文章编号: 1001-0920(2005)04-0463-04

3D 安全协议的改进及应用

吴小强[1], 刘 晶[2], 李秀生[2], 邱菀华[1]
(1. 北京航空航天大学 经济管理学院, 北京 100083; 2. 中国工商银行 软件开发中心, 北京 100081)

摘 要: 改进 3D 安全协议, 引入支付认证交易码, 使得 3D 安全协议中的 3 个域间在保护敏感隐私信息的前提下进行安全交易. 应用该协议给出跨国跨行网上银行个人转帐模型, 表明改进的 3D 安全协议可在不披露汇款人信用卡号的前提下进行安全转帐, 保障了交易中各参与者彼此间的信息隐私, 并创新了汇款方式.

关键词: 3D 安全协议; 隐私保护; 电子商务; 汇款
中图分类号: TP393; TP317 **文献标识码**: A

Improvement and application of 3D secure protocol

WU Xiao-qiang[1], *LIU Jing*[2], *LI Xiu-sheng*[2], *QIU Wan-hua*[1]
(1. School of Economics and Management, Beijing University of Aeronautics and Astronautics, Beijing 100083, China; 2. Beijing Software R and D Center, Industrial and Commercial Bank of China, Beijing 100081, China. Correspondent: WU Xiao-qiang, E-mail: wuxiaoqiang@buaa.edu.cn)

Abstract: An improvement on 3D secure protocol is proposed for securing E-commerce transactions. PATV (Payment Authentication Transaction Value) is introduced to protect privacy information in the overall e-business process. An internet banking system of cross-border remittances is demonstrated and integrated with the proposed improved protocol. It shows that remittance transactions can be securely performed without disclosing sender's credit card number information among the members in 3D SET. In addition, a novel way for remittance is provided.

Key words: 3D secure protocol; privacy protecting; E-commerce; remittance

1 引 言

近年来, Internet 技术的提高促进了电子商务的发展, 在线支付需求也大大增加, 而电子渠道的扩展带来了网上支付的欺诈风险[1]. 1999 年 VISA 组织在电子商务领域引入 3D 安全协议, 并在欧洲区推行, 至 2003 年已在全球范围内采用了 3D 安全协议, 并要求各发卡行和收单行支持该规范[2]. 3D 安全协议的目标是给发卡行提供一个持卡人身份许可的环节, 减少使用 VISA 卡进行欺诈的可能性, 从而提升交易安全性能. 但是, 目前 3D 安全协议对电子交易中敏感隐私信息(如信用卡号等)的保护考虑不足, 在整个电子交易流程中, 持卡人信用卡号可被 Visa, 商户或收单行获取, 这种模式增加了持卡人的风险.

Jing-jang Hwang 提出了对隐私保护的概念模型[3]. 本文结合该概念规则和 VISA 的 3D 安全协议提出改进的 3D 安全协议, 并将改进的安全协议应用于跨国跨行网上银行转帐模型.

2 3D 安全协议概述

3D 安全协议涉及的组织是: 收单行域: 包括商户和收单行; 发卡行域: 包括持卡人和发卡行; 协作域: 包括可信第 3 方(TTP), 本文指 VISA. 在基于 3D 安全协议的电子商务模式下, 电子商务流程如图 1 所示, 具体步骤如下:

1) 持卡人向商户发出带有其支付信用卡卡号的购买请求.

收稿日期: 2004-06-21; **修回日期**: 2004-10-08.
基金项目: 国家自然科学基金项目(70372011); 国家"十五"科技攻关计划专题项目(2001BA 102A 06-09).
作者简介: 吴小强(1977—), 男, 陕西咸阳人, 博士生, 从事电子商务、网上支付等研究; 邱菀华(1946-), 女, 江西临川人, 教授, 博士生导师, 从事项目管理、决策与风险理论等研究.

