一种防超额花费的小额电子支付协议*)

姬东耀　冯登国

(中国科学院研究生院信息安全国家重点实验室　北京100039)

摘　要　本文提出一个新的小额电子支付协议，新协议继承了现有小额电子支付协议的优点，同时提供了一种防用户超额花费的机制，有效地解决了用户利用有限信用作超额花费的问题。最后对新协议的安全性和运行效率进行了分析。

关键词　小额支付，密码协议，概率检测

A Micropayment Protocol Against Overspending

JI Dong-Yao　FENG Deng-Guo

(State Key Laboratory of Information Security, Graduate School, Chinese Academy of sciences, Beijing 100039)

Abstract　This paper presents a new micropament protocol. This protocol provides security services required by regular micropament protocol and is secure against overspending. Finally, the security and the efficiency of the new protocol are analyzed in detail.

Keywords　Micropament, Cryptographic protocol, Probabilistic checking

1　引言

因特网上存在着大量的信息服务，这些信息服务具有信息源的多选择性、可即时获取性等优点，用户可从网上快捷地获取有价值的信息，因而这种信息服务蕴藏着巨大市场。但是很多信息服务都是低值的，像网上视频点播、网上阅读，网络广告，金融市场报价单、网络数据库查询等数字服务业务。在传统商务中，这些服务通常都采用预定支付方式，用户预先支付，然后定期收到服务和产品。这虽然保证了服务提供者得到支付，但它把大量仅仅偶尔需要服务的用户隔离在外，它也限制了人们尝试新服务的机会。若采用常规电子支付协议实现时，为了保证电子支付系统安全可靠地运行，电子支付中都引入了公钥加密和数字签名，在支付过程中，至少要有一个数字签名生成和验证。因为可证明安全支付协议依赖于它所使用的数字签名的安全性，所以支付协议所选用的数字签名方案越安全可靠性越好。但是，数字签名的复杂性使得支付方案的执行效率降低，也就是说，执行支付交易所需要的时间与签字的生成和验证过程紧密相关，而执行协议设备的存储量要依赖于签字的长度。一般情况下，大额常规支付所做支付的成本也高，允许采用这样的结构。当被支付物价值本身就很低时(例如每次¥0.001-¥1)，其支付成本也要求很低，用较复杂的支付方案就不具有实用价值。针对于此，可行的方法是构造出协议结构简单处理高效的支付形式，即小额的支付系统。小额电子支付适用于支付额低，重复频率高，支付额不固定的支付场合。小额电子支付存在许多应用，范围包括电子出版，电子计量，电信和信息服务，网络视频服务和第三代移动通信等。

小额支付的概念是在1995年提出的，并很快得到广泛研究。提出的方案可以分为两类，一类是基于代金券的小额支付方案，像 Milicent[1,2]、SubScrip[3]；另一类是基于杂凑链的小额支付方案，如 Payword[4]、MicroMint[4]、NetCard[5]，μ-iKP[6]，Pederson 提出的方案[7]。

Millicent 没有使用公钥密码运算，对于重复的向同一商人作小额支付是最优的。它的支付方式允许验证支付是否有效，交易期间不需要在线接触可信第三方，适合于价位低于十分之一分的小额支付。它的缺陷是顾客需要相继对多个商人支付时必需相继地接触这些商人的经纪人。

SubScrip 对于重复的向同一商人作小额支付同样是最优的。但是，用户需要在商人处设一临时账户将迫使用户必须在一商人处花费一定量的钱，所以它更适合取代短期预定服务或对一需要定期访问的商人作小额支付。

PayWord、micro-iKP、NetCard 及 Pederson 协议克服了 Millicent 和 SubScrip 协议当顾客需要相继对多个商人支付时必需相继地接触这些商人的经纪人的缺陷，而且不需要找零。但它们都是基于信用的方案，大量的购买依靠一个没有充分多金额的账户进行支付，给超额花费创造了机会。本文提出一个新的小额电子支付协议，继承了现有方案的优点，同时可以防止用户超额花费。

