安全电子支付系统研究*)

付 雄[1] 程文青[1] 郎为民[1,2] 谭运猛[1] 熊志强[1]
(华中科技大学电子与信息工程系 武汉430074)[1] (通信指挥学院 武汉430010)[2]

摘 要 给出了电子支付系统的安全需求,并深入探讨了各类安全电子支付系统的基本模型、主要特点和相关实例。同时,基于对安全电子支付系统发展现状和未决问题的分析和评述,指出了今后该领域的研究方向。

关键词 电子支付,微支付,移动支付,电子现金

Research on Secure Electronic Payment System

FU Xiong[1] CHENG Wen-Qing[1] LANG Wei-Min[1,2] TAN Yun-Meng[1], XIONG Zhi-Qiang[1]
(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)[1]
(University of Communication Commanding, Wuhan 430010)[2]

Abstract In this paper, we propose the security requirements of electronic payment system and probe into basic model, main characteristics and typical examples of all kinds of secure electronic payment systems. Furthermore, we point out its development direction based on the analysis and remark of status quo and problems remaining unsolved.

Keywords Electronic payment, Micropayment, Mobile payment, Electronic coin

1 引言

随着 Internet 的迅速发展和广泛应用,人们开始习惯于利用开放快捷的网络进行各种采购和交易,从而导致了电子商务的出现,并使其成为业界新热点。电子商务的显著特点就是增加贸易机会,降低贸易成本,简化贸易流程,提高贸易效率。在交易过程中,消费者、商家、企业、中间结构和银行等需要通过 Internet 网络进行资金的流转,这就需要通过网络支付或电子支付的手段来实现。因此,电子商务活动必然牵涉到支付,安全有效的电子支付系统[1]是电子商务的重要环节。从技术上讲,电子商务最关键的问题是如何安全地实现支付功能,并保证交易各方的安全保密。因此,支付安全是整个电子商务安全的瓶颈,研究和开发适合于商务交易的安全电子支付系统势在必行。

2 电子支付系统的安全需求

不同的电子支付系统[2~6]可能使用不同的电子支付工具,而不同的电子支付工具常常对应于不同的支付形式,因此不同的支付系统完成支付的方法和途径也不尽相同,但是安全、便捷、有效是对各种电子支付系统的共同要求。一个安全的电子支付系统应具备如下基本功能:

1 *消息传输的机密性* 由于电子支付是在开放的网络环境中进行的,交易信息的机密性是电子支付系统得以推广和应用的重要保障。因此,系统要具备防止非法的信息存取和信息在传输过程中被非法窃取的能力,并能对硬件故障、操作错误、网络故障、应用程序错误、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防。

2 *支付交易的安全性* 在电子支付系统中,消费者、商家和银行之间的交易通常都是在虚拟的网络环境中进行的,因而对交易各方的身份进行鉴别显得至关重要。系统应当具备对交易参与者的身份进行认证以鉴别真伪,从而使得交易各方在相互不见面的情况下能够确认对方身份的能力。

3 *支付业务的不可否认性* 支付业务的不可否认性用于保护交易一方对付来自其他各方的威胁,如消费者否认向商家发送了订货单、商家否认收到了消费者的支付指令等。因此,当交易参与者之间发生争议时,系统必须能够为相关的消费者、商家或银行生成并提供足够证据来解决交易各方的纠纷。

4 *交易信息的完整性* 数据输入时的意外差错或传输过程中信息丢失、重复或传送次序变更都可能导致交易各方信息的差异,从而影响到交易的正常进行。因此,系统要能够保护信息不被未授权者伪造、假冒、修改、删除或重放,并能防止传送过程中数据信息的丢失、篡改和重复。

5 *支付业务的多边性* 电子支付以电子形式取代了传统的面对面交易方式,它牵涉到消费者、商家和银行等多方,能否处理交易业务的多边支付问题是进行电子商务的前提。因此,支付系统要保证商家不能读取消费者的支付指令,而银行不能读取商家的购货信息。

3 安全电子支付系统的发展现状

目前的安全电子支付系统大致可以分为五类:基于信用卡的电子支付系统、基于电子支票的支付系统、基于电子现金的支付系统、微支付系统和移动支付系统。

3.1 基于信用卡的电子支付系统

在这种系统中,消费者首先在银行开立一个账户以得到其信用卡的卡号和密码。当消费者在开放网络环境下购物或

*)基金项目:国家自然科学基金资助项目(90104033)。付 雄 博士研究生,研究方向为电子支付、信息安全和应用密码学。程文青 副教授,研究方向为网络安全和下一代互联网。郎为民 博士研究生,研究方向为电子支付、信息安全和传感器网络。谭运猛 博士,副教授,研究方向为网络安全、信息安全和应用密码学。熊志强 博士,研究方向为信息安全、传感器网络和应用密码学。