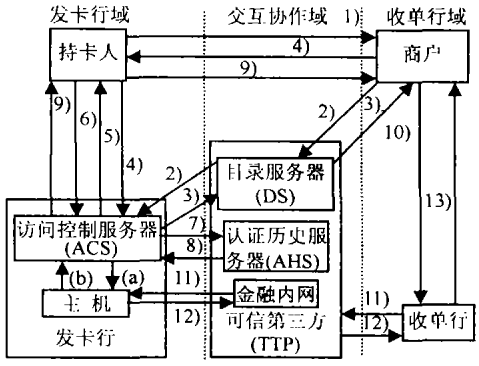

图 1 3D 安全协议基本流程

2) MPI 将卡号等数据按照 VEReq 格式组织数据送可信第 3 方目录服务器 DS, DS 判断该卡所属发卡行, 发卡行检查卡号是否在合法卡号范围之内, 若在此范围内, 则查询发卡行的访问控制服务器 ACS, 以确定该卡是否已在 ACS 上注册.

3) ACS 处理 VEReq 后将 VERes 返回给 DS, DS 收到 ACS 响应后将 VERes 返回 MPI.

4) 商户向发卡行发出认证请求 PAReq.

5) ACS 收到请求信息后处理商户的校验认证请求 PAReq 的要求, 无误后要求持卡人输入网上交易的密码来认证身份.

6) 持卡人向 ACS 系统提交网上交易支付密码.

7) ACS 系统根据持卡人密码确认持卡人身份, 无误后生成持卡人身份验证值 CAVV, 并将支付认证信息和交易状态信息按照 PATransReq 的形式发给可信第 3 方的 AHS 保存备案.

8) 可信第 3 方的 AHS 处理 PATransReq 完成后, 按照 PATransRes 格式返回给 ACS 系统.

9) ACS 系统以 PARes 的格式将支付认证响应信息返回给 MPI.

10) MPI 收到响应信息后校验签名, 然后将 CAVV 等信息和卡号、金额等要素与 ECI 值组成授权交易数据包, 再向收单行转发认证校验请求.

11) 网上授权数据按照电子商务消费授权的流程, 通过收单行主机经金融内网送发卡行主机. 网上授权数据转发至发卡行进行认证校验, 如果成功, 则发卡行经收单行转发认证校验成功信息并转发批量转帐; 如果认证校验失败, 则由收单行转发认证校验失败信息并拒付.

12) 发卡行主机拆包后检查 ECI 值、校验 CAVV、进行授权检查, 并将校验结果由内网返回收单行;

13) 收单行将 ACS 系统返回的校验结果转发到商户, 商户根据认证校验成功失败信息确定是否发货.

在以上基于 3D 安全协议的认证支付交易流程中, 步骤 1)～步骤 10) 和步骤 13) 为开放系统的交易步骤, 步骤 11) 和步骤 12) 为金融网内的主机认证交易. 图 1(a) 和(b) 是 ACS 系统向主机系统请求和响应生成 CAVV[2]. 在交易前为确保交易实体的合法性, 在支付流程中对各参与者的操作进行数字签名[5].

3D 安全协议是一种基于可信第 3 方 TTP 的安全协议. 基于 TTP 的安全协议在近年得到很大的发展, 如 Needham/Schroeder 协议和 Kerberos 协议[4].

3 3D 安全协议的改进方法

3.1 隐私信息保护的规则和约定

为了保护持卡人卡号和订单等敏感隐私信息, 提出如下两个原则:

规则 1 在整个安全模型流程中, 需强调持卡人的卡号信息只能由持卡人和发卡行掌握, 商户和收单行不必了解持卡人的卡号信息[6,7].

规则 2 只有持卡人和商户掌握订单信息, 而发卡行与收单行不必了解订单的具体内容.

披露卡号信息易导致持卡人受到攻击. 商户一般不具备设计专门安全设施的技术, 在其服务器上保留大量的持卡人的卡号信息容易成为攻击的目标, 也给有恶意的商户留下可乘之机, 他们可能使用卡号进行欺诈性交易.

为便于描述协议作如下约定: CH 为持卡人; M 为商户; CR 为卡号范围; S 为汇出人; R 为汇入人; PM 为收单行的 Pseudo-MPI; A 为收单行; TTP 为可信第 3 方; Sx(m) 为被 X 的私钥签名消息 m; DSx(m) 为被双重签名的消息, 该签名可使用 X 的私钥解密; ENVx(m) 为数字信封保护的消息 m, 该消息可使用 X 的公钥解密; ENC(X) 为通过硬件手段对 X 进行加密; PI 为支付信息; OI 为转帐或订单信息.