2　新的小额支付协议 NMP

NMP 协议的参加方还是用户 U、信息商品供应商 V、银行 B。新协议不需要银行 B 在线参与交易，但提供一种概率检测机制防止用户超额花费。银行初始化时，依据每个用户的信用和过去交易记录选取两个常数 c 和 M，其中 c 是预期的用户消费到他的信用限度银行所需检测次数；M 是一门限值，当银行检测到 M 个消息后开始怀疑用户超额花费。对于每个用户，银行存储信息 $I_U=\{\omega_U, x_U, L_U\}$。$\omega_U$ 是银行 B 允许用户 U 花费的金额，x_U 是一检测消息数记数变量，初始为0；L_U 是一商家列表，和用户有交易的商家都在其中，初始为空。协议流程如下。

*)基金项目：国家自然科学基金项目(编号：60273029，60025205)。

2.1 用户登记子协议

一个用户 U 想从 V 得到信息商品，他首先必须在一 U 和 V 都信任的银行 B 处申请一账户和一用杂凑链作支付的证书，证书包含银行名 B、用户名 U 及 IP 地址 A_U、用户公钥 K_U^+ 及有效期 E 和 $f_U=c/\omega_U$。证书必须由银行 B 按期更新(每月或年)，更新的条件是用户的账户可以支付，而且用户的公钥证书没有过期或吊销，同时在用户存入数量 ω 的电子现金时重新计算 f_U。证书的格式为：

$C_U=\{B,U,A_U,K_U^+,E,f_U\}_{K_B^-}$

2.2 服务请求子协议

用户通过浏览器选择信息商品，包括第 i 个信息商品的标识 Id_i，计费单位 L_i，价格 P_i，信息商品包含的记费单位数 m_i，U 选取的随机数为 w_n'，生成一条杂凑链 $w_0',w_1,w_1',w_2,w_2',\cdots,w_n,w_n'$，其中 $w_i=h(w_i')$，$w_{i-1}'=h(w_i)$，$i=n,n-1,\cdots,1$。w_0'叫做杂凑链的根，用户可以利用它向服务提供者承诺。U 然后执行：

1. $U\rightarrow V$：$C_U,Id_i,P_i,Li,m_i,w_0',T_i,\{V,C_U\ Id_i,P_i,L_i,m_i,w_0'T_i,\}_{K_U^-}$

IF $P_if_U\leqslant 1$ THEN V 接受服务请求并转发消息1到银行 B

银行 B 检查消息1：IF $x_U<M$ THEN 向 V 发送同意交易信息。

2. $V\rightarrow U$：$\{\{U,Id_i,T_i,K_S\}_{K_V^-}\}_{K_U^+}$

ELSE 向 V 发送拒绝交易信息。

ELSE V 拒绝服务请求。

其中，T_i 为一时戳，K_S 是由 V 提供的解密将要传送的信息商品的密钥。

2.3 服务子协议

V 和 U 相互认证并建立会话密钥后，V 把信息商品分成 n 个单位，开始逐单位为 U 提供信息商品，用户 U 把 (w_i,w_i') 组成一对，作为他对一个单位信息商品的支付，每次用户 U 首先向 V 发送前一半 w_i，V 检查是否有 $w_{i-1}'=h(w_i)$，若不相等，则不提供第 i 个单位信息商品；若相等，则提供第 i 个单位信息商品。当 U 得到第 i 个单位信息商品时，再提供另一半 w_i'。同时，V 把存储的前一个杂凑值 w_{i-1}'修改为 w_i'，作为从 B 得到支付的证据。若 U 提供了前一半 w_i，但 V 没有提供第 i 个单位信息商品；或者 U 得到了第 i 个单位信息商品，但没有提供另一半 w_i'，B 按照 U 得到 i 个单位信息商品记费，而 V 也只能得到 $i-1$个单位信息产品的费用，第 i 个单位信息商品的费用充公用于公益事业。这样 U 和 V 无论谁中断都得不到好处，并且协议也不会带来通信负荷的增加，因为 w_i' 可以和 w_{i+1}合在一起发送。进一步因为 w_i' 可以从 w_{i+1}计算出来，所以可以只发 w_{i+1}。

