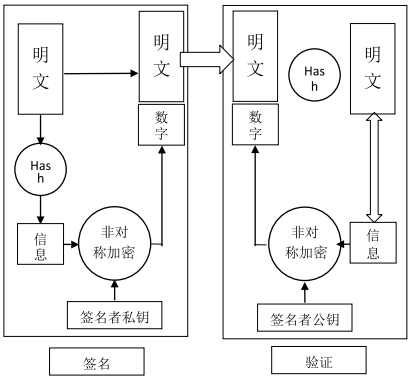

图3 数字签名验证过程

Fig.3 Digital signature verification process

在电子商务中的数字时间戳，不但要考虑交易时间等信息的安全性，而且与此同时，还必须要全局角度来思考，各个方面存在的安全因素问题，比如，数据信息的不可否认和伪造性，数据信息正确性、保密性和完整性等，还要考虑数据信息的保密性、完整性、正确性，以及不可否认和伪造等方面的安全因素。从时间层面上来分析，数字时间戳可以认证电字商务交易信息，进而更好地保护电子信息时间。

4.2.2 数字证书

数字证书就是电子商务中的交易凭证，这是证明用户的合法身份的关键，其中开发者证书、服务器证书、个人数字证书都属于数字证书。其主要采用电子文档的方式记录用户的身份信息的合法性，以及访问资源的权限。

4.2.3 CA认证中心

CA认证中心是用户在申请数字证书，以及证书的签发、管理过程中的第三方权威机构，其权威的认证行为是推动我国电子商务事业安全发展的重要保障。

4.3 网络边界的安全防护技术

4.3.1 访问控制技术

将访问控制技术运用在内部网络与外部网络的交界处，能有效在两种网络之间建立起一道保护屏障，防止内部网络遭受来自外部网络的重击。同时网络控制技术也是确保信息安全的重要保障。在电子商务系统中运用该技术，能够有效在系统与外部网络之间建立安全隔离带，进而实现最大限度减少来自电子商务系统内部的安全风险。

4.3.2 入侵防御技术

这种技术主要是采取防火墙技术开展访问控制，以及安全边界隔离，在很大限度上规避了电子商务系统所出现的运行风险，如果我们知识单纯的运用防火墙技术并不能从根本上解决该问题。IPS作为填补防火强，以及防毒软件的一个系统，该系统可以在第一时间内检测或是预防各种网络安全设备的侵犯，充分发挥出自身的监视作用，同时还可以针对电子商务系统访问过程当中，一些不正常或是具有超强伤害性行为，及时的采用相应的对策，比如调整、隔离或中断等[5]。

4.3.3 服务器与网站的安全防护技术

一是网络防火墙技术。Web应用防火墙与传统的防火墙和IPS产品相比，其就是Web整体安全防护设备，其保函了页面保护、Web保护、负载应用，可以为就Web应用攻击提供更准确、更全面的保护。Web应用程序防火墙是作为一种安全产品，它通过运用一系列关HTTP/HTTPS的安全对策来专门保护Web应用程序。

二是服务器防护安全技术。通过安全配置、用户权限更改、开启审核、科学设立安全账号和密码规则，以及将不必要的服务端口关闭等措施，能确保系统管理者对促进服务器安全管理的实效。另外，将病毒防护策略运用到服务器中，例如安装蛇毒软件等，不仅能对系统病毒进行定期维护，还能提前进行木马病毒和一些后门程度的检测，达到安全预防的目的。

4.4 计算机网络的病毒防范技术

计算机网络安全中特别具有威胁的一项就是网络病毒感染。计算机由于病毒的不断感染，为想要攻击计算机的攻击者提供了十分良好的条件，这非常不利于电子商务活动的顺利开展，如今对于病毒的防范，计算机网络已经有探测技术与入侵检测技术相结合的防御系统，能够监控所有计算机网络，是计算机网络安全技术主要的构成部分，也为电子商务的顺利开展奠定良好的基础。

5 结论(Conclusion)

在电子商务的建设过程中，必定会遇到诸多安全技术问题。为此，笔者重点论述了计算机网络技术与电子商务之间的关系，并立足于当前电子商务中存在数据信息安全隐患、网络边界安全隐患、电子商务服务器和网站安全隐患、用户计算机安全隐患，同时并分析了数据加密技术、认证技术网络边界的安全防护技术、计算机网络的病毒防范技术在电子商务当中的运用。由于网络在变化，应用在变化，入侵方式同破坏的手段也发生着很大的变化。因此，任何一种安全技术都不是绝对的安全，因此，我们要必须要不断与时俱进，不断进步，科学的制定相关安全技术，并切实实施安全技术，确保电子商务的安全，促使其稳健长远发展。

参考文献(References)

[1] 张振江,刘昆,程军军,等.基于图形口令的认证方案及其在电子商务中的应用[J].北京理工大学学报,2017,37(12):1253-1258.

[2] 张滨,冯运波,吴秦建,等.移动电子商务安全技术与应用实践[J].通信学报,2016,37(04):200.

[3] 龚俭,臧小东,苏琪,等.网络安全态势感知综述[J].软件学报,2017,28(04):1010-1026.

[4] 蔡辉泉.电子商务中计算机网络安全技术的使用探讨[J].品牌,2015(7):62.

[5] 金红兵.电子商务网络安全问题现状及防范措施[J].信息安全与技术,2016,7(02):12-14.

作者简介：

赵 炎(1984-)，男，本科，讲师.研究领域：计算机网络，电子商务.