基于GSM的移动微支付方案*)

杨宗凯[1] 付 雄[1] 郎为民[1,2] 吴世忠[2]

(华中科技大学电子与信息工程系 武汉430074)[1] (中国国家信息安全测评中心 北京100091)[2]

摘 要 本文提出了一种基于GSM移动环境的微支付方案,它通过将计算、存储和通信量转移到静态的网络主机上使得移动电话的负荷最小化。在整个支付过程中,移动电话发送和接收的信息非常简单,且避开了复杂的公钥运算,减少了系统延时并消除了因通信失败而造成不完全支付的可能性。同时,本方案使用会话密钥对交易信息进行加密,保护了移动用户隐私和支付信息的安全。与其它移动微支付方案相比,由于本方案完全没有使用公开密钥算法,因而效率大大提高。此外,方案还为移动用户提供了有限的匿名性。

关键词 微支付,移动电话,GSM,公平性

A Mobile Micropayment Scheme Based on GSM

YANG Zong-Kai[1] FU Xiong[1] LANG Wei-Min[1] WU Shi-Zhong[2]

(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)[1]

(China National Information Security Testing Evaluation and Certification Center, Beijing 100091)[2]

Abstract In this paper, we propose a micropayment scheme designed for use in a GSM mobile environment, where the overload of computation, storage and communication for mobile phone is reduced by directing operations normally performed by the mobile user to the static portion of the network. Messages received and sent during the payment are very simple and public key infrastructure is not needed, which reduces delay and removes the possibility of incomplete payment protocols due to communications failures. Furthermore, all the information with regard to payment is encrypted by a shared symmetric key in our scheme, where the privacy of the mobile user is protected and the security of information is guaranteed. Compared with other mobile micropayment schemes in existence, no public-key operation is required, which minimizes the computation and storage overhead dramatically. In addition, restricted anonymous is provided in our scheme.

Keywords Micropayment, Mobile phone, GSM, Fairness

1 引言

微支付[1~3]作为数字货币的一种支付形式,是目前电子支付发展的一个新方向,它能够较好地满足信息商品或服务的需求。与大额支付相比,它的每一笔交易额非常低,在满足安全性的前提下要求系统简单高效。随着移动通信设备的迅猛发展和广泛应用,具有身份识别功能的移动电话能够代替各种银行卡成为个人的随身电子钱包,使支付形式彻底摆脱空间上的一切束缚。移动微支付作为一种全新的支付手段,它实现了钱包的电子化和移动化,不仅快捷,而且实现方便,从而为客户创造了更灵活、更亲切的消费环境。移动微支付平台由于支付金额较小,因而系统结构相对简单,可以避开目前移动领域还不成熟的、复杂的公共密钥安全系统,它将成为未来几年的社会热点,并形成巨大的市场空间。

目前已有多种基于GSM的移动微支付[6,7]方案,但都存在一定的问题和缺陷。在Millicom International Cellular公司开发的GiSMo系统中,要求用户的设备必须支持公钥运算,由于目前的无线通信系统不支持公钥运算,因而它不适用于移动通信环境,该项目已于2001年中止。在Paybox系统中,用户和商家都是使用移动电话进行交易的,因而系统的稳定性差,支付过程容易被中断,同时,由于交易时间短,需要进行GSM在线对话及必须通过传统金融网络进行转账,因而这个方案不适用于微支付。由Stern和Vaudenay提出来的小额支付(SVP)[8]方案是基于抗篡改设备和对称加密算法的,但它要求用户终端和商家终端使用抗篡改设备,且支付过程需要执行三次交互协议来完成,因而效率不高。

本文设计了一种基于GSM的移动微支付方案,它充分考虑到移动电话有限的计算能力、存储容量和处理能力,并通过将计算、存储和通信量转移到静态的网络主机上使得移动电话的负荷最小化。同时,在支付过程中,交易信息都使用共享密钥进行了加密,移动用户隐私和支付信息的安全得到了有效的保护。与其它移动微支付方案相比,由于本方案完全没有使用公开密钥算法,因而效率大大提高。此外,方案还为移动用户提供了有限的匿名性。

2 基本模型和协议

本文所提出的移动微支付方案涉及到交易的三方:移动用户U、增值服务提供商VASP和网络服务提供商SP。其中,移动用户是使用数字货币和移动电话购买信息商品或服务的主体,增值服务提供商是为移动用户提供商品或服务并接受其支付的网上商店,网络运营商在方案中相当于经纪人的角色,其作用在于搭建移动支付服务平台,为移动用户和VASP开立并维护账户,认证交易双方的身份,进行货币销售和交易结算,并协调解决可能引起的争端。

2.1 开户协议

移动用户选择一个匿名标识ID_U,该标识与移动用户的真实身份没有必然联系。移动用户将ID_C和自己的移动电话号码N_U发送给SP,同时向SP出示其身份证或护照等来唯

*)国家自然科学基金资助项目(90104033)。杨宗凯 博士后,教授,博士生导师,研究方向为电子商务、远程教育和网络安全。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。郎为民 博士研究生,研究方向为电子支付、信息安全和应用密码学。吴世忠 教授,主要从事网络攻防技术、应用密码学等研究。