1. $U\rightarrow V$：w_1,1； 2. $V\rightarrow U$：第一单位信息商品

3. $U\rightarrow V$：w_2,3； 4. $V\rightarrow U$：第二单位信息商品

… …

2n−1. $U\rightarrow V$：w_n,$2n-1$

2n. $V\rightarrow U$：最后一单位信息商品

2n+1. $U\rightarrow V$：w_n',$2n$

同时在服务协议中增加概率性检测机制，V 每从 U 收到一个支付，它以概率 $p=P_if_U(=\frac{P_i}{\omega_U}*c)$把 U 的名称发给 B。银行 B 每次收到关于 U 的报告后，给记数变量 x_U 加1，当 x_U 达到 M 时，B 向列表 L_U 中所有商家组播一警告消息，商家收到这一消息后，停止和 V 交易。

2.4 支付兑现子协议

在每天(或别的适当日期)的结束，V 把他最后收到的每条杂凑链的值及服务请求协议中的消息发给经纪 B，B 根据最后收到的每条杂凑链的值可以计算出用户得到的服务单位数(假如 V 收到的最后一个杂凑值为 w_i'，由于 $h^{2(n-i)}(w_i')=h^{2n}(w_n')=w_0'$，这表明 V 向 U 提供了 c 个单位信息商品)。再根据每个单位的价格，B 可以计算出 U 应该支付给 V 的钱数，并从 U 的帐户扣除相应数量和给 V 的帐户存入相应数量。而且 B 可以非在线地处理这些支付信息，不会成为瓶颈。

2.5 出错处理子协议

如果在第 i 个信息商品传递中，在第 j 个单位时失去同步或通信中断，则链接恢复后 U 可直接向 S 发送消息 $U,Id_i,T_i,j,w_j,\{U,Id_i,T_i,j,w_j\}_{K_U^-}$，$V$ 即可用同一密钥从第 j 个单位开始续传第 i 个信息商品。

超额花费用户造成的损失由商家和银行按预先协商好的方式分担，若用 x_{UV}表示银行 B 从商家 V 收到的关于用户 U 的报告数，则对于每个 $V\in L_U$，银行可以按比例 x_{UV}/x_U 分别给每个商家偿还损失。

3 NMP 协议的性能分析与比较

3.1 安全性

在服务请求协议2中，增加了 V 对消息1中收到的信息商品标识 Id_i、时戳 T_i 以及信息商品加密密钥 K_S 的签名，确保了 U 对 V 的认证。同时保密的传递了用于后面信息商品加密的密钥，使得只有付费用户才能得到信息商品。协议中采用了时戳信息 T_i，重放任何截获的消息都会被检测出来。NMP 服务协议中两个相继杂凑值满足 $w_i=h(w_i')$，$w_{i-1}'=h(w_i)$，商家或经纪想欺骗用户基于求单向函数逆的困难性[8]。除了与 PayWord 一样提供了用户对记费的不可否认性外，NMP 中 V 对解密信息产品的密钥、用户身份及商品名称一起签名保证了他对这一密钥的不可否认性，如果提供了不正确的密钥，仲裁方可以追究其责任。同样双方对商品名称、价格、计费单位及长度的签名都为其后计费提供了不可否认证据。

3.2 公平性

在服务协议2中，我们把一个杂凑值分成两半，作为对一个单位信息商品的支付。先支付前一半，得到一个单位信息商品后，再支付另一半，并对 V 最后提供给 B 的半对杂凑值按一个单位记费，这一单位收费充公。这样 U 和 V 无论谁先中断协议运行都得不到好处。虽然 NMP 仍然没有取得完全的公平性，但比现有的小额支付协议具有更好的公平性。