索取服务时，他需要把信用卡的号码和口令进行加密后，通过互联网络传送给商家，再由商家转发给银行，然后依照特殊协议进行网上支付。其模型如图1所示，整个支付过程包括对消费者、商家及付款请求的合法性验证。

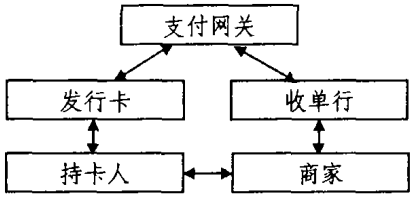

图1　基于信用卡的电子支付系统模型

基于信用卡的电子支付系统的主要特点是：每张电子信用卡代表着一个账户，银行通过转账实现消费者的付款功能。消费者先取得商品或服务，后通过银行进行支付，银行对信用卡账户的处理滞后于贷款支付，因此它与电子转账有本质的区别，是一种"延迟付款"的支付方法。电子信用卡支付系统需采用在线操作，允许透支。目前基于信用卡的电子支付系统主要有 First Virtual、CyberCash 和 iKP 等。

3.2　基于电子支票的支付系统

消费者向商家递送电子支票，电子支票是一个带有消费者数字签名的电子报文或数字电文。商家将其存入可以提供电子支票服务的银行，并凭借电子支票兑换等额的现金，其模型如图2所示。

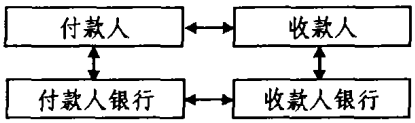

图2　基于电子支票的支付系统模型

基于电子支票的支付系统的主要特点是：它属于"即时付款"的一类支付方法，在付款人对支付确认后，即开始对账户的处理过程。账户处理完毕，支付过程也就结束。即时付款实现起来最复杂，因为在交易过程中必须直接访问银行的内部数据库，且安全措施要比其它付款类型更严格。此系统需采用在线操作的支付方式，不可以透支，适用于小额的结算。目前开发的基于电子支票的支付系统比较多，如 NetCheck、NetBill、FSTC 电子支票系统和 NACHA 网上支付系统等。

3.3　基于电子现金的支付系统

消费者在提供电子现金服务的银行开立一个账户，并预先存入资金，从而取得与现金货币值相同的电子现金（通常是可存储的智能卡或纯电子形式的硬盘文件），然后使用电子现金终端软件下载到自己的计算机硬盘上备用，用以支付后续所购商品的费用，最后接收消费者电子现金的商家与授权的电子现金银行进行结算，银行将消费者购买商品或索取服务的费用转给商家，其模型如图3所示。

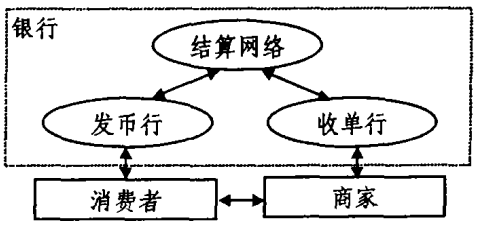

图3　基于电子现金的支付系统模型

基于电子现金的支付系统的主要特点是：它属于"预先付款"的一类支付系统，先付款后交易。消费者通过预付资金先取得等值的电子现金，并将其保存到硬盘或智能卡上以备后用。它不直接对应任何账户，而且可以离线操作。目前已开发出来的基于电子现金的支付系统包括 NetCash、Worldpay、CyberCoin、CAFé 和 Ecash 等。

3.4　微支付系统

消费者向经纪人购买票据或获取证书，然后在线浏览商家网页选择待购商品或服务生成订购信息，并通过使用票据等数字货币与商家执行支付协议，得到所需商品或服务。商家则通过与经纪人进行结算完成现金转账，其模型如图4所示。

微支付系统的主要特点是：交易额非常小，在满足一定安全性的前提下，要求它有尽可能少的信息传输、较低的管理和存储需求，即速度和效率要求比较高。其安全性主要是通过审计或管理策略来保证，一般适用于交易费用相当低或手续简便的系统。目前的微支付系统包括 Millicent、CyberCash、PayWord、Subscrip 和 MicroMint 等。

