Virtual Debit-Based Micro-Payment System NPAY

YANG Maoyun
School of Computer Science & Technology, Xuzhou Normal University, Xuzhou, China
e-mail: *ymaoyun@163.com*

Abstract: This debit-based micro-payment system which has not the problem of extra-consuming must refresh overdue electronic cash. The credit-based micro-payment system that needn't refresh overdue electronic cash could not prevent consumer from consuming excessively. Based on the concept of virtual debit, presenting a micro-payment system NPAY, which can solve the problem of extra-consuming, greatly reduce the system communication overhead, and the consumer can consume anonymously.

Keywords: micro-payment; virtual debit; electronic cash; cryptography

基于虚借记的微支付系统 NPAY

杨茂云
徐州师范大学计算机科学与技术学院，徐州，中国，221116
e-mail: ymaoyun@163.com

【摘　要】基于借记的微支付系统不存在超额消费问题，但要更新没有花掉的过期电子现金；基于信用的微支付系统不必更新没有花掉的过期电子现金，但不能防止用户超额消费。提出“虚借记”的概念，设计了一个微支付系统 NPAY，较好地解决了消费者超额消费问题，系统的通讯开销也大大减少，并且消费者可以匿名消费。

【关键词】微支付；虚借记；电子现金；密码学

1 引言

微支付的概念是在 1995 年提出的，到目前为止，主要提出了两类方案：基于借记的微支付系统和基于信用的微支付系统。基于借记的微支付系统不存在超额消费问题，但要更新没有花掉的过期电子现金；基于信用的微支付系统不必更新没有花掉的过期电子现金，但不能防止用户超额消费[1]。

Milicent[2]是基于借记的系统的代表，不存在超额消费问题，但要更新没有花掉的过期 Scrip。Milicent 没有使用速度较慢的公钥加密技术，而使用了速度较快的哈希函数和分组密码技术来防止伪造和重复花费，这提高了协议执行的速度。但是 Milicent 使用共享的密钥进行认证和加密，Broker 和 Vendor 都有查找数据库的耗费，规模很大时这种耗费可能占主导地位。Milicent 不能保证用户的匿名性。Milicent 要求 Customer 与 Vendor 的关系是长期的，只有这样 Customer 才不用频繁的到 Broker 处购买 Vendor 的 Scrip，才能保证了协议的高效率。Payword 是基于信用的系统的代表，不能防止用户超额消费，必须采取策略减少损失，比如短周期的支付结算等。基于信用的好处是用户没有使用完的 payword 可以抛弃掉，不用更新。Payword 使用少量的公钥加密码技术，不用保持和查找密钥数据库。Payword 不能保证用户的匿名性。Payword 要求用户与商家的联系是长期的，只有这样，用户才不用频繁地申请证书，才能保证系统的高效率[3]。

基于信用的和基于借记的系统各有千秋，基于信用的系统不用更新过期的货币，但却不能防止超额消费；基于借记的系统能防止超额消费，但必须更新过期的货币。本文提出“虚借记”的概念来解决这个问题。

2 NPAY 的设计

2.1 虚借记

用户不是借记实际的现金，而是借记提取微电子现金的能力。即制造微电子现金时，并不从用户的帐户上扣除相应的金额，只是扣除相应的用户提取微电子现金的能力。

2.2 NPAY 的协议过程

NPAY 的安全模式和参与方与上述两个系统基本一致。NPAY 中的经纪人 B 不仅要维护用户和商家的帐

978-1-935068-06-8 © 2009 SciRes.