3.3 运行效率

NMP 协议给用户端增加的计算负荷主要在服务请求协议的消息2中，这里有一个解密运算，一个签名验证，但是解密信息产品的密钥 K_S(20bytes)，用户的身份 U (20bytes)，信息商品标识 Id(10bytes)，请求时间 T(14bytes)，这些项最多总共64bytes。这样一个短消息的解密与签名验证时延很小[9]，不会对用户造成太大影响。而新的服务协议则几乎与 *PayWord* 的服务协议的运行效率一样。

若用|U|表示系统中的用户数，|V|表示参加交易的商家数，N 表示每个用户每天购买的平均数，W 表示每天和每个用户参与交易的商家的平均数，t|U|表示每天系统中的超额花费用户数，kω_U 表示用户 U 引发银行发出警告的预期购买金额，d 表示诚实用户被怀疑超额花费的概率，则每天由概率

(下转第156页)

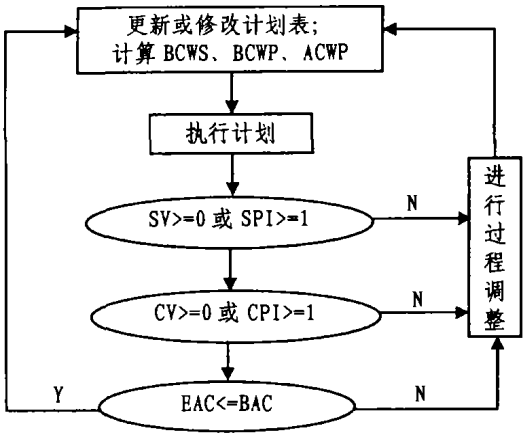

图3 评估阶段工作流程图

(3)打包阶段

⑨ 从经验库中分析过程产生的经验。将成功的经验制订规范和标准予以推广,将失败的经验做成反面教材予以警示。

⑩ 根据经验库的经验改进软件过程,返回到步骤①。

3.3 EVMS 的组织关系

根据 EVMS 的实施步骤,考虑在软件企业内建立三种组织:开发组、过程组和支持组。其功能分别是:

(1)开发组负责软件开发、维护以及应用有效的软件工程技术方法于软件开发过程中。其目标是开发高质量的软件产品,充分满足客户需求。

(2)过程组负责评价软件过程,将软件过程中得到的经验进行分类以及将成功经验打包予以推广。其目标是充分支持开发组的工作,帮助开发组避免以前的错误,吸取成功的经验更好地进行开发工作。

(3)支持组负责配置软件开发环境、平台,管理经验库以及有效地收集、存储、跟踪信息等。其目标是为开发组和过程组做好后勤工作,保证它们的工作能够有效地进行。

三个组织的关系如图4所示。

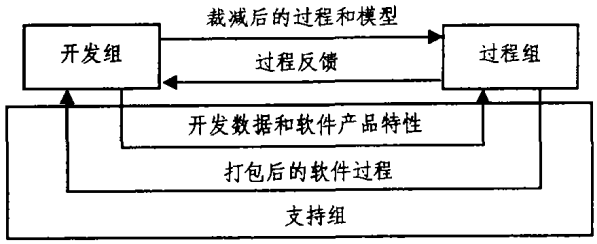

图4 EVMS 的组织关系

结束语 软件企业进行软件过程改进的最终目的是为了高质量、高效率、低投入地生产软件。自底向上模型是软件过程改进的一种方式,它以最终产品为出发点,根据产品生产的具体需求改善过程;EVMS 是项目管理的一种先进方法,它能够在项目进行过程中随时报告项目进展,并能预测项目完成后的状态,协助项目经理提高决策质量,帮助项目沿着一个良性的轨道发展。而将两者结合起来进行软件过程改进,则能够帮助软件企业降低项目风险,提高开发效率和软件质量,保证企业获得最大的利润。