3.2 改进的 3D 安全协议

根据以上规则, 提出了改进的 3D 安全协议. 在输入步骤 1) 的 MPI 界面时, 不再输入信用卡的卡号, 而是输入或从注册信息中获取持卡人的卡号范围 CR, 即卡的前 6 位. 同时, 需要提出一个贯穿交易全程的唯一不可伪造的支付认证交易码 PATV. 自步骤 2) 步起, 每一步的消息包中都增加了 PATV.

设计 PATV 要求如下: 1) 随机产生; 2) 唯一不重复; 3) 给定输入参数可再次产生. 加密位不可解密, 即理论上无法伪造, 可采用硬件加密机计算. 支付认证交易码 PATV 可表示为

$$\mathrm{PATV} = \mathrm{TimeStamp} + \mathrm{StochasticNumber} + \mathrm{ENC}(\mathrm{StochasticNumber}). \quad (1)$$

其中: TimeStamp 为时间戳, 共 17 位; StochasticNumber 为软件生成的随机数, 共 4 位; ENC 为对以上随机数硬件加密产生的 4 位数字.

图 2 是改进的 3D 安全协议流程. 其中, 自步骤 3) 开始每一步的信息中需要增加 PATV 信息, 除此变化外, 3D 安全协议中还需要修改的步骤有步骤 1)～步骤 3) 和步骤 6), 步骤中详细内容如下:

1) $CH \rightarrow M$: $CR_{CH} \| DS_{CH}(OI) \| ENV_A\{DS_{CH}(PI)\}$;

2) $M \rightarrow TTP$: $E_{KV}\{CR_{CH} \| DS_{CH}(OI) \| ENV_A\{DS_{CH}(PI)\} \| PATV\}$;

3) $TTP \rightarrow M$: $E_{KV}\{ACSURL \| PATV \| CR_{CH} \| DS_{CH}(OI) \| ENV_A\{DS_{CH}(PI)\}\}$;

6) $CH \rightarrow I$: $E_{KV}\{PATV \| ID_{CH} \| P_{CH} \| ID_V\}$.

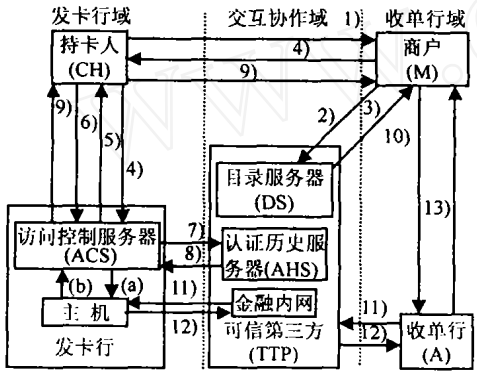

图 2　改进的 3D 安全协议基本流程

图 2 中, CR 表示长度为 6 位的卡号范围, 信用卡号码前 6 位若为"427030", 从可信第 3 方即可返回为中国工商银行为发卡行电子支付认证 URL.

4　应用改进 3D 安全协议的跨国跨行网上银行转账模型

改进的 3D 安全协议可用于跨国跨行的网上银行转帐汇款个人业务, 本文给出一个基于改进 3D 安全协议的跨国跨行网上银行转帐模型, 应用改进的 3D 安全协议的发卡行设计简化类如图 3 所示.

图 4 是跨国跨行网上银行转帐模型交易时序图. 在收单行系统中 Pseudo-MPI 是必不可少的模块之一. 本文将跨国跨行网上银行转帐的详细流程划分为 15 步, 其中步骤 1)～步骤 10) 和步骤 13) 为开放系统的交易步骤, 步骤 11) 和步骤 12) 为金融网内的主机认证交易, 步骤 14) 和步骤 15) 为柜面或自助机交易, 每一步消息的内容见图 5. 详细流程如下:

1) $S \rightarrow PM$: $CR_S \| DS_S(OI) \| ENV_A\{DS_S(PI)\}$;

2) $PM \rightarrow TTP$: $E_{KV}\{CR_S \| DS_S(OI) \| ENV_A\{DS_S(PI)\} \| PATV\}$;

3) $TTP \rightarrow PM$: $E_{KV}\{ACSURL \| PATV \| CR_S \| DS_S(OI) \| ENV_A\{DS_S(PI)\}\}$;

