文章编号：1005-8451（2003）10-0024-03

电子商务中安全技术的探讨

杨立春，刘知贵
（西南科技大学 计算机科学院，绵阳 621002）

摘 要：针对电子商务中的安全问题加以论述。分析了电子商务中存在的安全隐患，及其对安全性的要求。阐述目前解决电子商务安全的主要技术和最新成果。并对我国的电子商务安全现状给予概述。

关键词：电子商务；安全技术；网络
中图分类号：TP39 **文献标识码**：A

Development of security technology of e-Business

YANG Lichun, LIU Zhigui
(School of Computer Science of Southwest University of Science and Technology, Mianyang 621002)

Abstract: It was introduced the security problems existing in e-Business, analyzed the hidden trouble and the demand of safety in electronic activity, described the main and new technologies used to solve the security of e-Business, emphasized the present state about security of e-Business in our country.

Keywords: e-Business; security technology; network

1 引言

电子商务的发展给人们的工作和生活带来了新的尝试和便利性，同时也促进了世界经济的全球化发展。但电子商务并没有像人们想象的那样普及和深入，除其他因素外，一个很重要的原因就是电子商务的安全性，它成为阻碍电子商务发展的瓶颈。

2 电子商务中的安全分类

电子商务的一个重要技术特征是利用IT技术来传输和处理商业信息。因此，电子商务安全从整体上可分为2大部分：计算机网络安全和商务交易安全。

计算机网络安全包括：计算机网络设备安全、计算机网络系统安全和数据库安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，保证计算机网络自身的安全性为目标。

商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

3 电子商务中的安全隐患

窃取信息：利用搭线窃听窃收，利用高性能的协议分析仪和信道检监测设备、接受电磁辐射信息、陷阱和后门程序、黑客手法、窃收计算机操作系统得到密码、破解系统核心密码、窃取用户帐号密码等。

篡改信息：当入侵者掌握了信息的格式和规律后，通过各种技术手段和方法，将网络上传送的信息数据在中途篡改，然后再发向目的地。在路由器或网关上都可以做此类工作。

假冒信息：攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。

抵赖行为：就是不承认已经作过的交易或行为。

恶意破坏：由于攻击者可以接入网络，则可能对网络中的信息进行篡改，掌握网上的机要信息，甚至可以潜入网络内部，其后果是非常严重的。

安全漏洞：安全漏洞可以分为2大类，操作系统、数据库、路由器、应用软件等本身所固有的；用户在组建企业网络时造成的，这是因为将缺乏集成性和互操作性的不同厂商的不同产品进行综合时，其结果必然会造成网络的复杂性加剧和漏洞增多。

4 电子商务对安全的要求

（1）易者身份的确定性：常用的处理技术是身份认证，依赖某个可信赖的机构（认证中心－CA）发放证书，双方交换信息之前通过CA获取对方的证

收稿日期：2003-04-04
作者简介：杨立春，在读硕士研究生；刘知贵，副教授。

书，并以此识别对方。

（2）信息保密性：交易中的电子商务信息均有保密的要求，常用的处理技术是数据加密和解密。

（3）不可丢失性：对于固定且具有频繁贸易往来的伙伴，可以采用单证传输的序列性检验（即为单证分配序列号，或者增加时间戳）；也可采用双方约定的方法，即在规定的时间内，通过某种方式进行确认，包括采用特定的确认报文（如：订单确认报文），或者电子邮件确认和电话确认等。

（4）不可修改性：主要采用散列技术来防止非法用户对单证的篡改，通过散列算法对被传输的单证进行处理。

（5）不可否认性：鉴别单证真实性的主要手段是数字签名技术。

（6）电子商务仲裁解决：通常要求引入认证中心进行管理，由CA发放密钥，传输的单证及其签名的备份发至CA保存，作为可能争议的仲裁依据。

（7）数据库存储安全：当使用WWW服务器支持电子商务活动时，应注意数据的备份和恢复，并采用防火墙技术，有些公司直接采用物理分割WWW服务器和内部网络的连接，保护内部网络的安全性。同时企业、政府内部的人员有效管理也是很重要的。

5　目前电子商务中所采用的安全技术

5.1　安全协议

（1）安全套接层SSL：SSL被许多知名厂商的Intranet和Internet网络产品所支持，采用对称密码技术和公开密码技术相结合，提供了3种基本安全服务：

秘密性：SSL客户机和服务器之间通过密码算法和密钥的协商，建立起一个安全通道。以后在安全通道中传输的所有信息都经过了加密处理，网络中的非法窃听者所获取的信息都将是无意义的密文信息。

完整性：SSL利用密码算法和hash函数，通过对传输信息特征值的提取来保证信息的完整性，确保要传输的信息全部到达目的地，可以避免服务器和客户机之间的信息内容受到破坏。

认证性：利用证书技术和可信的第三方认证机构，可以让客户机和服务器相互识别对方的身份。为了验证证书持有者是其合法用户（而不是冒名用户），SSL要求证书持有者在握手时相互交换数字证书，通过验证来保证对方身份的合法性。

（2）SET协议采用了对称密钥算法和非对称密钥算法相结合的加密体制，从而充分利用对称密钥算法的速度和非对称密钥算法用于密钥交换的便利性，可以很好地保证网络信息的机密性。SET采用X.509数字证书、数字签名、报文摘要、数字信封和双重签名等技术来保证商家和消费者的身份和商业行为的认证和不可抵赖性。SET由于其高度的安全性和规范性，使其逐步成为目前安全电子支付的国际标准。