参 考 文 献

1 Staley M J,Oberndorf P,Sledge C A. Using EVMS with COTS-Based System. CMU/SEI-2002-TR-022,ESC-TR-2002-022,2002
2 Banerjee G,Das R. Earned Value Management System - for IT Projects,May 2003
3 何轶彬,陈晓彬,金和平,何文. 工程项目成本/进度综合控制方法及应用,2001,URL: http://www.cws.net.cn/Journal/Three_Gorges/200107/14.html
4 What Is Earned Value Management. URL: http://evm.nasa.gov/definition1a.html
5 Fleming Q W,Koppelman J M. Earned Value Project Management - A Powerful Tool for Software Projects. The Journal of Defense Software Engineering,July 1998. 19～23
6 Wilkens T T. Earned Value,Clear and Simple,April 1999
7 Boehm B. Value-Based Feedback in Software/IT Systems,2000
8 李健,金茂忠. 有效改善软件过程方法研究. 计算机研究与发展,2001,38(1): 26～35

(上接第139页)

性检测增加的通信量=正常情况下的概率性检测消息+商家转发给银行的服务请求消息+银行给商家的应答消息+超额花费者引发的警告消息+诚实用户引发的警告消息+ 超额花费者引发的概率性检测消息=$c|U|+(1-c/N)|U|W+|U|W+2t|U|W+3d|U|W+t|U|M$。

所以新协议给每个用户每天增加的通信量=$(c+tM)+W(2+3d+2t-c/N)$。

Payword 协议每个用户每天的通信量=$2N$。

在实际电子交易中检测次数 c、每天每个用户参与交易的商家的平均数 W 以及错误门限 M 和 k 可控制在一定范围内,从而可把概率检测机制增加的通信量控制在实际交易可接受的限度。

小结 在分析现有小额电子支付协议的基础上,提出了一个新的小额电子支付协议,新协议可以防止用户超额花费,同时具有特点:(1) 具有较好的公平性。(2)记费的双向不可否认功能。(3)信息产品的保密传输功能。(4)双向认证功能。(5)适当的运行效率。(6)出错处理功能。

参 考 文 献

1 Glassman S,et al. The Millicent protocol for inexpensive electronic commerce. In:Proc. 4th Int. World Wide Web Conf. Boston,MA,Dec. 1995. 603～618
2 Manasse M. The Millicent protocols for electronic commerce. In: Proc. 1st USENIX workshop on electronic commerce,New York,USA,July 1995. http://www.research.digital.com/SRC/millicent/
3 Furche A,Wrightson G. SubScript-An efficient protocol for pay-per-view payments on the internet. In:Proc. 5th Int. Conf. on computer communications and networks (ICCCN'96),Rockville,MD,Oct. 1996 . http://www.cs.newcastle.edu.au/Research/a-furche/subscrip.ps
4 Rivest R,Shamir A. Payword and Micromint: Two simple micropayment protocols. In:Proc. Security Protocols 1996,Springer LNCS 1189,69～88
5 Anderson R,Manifavas C,Southerland C. NetCard-A practical electronic cash system. In:Proc. Security Protocols 1996,Springer LNCS 1189,49～57
6 Hauser R,Steiner M,Waidner M. Micropayment based on iKP: [Technical report RZ 2791]. IBM Research,Feb. 1996
7 Pederson T. Electronic payment of small amounts. In:Proc. Security Protocols 1996,Springer LNCS 1189,56～68
8 Damgard I. A design principle for hash functions. Advances in Cryptology-CRYPTO'89,Springer-Verlag,1990. 416～427
9 Even S,Goldreich O,Micali S. On-line/off-line digital signatures. J. Cryptology,1996,9:35～67