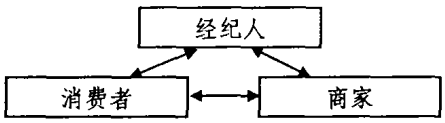

图4　微支付系统模型

3.5　移动支付系统

消费者通过移动电话无线上网，浏览服务提供商网站，生成订单信息并将其与数字证书、支付信息提交给服务提供商。服务提供商将消费者的支付信息送给支付网关，并由支付网关将其传送给金融机构。金融机构根据用户的账户信息，进行转账，并且将结果通过支付网关返回给服务提供商。服务提供商在收到了支付网关的确认之后，将商品或服务提供给用户，其模型如图5所示。

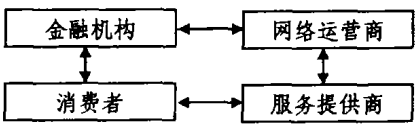

图5　移动支付系统模型

移动支付系统最大的特点在于其独特的随身性和便携性，可以为消费者提供各种贴身的服务。由于支付金额较小，因而系统结构相对简单，它可以避开目前移动领域还不成熟的、复杂的公钥安全系统。目前已开发出来的移动支付系统主要包括 Paybox、Sonera MobilePay、GiSMo 和移动 Set 等。

4　安全电子支付系统的研究方向

由于电子支票和信用卡支付系统本身存在的非匿名性，且信用卡支付系统已形成国际标准，因而这两个方向并未引起人们的极大兴趣，安全电子支付系统的研究热点主要集中在电子现金支付系统、微支付系统和移动支付系统上。目前已开发出多种电子支付系统，然而多数都是在封闭的专用网络上运行的。虽然它们在某些国家或某一地区具有一定的市场，但从总的来看，仍然存在着如下尚未解决的实际问题：

①没有一种电子支付安全的完整解决方案、支付模型与体系结构。尽管一些系统正逐渐成为标准，但仅有很少几个标准的 API。从开放市场的角度来看，协议间的通用 API 和网

关是绝对需要的；

②大多数电子支付系统都是封闭式的，即使用专有技术，仅支持一些特定集合的协议和机制。这些支付系统通常需要一个中央服务器作为所有参与者的可信第三方，有的甚至要求使用特定的服务器或浏览器；

③尽管大多数方案都使用了公钥密码，但多方安全受到的关注远远不够，消费者的匿名性和隐私也还未得到充分的考虑。大多数系统都限制为两方，因此难于集成一个安全连接到第三方，且没有建立一种解决争议的决策程序；

④大多数系统都将销售商服务器和消费者浏览器间的关系假设为主从关系，这种非对称关系限制了在这些系统中执行复杂的协议，而且不允许消费者之间进行直接交易；

⑤所有方案和产品都仅考虑了在线销售，但很少考虑多方交易问题（如拍卖）和公文交换问题（如签合同和可证实电子邮件）等。

结论 本文旨在研究电子支付系统的安全性，我们首先给出了电子支付系统的安全需求：消息传输的机密性、支付交易的安全性、支付业务的不可否认性、交易信息的完整性和支付业务的多边性，从基于信用卡的电子支付系统、基于电子支票的电子支付系统、基于电子现金的电子支付系统、微支付系统和移动支付系统五个方面给出了当前各种安全电子支付系统的基本模型、主要特点及实例代表。最后，对安全电子支付系统的发展现状及未决问题进行了深入的分析和评述，指出了该领域未来的研究方向。

参 考 文 献

1 O'Mahony D, Peirce M, Tewari H. Electronic payment systems for E-commerce. Boston: Artech House, 2003

2 Kalden R, Meirick I, Meyer M. Wireless Internet acess based on GPRS. IEEE Personal Communications, 2000, 7 (2): 8～18

3 Rivest R L, Shamir A. PayWord and MicroMint: Two simple micropayment schemes. In: Lomas M, ed. Security Protocols--International Workshop, Berlin: Springer-Verlag, 1997

4 Lang Weimin, Yang Zongkai, Liu Gan, et al. A New Efficient Micropayment Scheme Against Overspending. In: J. Carlsen ed. Proc. of The Ninth IEEE Symposium on Computers and Communications (ISCC 2004). Los Alamitos, California: IEEE Computer Society, 2004. 137～143

5 Yang Zongkai, Lang Weimin, Yun Mengtan. A New Fair Micropayment System Based on Hash Chain. In: Soe-Tsyr Yuan, Jiming Liu eds. Proc. of IEEE Intl. Conf. on e-Technology, e-Commerce, and e-Service (EEE'04), Los Alamitos, California: IEEE Computer Society, 2004. 139～145

6 郎为民，杨宗凯，谭运猛. 一种可提升用户匿名性的离线电子支付方案. 计算机工程，2004，30 (1)：30～32

（上接第105页）

8 Pâris J F, Cater S W, Long D D E. Effocoent broadcasting protocols for video on demand. In: Proc. of MASCOTS'98, July 1998. 127～132