4) $PM \rightarrow S$: $E_{KV}\{ACSURL \| PATV \| CR_S \| DS_S(OI) \| ENV_A\{DS_S(PI)\}\}$;

$S \rightarrow I$: $E_{KR_{CH}}\{ACSURL \| PATV \| CR_S \| DS_S(OI) \| ENV_A\{DS_S(PI)\}\}$;

5) $I \rightarrow S$: $E_{KV}\{PATV \| DS_S(OI) \| ENV_A\{DS_S(PI)\}\}$;

6) $S \rightarrow I$: $E_{KV}\{PATV \| ID_S \| P_S \| ID_V\}$;

7) $I \rightarrow TTP$: $E_{KV}\{PATV \| CAVV \| E_{KV}\{DS_I(OI) \| DS_S(PI)\}\}$;

8) $TTP \rightarrow I$: $E_{KV}\{PATV \| CAVV \| E_{KV}\{DS_{TTP}(DS_I(OI) \| DS_S(PI))\}\}$;

9) $I \rightarrow S \rightarrow PM$: $E_{KV}\{PATV \| CAVV \| E_{KV}\{DS_I(DS_S(PI)) \| DS_I(DS_S(OI))\}\}$;

10) $PM \rightarrow A$: $E_{KV}\{PATV \| CAVV \| E_{KV}\{DS_I(DS_S(PI)) \| DS_I(DS_S(OI))\}\}$;

13) $A \rightarrow PM$: $E_{KV}\{PATV \| E_{KV}\{DS_I(DS_S(PI)) \| DS_I(DS_S(OI))\}\}$;