户，并且还要维护用户的提取微电子现金的能力。比如用户的帐户上的金额为 100 元，微电子现金的单位为 5 分钱，那么用户提取微电子现金的能力是 2000。在 NPAY 中用一个与用户帐户关联的计数器来表示用户提取微电子现金的能力（以下简称能力计数器，用 Counter 表示），NPAY 使用与 Payword 相同的方式表示微电子现金。

2.2.1 系统初始化

用户和商家在经纪人处建立帐户。同时经纪人根据用户帐户中的金额给能力计数器Counter赋值。

2.2.2 提取 payword

用户产生密钥对，向经纪人请求提取 n 个 payword。用户选取随机数 w_{n+1}，计算 $w_i = h(w_{i+1})$ $i = n, n-1, \ldots 0$，向经纪人发送消息 M1={IDU，random, IDV, PKU, w0, n}PKB。经纪人检查能力计数器的值大于等于 n 后，发送消息 M2＝{CU}PKU, CU={h(IDU, random), IDV, PKU, w0, expires}SKB 是经纪人发给用户的证书。经纪人把{h(IDU, random), w0}存储在数据库中，以检测商家重复存款。H(IDU, random)的作用是隐藏用户的身份信息，这样消费者可以匿名消费。如图 1 所示。

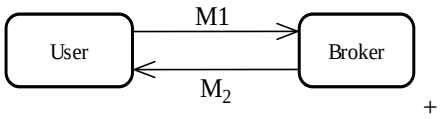

Figure 1. Withdrawing payword

图 1. 提取 payword

2.2.3 购买支付

U 通过浏览器浏览 Vendor 的商品信息，包括商品的 ID 及计费长度 m。

1. $U \longrightarrow V$: $C_U, ID, m, w_0, T_i, \{V, C_U, ID, m, w_0, T_i\}SK_U$

商家利用 CU 取得用户的公钥，验证签名正确，同意提供服务。

2. $U \xleftrightarrow[\text{信息商品：单位}\,i]{(w_i, i)} V$

V 收到（wi, i）后验证wi在数据库中不存在后，计算 $h^i(w_i)$，如果 $h^i(w_i) = w_0$ 表示收到的w_i有效，把{h (IDU, random), wi}保存在数据库中，以检测U重复花费。

2.2.4 支付结算

一段时间以后（一般为一周）V 把最后收到的 payword 如：（wk, k）及 CU 等传送给经纪人 B 进行支付结算。B 首先验证 $h^k(w_k) = w_0$，再检查 w0 在数据库中存在后，最后按照 payword 的序号值把相应的金额从用户的帐户上转移到商家的帐户上，并把 w0 从数据库中删除，以检测商家重复存款，同时能力计数器 Counter=Counter＋n－k。

2.3 协议的安全性分析

2.3.1 提取 payword

M1 使用公钥加密，只有经纪人才能解密；M2 使用用户的公钥加密，只有用户才能解密。对窃听者来讲，由于他不具有用户和经纪人的私钥，所以他既不能得到 M1 和 M2 的明文信息，又不能进行欺骗攻击。如果他进行密码分析的话，那么他得到的利益比所需要的花费要大许多。

2.3.2 购买支付

商家在提供服务前，要验证用户的身份只有合法的用户的合法的 payword 才能被提供服务。用户提供一个 payword 就会得到一个单位的服务。由于哈希函数的单向性，窃听者不能从已花费的 payword 推出未花费的 payword。由于 payword 是指定商家的，并且他也不能伪造 CU，所以窃听者不能利用得到的 payword 从经纪人处获得实际的支付。如果在购买支付的第一步，用户提供会话密钥，商家利用用户提供的会话密钥加密提供的服务内容，就可实现服务内容的保密性，不过协议的效率会有所损失。一般我们采取浏览过的内容，以后再使用时不用再交费的策略。

3 NPAY 评价

NPAY 是基于“虚借记”的，能有效地防止用户超额消费。利用 h（IDU，random）很好地隐藏了用户的身份，保护了用户的隐私权。象 Payword 一样，用户没有使用完的 payword 可以抛弃掉，不用更新；NPAY 使用少量的公钥加密码技术，不用保持和查找密钥数据库；为保证协议的高效性，NPAY 要求用户与商家的联系是长期的。下面以表格的形式对上述三个微支付系统的效率进行比较。