9 Pâris J F, Cater S W, Long D D E. A low bandwidth broadcasting protocol for video-on-demand. In: Proc. of IC3N'98, Oct. 1998. 690～697

10 Pâris J F, Cater S W, Long D D E. A hybrid broadcasting protocol for video-on-demand. In: Proc. of MMCN'99, Jan. 1999. 317～326

11 Paris J F. A simple low-bandwidth broadcasting protocol for video-on-demand. In: Proc. of IC3N'99, Oct. 1999. 118～123

12 Dan A, Sitaram D, Shahabuddin P. Schduling policies for an on-demand video server with batching. In: Proc. of ACM Multimedia. San Francisco, California, Oct. 1994. 15～23

13 Aggarwal C C, Wolf J L, Yu P S. The maximum factor queue batching scheme for video-on-demand systems. IEEE Trans. Computers, 2001, 50(2): 97～110

14 杨灿，徐重阳，刘政林. VOD系统批处理调度策略优化研究. 计算机学报，2002，25(11)：1263～1268

15 Hua K A, Cai Y, Sheu S. Patching: A multicast technique for true video-on-demand services. In: Proc. of ACM Multimedia, Britstol UK, Sept. 1998. 191～200

16 Cai Y, Hua K A, Vu K. Optimizing patching performance. In: Proc ACM/SPIE Multimedia Computing and Networking. Jan. 1999. 203～215

17 White P P, Crowcroft J. Optimized batch patching with classes of service. ACM Communications Review, 2000, 30(4)

18 Venkatramani C, Verscheure O, Frossard P, Lee K W. Optimal proxy management for multimedia streaming in content distribution networks. In: ACM NOSSDAV 2002, Miami Beach, FL, USA, May 2002. 147～154

19 Frossard P, Verscheure O. Batch patch caching for streaming media. IEEE Communications Letters, 2002, 6(4): 159～161

20 Carter S W, Long D D E. Improving video on demand server efficiency through stream tapping. In: Proc. IEEE ICCCN'97. Las Vegas, NV, Sept. 1997. 200～207

21 Gao L X, Towsley D. Supplying instantaneous video on demand services using controlled multicast. In: Proc. IEEE Int. Conf. Multimedia Computing and Systems, 1999, 2: 117～121

22 Eager D L, Vernon M K, Zahorjan J. Minimizing bandwidth requirements for on-demand data delivery. IEEE Trans. on Knowledge and Data Engineering, 2001, 13(5): 742～757

23 Eager D L, Vernon M K. Dynamic skyscraper broadcasts for video-on-demand. In: Proc. of MIS'98, Istanbul, Turkey, Sept. 1998

24 Eager D L, Vernon M K, Zahorjan J. Minimizing bandwidth requirements for on-demand data delivery. In: Proc. 5th Int'l Workshop on Multimedia Information Systems, Indian Wells, CA, Oct. 1999. 80～87

25 Eager D L, Vernon M K, Zahorjan J. Optimal and efficient merging schedules for video-on-demand servers. In: Proc. of ACM MULTIMEDIA'99, Orlando, FL, Nov. 1999. 199～203

26 Coffman E G, Jelenkovic P, Momcilovic. Provably efficient stream merging. In: Proc. the 6th Intl. Workshop on Web Caching and Content Distributio, 2001

27 Bar-Noy A, Ladner R E. Competitive on-line stream merging algorithms for media-on-demand. In: Proc. the 20th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2001. 364～373

28 Bar-Noy A, Goshi J, Ladner R E, Tam K. Comparison of stream merging algorithms for media-on-demand. In: Proc. Conf. on IS&T/SPIE MMCN'2002, San Jose, CA, Jan. 2002. 115～129

29 Poon W-F, Lo K-T, Feng J. Determination of efficient transmission scheme for video-on-demand (VOD) services. IEEE Trans. on Circuits and Systems for Video Technology, 2003, 13(2): 188～192

30 Tseng Y-C, Yang M-H, Hsieh C-M, et al. Data broadcasting and seamless channel transition for highly demanded videos. IEEE Trans. on Communications, 2001, 49(5): 863～874

31 Guo Y, Gao L, Towsley D, Sen S. Seamless workload adaptive broadcast. In: Proc. of Intl. Packetvideo Workshop, Pittsburgh, PA, April 2002

32 Guo Y, Sen S, Towsley D. Prefix caching assisted periodic broadcast: framework and techniques to support streaming for popular videos. In: Proc. of IEEE ICC'2002, April 2002