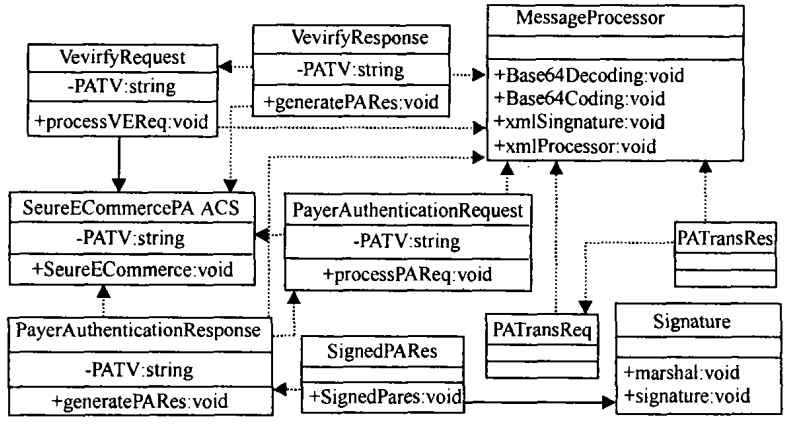

图 3　发卡行 ACS 系统设计简化类

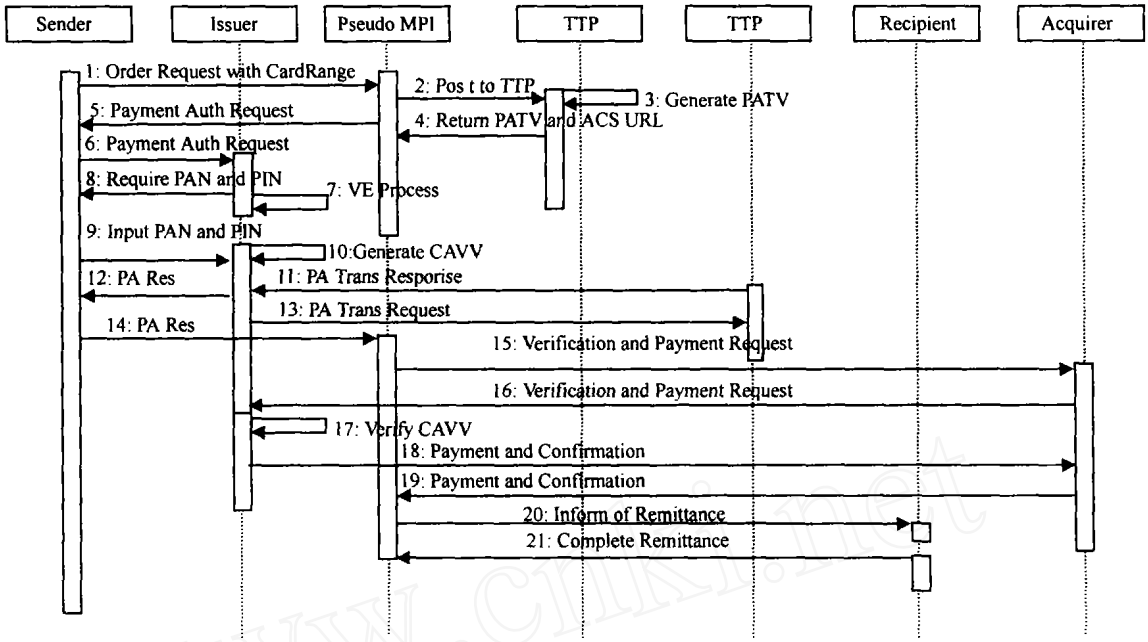

图 4 跨国跨行网上银行转帐模型交易时序

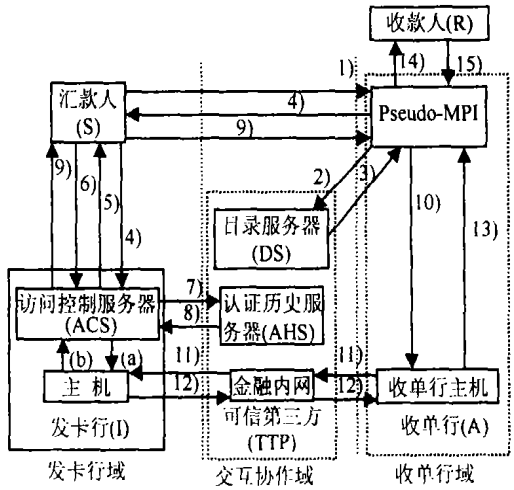

图 5 应用改进 3D 安全协议的网上转帐模型

5 结 论

几乎在所有实用的安全电子商务协议中, 可信第 3 方都不同程度地发挥作用. 基于可信第 3 方的安全协议在理论研究和商业应用中都将深入地发展[8]. 通过对 3D 安全协议的改进和在跨国跨行网上转帐模型中的应用, 可得出结论: 1) 敏感信息(如信用卡号) 得以保护, PATV 确保了只有发卡行和持卡人具有持卡人的卡号信息, 而 3D 协议中其他成员了解的是持卡人的卡 BIN, 即卡号前 6 位的卡号范围; 2) 改进的 3D 安全协议具有事后离线审计与仲裁特性; 3) 改进后的 3D 安全协议同时具有 3D 安全协议自身的优点, 如在线3方电子商务即时校验的安全性能等.

参考文献(References)

[1] Ranganathan C, Ahobha Ganapathy. Key dimensions of business-to-customer web sites[J]. *Information and Management*, 2002, 39(1): 457-465.

[2] Visa Int Service Association. 3D Secure protocol specification core functions [EB/OL]. http://international visa.com/fb/paytech/secure/main.jsp. 2003/2004-01-07.

[3] Hwang J J, Yeh T C, Li J B. Securing on-line credit card payments without disclosing privacy information [J]. *Computer Standards and Interfaces*, 2003, 25(2): 119-129.

[4] Wu X Q, A hybrid approach in intelligent workflow modeling using Petri nets and neural network for inter-organizational cooperation [A]. *The 8th Int Conf on CSCW in Design* [C]. Xiamen, 2004: 307-311.

[5] Coffey T, Saidha P. Non-repudiation with mandatory proof of receipt [J]. *Computer Communication Review*, 1996, 26(1): 6-17.

[6] Petra van Krugten, Mark Hoogenboom. B2C security-be just secure enough [J]. *Computers and Security*, 2000, 19(4): 348-356.

[7] Eloy Portillo, Ahmed Patel. Design methodology for secure distributed transactions in electronic commerce [J]. *Computer Standards and Interfaces*, 1999, 21(3): 5-18.

[8] Mikael R Jensen, Thomas H Moller, Torben Bach Pedersen, et al. Converting XML DTDs to UML diagrams for conceptual data integration [J]. *Data and Knowledge Engineering*, 2003, 44(7): 323-346.