4 NPAY 的系统架构

从效率上考虑，NPAY 采用 768 比特的 RSA 和 MD5，与 Web 高度集成，不需要额外的通讯协议，使用捎带技术传送支付信息，系统架构如图 2 所示：Wallet 负责提取 payword 和进行购买支付，GateWay 负责对支付请求进行验证和响应。

Table 1. Features of system

表 1. 系统特点

系统	微电子现金	制造实体	防止超额消费	匿名性	更新货币	协议周期
Milicent	V 和 B 的 Scrip	V 或 B	能	无	需要	长
Payword	U-V 的 Hash 链	U	不能	无	不需要	短
NPAY	U-V 的 Hash 链	U	能	有	不需要	长

Table 2. Memory requirement

表 2. 存储需求

系统	用户	商家	经纪人
Milicent	已购买的 Scrip 共享的秘密	所有 V 的合法 Scrip 共享的秘密	所有 B 的合法 Scrip (V 的合法 Scrip） 共享的秘密
Payword	证书 CU 每个 Hash 链的（wn，n，i）	最后接受的 payword	最后接受的 payword
NPAY	证书 CU 每个 Hash 链的（wn，n，i）	最后接受的 payword	能力计数器 hash（IDU,random） 用户申请的还没有结算的 Hash 链的根

Table 3. Calculating expense

表 3. 计算耗费

系统	支付前	支付中（U）	支付中（V）	结 算
Milicent	无 (假设 U 已有 V 的 Scrip)	1 hash	1hash/请求验证 1 hash/V's Scrip 验证 1 hash/找零生成 1 hash/响应生成	无
Payword	1 C_U 请求 1 C_U 验证 1 签名/承诺 1 hash/payword	无	1 签名生成/承诺 1 签名验证/C_U。 最新的 payword 的索引值个哈希	1 承诺验证/C_U ,最新的 payword 的索引值个哈希
NPAY	1 C_U 请求 1 C_U 验证 1 hash/payword	无	1 签名验证/C_U 最新的 payword 的索引值个哈希	C_U 验证,最新的 payword 的索引值个哈希,counter 累加运算

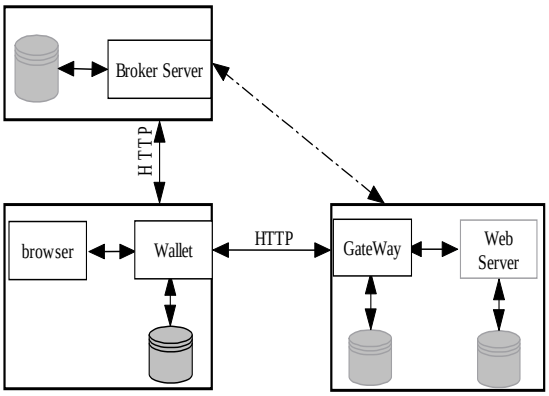

Figure 2. Architecture of system

图 2 NPAY 架构

客户端设计要求：用户购买信息和服务就像正常浏览一样，对用户基本没有影响，但是当光标指向付费的链接时，光标应显示特殊的形状，并且在状态栏显示提示信息。

Reference (参考文献)

[1] Rivest R. Shamir A. PayWord and MicroMint: Two simple micro-payment protocols. Proc.Security Protocol 1996, Spinger LNCS 1189, pages 69-88. http://theory.lcs.mit.edu/~rivest/Rivest Shamir-mpay.ps.

[2] Compaq, Millicent microcommerce network, 1997–2000. http://www.millicent.com/home.html.

[3] Kai CHEN, Shimin WEI and Guozhen XIAO, A New Approach to the Divisible E-cash System, IFIP, WCC2000-SEC2000, 2000. 8, Beijing, pp. 271-274.

978-1-935068-06-8 © 2009 SciRes.