5.2　安全技术

5.2.1　网络安全技术

（1）防火墙技术：它可通过监测、限制、更改跨越防火墙的数据流，尽可能地屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。防火墙主要有包过滤防火墙和应用代理防火墙2大类。

（2）虚拟专用网（VPN）技术：为了保证信息在公用网络上的传输安全性，VPN技术采用了认证、存取控制、数据加密、数据完整性的措施，以保证信息在传输中不被窃听、篡改和复制。

（3）入侵检测与漏洞扫描技术：它通过实时截获受保护网络的数据流，能够识别、记录入侵行为和破坏性代码流，寻找网络违规模式和未授权的网络访问尝试。漏洞扫描技术属于安全评估和检测范畴。它是指通过采用网络安全评估和检测工具，用实践性的方法扫描分析网络系统，包括网络设备、防火墙、主机、操作系统等各个方面，检查、报告系统存在的漏洞和安全隐患，并提出补救措施和安全策略，以达到增强网络安全性的目的。

5.2.2　加密技术

（1）私钥加密：又称对称密钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据，目前常用的私钥加密算法包括DES和IDEA等。对称加密技术的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。尤其在BtoC的情况下，商户需要与成千上万的购物者进行交易，密钥管理是一个几乎不可能解决的问题。

（2）公钥密钥加密：信息发送者用公开密钥去加密，而信息接收者则用私有密钥去解密。通过数学的手段保证加密过程是一个不可逆过程，即用公钥加密的信息只能是用与该公钥配对的私有密钥才能解密。常用的算法是RSA、ElGamal等。公钥机制灵活，但加密和解密速度却比对称密钥加密慢的多。

（3）电子信封：发送者自动生成对称密钥，用对称密钥加密钥发送的信息，将生成的密文连同用接收方的公钥加密后的对称密钥一起传送出去。收信

者用其秘密密钥解密被加密的密钥来得到对称密钥，并用它来解密密文。这样保证每次传送都可由发送方选定不同密钥进行，更好的保证了数据通信的安全性。使用混合密码系统可同时提供机密性保障和存取控制。

5.2.3　数字签名

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2种机制结合起来就可以产生所谓的数字签名（Digital Signature）。

5.2.4　认证机构CA和数字证书

对数字签名和公开密钥加密技术来说，都会面临公开密钥的分发问题，即如何把一个用户的公钥以一种安全可靠的方式发送给需要的另一方。这就要求管理这些公钥的系统必须是值得信赖的。数字证书是解决这一问题的有效方法。它通常是一个签名文档，标记特定对象的公开密钥。电子证书由一个认证中心（Certification Authority）签发，它是一个可信的第3方实体，其主要职责是保证用户的真实性。

5.3　最新技术

（1）安全中间件：它屏蔽了安全技术的复杂性，在电子商务、电子政务日渐兴起的今日，安全中间件将迎来广阔的发展空间。

（2）伪装术：伪装术通常依赖于第三方不知道隐蔽通信的存在的假设，而且主要用于互相信任的双方的点到点秘密通信。

（3）数字水印：数字水印在证据篡改鉴定、数据的分级访问、数据的跟踪和检测、商业和视频广播、互联网数字媒体的服务付费以及电子商务的认证鉴定等方面也具有广阔的应用前景。

（4）数据隐藏和数据嵌入：通常用在不同的上下文环境中，在这些应用中嵌入数据的存在是公开的，但无必要保护它们。例如：嵌入的数据是辅助的信息和服务，它们可以是公开得到的，与版权保护和控制存取等功能无关。

6　电子商务中的安全策略

6.1　在实施网络安全防范措施时

（1）加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；（2）用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，并及时加以修补；（3）路由器到用户各级建立完善的访问控制措施，安装防火墙，加强授权管理和认证；（4）利用RAID5等数据存储技术加强数据备份和恢复措施；（5）对敏感的设备和数据要建立必要的物理或逻辑隔离措施；（6）对在公共网络上传输的敏感信息要进行强度的数据加密；（7）安装防病毒软件，加强内部网的整体防病毒措施；（8）建立详细的安全审计日志，以便检测并跟踪入侵攻击。

6.2　网上交易采用电子支付

（1）用卡：常用的信用卡交易协议主要包括SET和SSL；

（2）电子支票（Electronic Check）：eCheck嵌在一个安全电子文件中，内容包括有关支票的用户自定义数据以及在纸制支票上可以见到的信息，比如被支付方姓名、支付方帐户信息、支付金额和日期等；

（3）电子现金：它模拟了现实世界中的货币功能，并采用数字签名等安全技术来保证电子现金的真实性和不可伪造性；

（4）ePass：它可预置密钥或存入数字证书，来确定用户的身份，使系统有效避开了传统身份认证过程的安全隐患，以高度安全的方式完成对网络用户的身份验证过程。

7　结束语

安全是电子商务的核心和灵魂，任何独立的个人或团体都不会愿意让自己的敏感信息在不安全的电子商务流程中传输。因此，发展电子商务安全技术是重中之中。这样才能促进电子商务及电子政务的蓬勃发展，扫平其前进道路上的“安全”障碍。

[参　考　文　献]

[1] 杨明，谢希仁，等. 原理与实践(第二版) [M]. 北京：电子工业出版社，2001.

[2] 韩宝明. 电子商务安全与支付 [M]. 北京：人民邮电出版社，2001.

[3] 张志明，王磊. 信息隐藏技术中的数字水印研究[J]. 计算机工程与应用，2002，38(24).

[4] 习兴春. 电子商务平台的安全体系研究[J]. 计算机工程与应用，2002,38(16).

[5] 沈涛，马红光. 网络数据加密算法研究及其应用[J]. 计算机工程与应用，2002，38(19).