一标识其身份。SP 验证其证明，为其开立并维护一个账户，然后在移动用户账户数据库中存储该移动用户的身份识别信息及 ID_U、N_U，从而将 ID_U、N_U 与移动用户的身份信息绑定在一起，移动用户在其账户上存储一定数额的现金。同时，移动用户与 SP 共享一个密钥 K_{US}，并从 SP 处得到移动用户和 VASP 共享的会话密钥 K_{UV}。

VASP 也必须在网络服务提供商 SP 处开户，将 ID_V 作为其身份标识发送给网络服务提供商，同时向网络服务提供商出示其营业执照和网址 A_V 等来唯一标识其身份。网络服务提供商验证其证明，为其开立和维护一个账户，并在 VASP 账户数据库中存储该 VASP 的身份识别信息 ID_V 和网址 A_V，从而将 A_V 与 VASP 的身份识别信息 ID_V 绑定在一起。同样，VASP 也与网络服务提供商共享一个密钥 K_{VS}，且可从 SP 处得到移动用户和 VASP 共享的会话密钥 K_{UV}。

2.2 支付协议

(1)用户 U 使用移动电话浏览 VASP 的站点选择需要购买的商品或服务，并记录 VASP 的网址 A_M 及商品或服务的价格，生成订单信息 OI，它包含购买商品或服务的种类、数量和总金额等信息。移动用户发送一个购买请求给 VASP，购买请求的格式如下：

$(ID_U, OI, V_U)_{K_{UV}}$

其中 V_U 为本次交易总额。

(2)VASP 为保证支付的安全可靠，需要访问 SP 服务器，并将包含移动用户订单信息的支付授权请求发送给 SP 服务器：

$(ID_U, ID_v, V_U)_{K_{VS}}$

(3)SP 服务器根据移动用户和 VASP 的标识通过遍历数据库来检查其对应账户的合法性，以保证其处于良好的状态且没有任何使用限制，然后根据 ID_U 确定移动用户的移动电话号码，并向其发送如下的扣账请求：

$(ID_U, ID_v, V_U)_{K_{US}}$

(4)移动用户收到 SP 服务器发送来的扣账请求后，首先检验其合法性并对支付信息进行确认，然后将包含个人识别码 PIN(通常为四位数)的扣账响应发送给 SP 服务器：

$(OK, PIN)_{K_{US}}$

(5)SP 服务器收到移动用户的个人识别码后，确认是移动用户本身参与了此次交易，然后向 VASP 发送如下的支付授权响应：

$(ID_U, OK, V_U)_{K_{VS}}$

如果在给定时间(如两分钟)内，SP 服务器没有收到移动用户发送来的扣账响应信息，则该交易将被自动取消。

(6)VASP 将信息商品或服务发送给移动用户。

2.3 转账协议

当移动用户 U 收到 VASP 提供的商品或服务后，他将使用其移动电话发送一个支付认可消息给 SP，网络运营商根据移动电话号码使用 GSM 中的 SIM 卡来鉴别并获得移动用户的身份 ID_U，并从移动用户账户上扣除与交易额相当的资金转移到 VASP 账户上。

3 系统性能分析

3.1 安全性

由于每次支付执行时，交易信息都使用共享密钥进行了加密，攻击者无法获取相关的敏感信息，从而保护了移动用户隐私和支付信息的安全。在本方案中，移动用户企图使用账户上不足的余额与 VASP 进行交易(移动用户企图进行超支花费)是不可能的，因为 SP 服务器需要通过检查移动用户和 VASP 账户的合法性来对 VASP 进行支付授权，非良好状态的账户将直接导致支付的中止。另一方面，若 VASP 发送与订单信息不同或便宜的商品，则移动用户在对商品或服务进行检查后，拒绝发送支付认可消息，因而 VASP 无法得到相应的交易资金。

3.2 公平性

在本方案中，我们假定 SP 是诚信的，移动用户在获得商品或服务之前，VASP 无法得到相应的交易资金，因为 SP 只有在得到移动用户的支付认可消息后才实施转账。同时，若移动用户宣称其收到的商品或服务与订单信息中规定的不符合，或否认已收到的 VASP 提供的商品或服务，则 SP 服务器会要求 VASP 对信息商品或服务进行重发，直到移动用户认可为止。在这种情况下，移动用户的欺诈行为并不能使其得到相应收益，因而方案使得消费者和商家的利益都得到了保障，从而具有一定的公平性。

3.3 效率分析

使用移动通信设备进行的微支付，必须考虑到其有限的计算能力和存储能力。同时，与网络通信相比，移动设备的通话费用相对较高。因此，设计移动环境下高效微支付方案的一个基本原则是减少移动电话的计算开销、存储开销和通信开销，以提高系统的执行效率。在本方案中，我们通过将计算、存储和通信量转移到静态的网络上来最小化移动电话的负荷，在整个支付过程中，移动电话发送和接收的信息非常简单，且完全避开了复杂的公钥运算，减少了延时并消除了因通信失败而造成不完全支付的可能性，从而很好地适应了移动微支付的特点。同时，本文所提出的微支付方案，由于完全没有采用公钥密码算法，而是使用简单快捷的对称加密算法，从而大大节省了计算开销和存储开销，其效率大大提高。

3.4 有限的匿名性

由于只有 SP 知道移动用户的匿名标识和真实身份之间的对应关系，因而在移动用户与 VASP 进行交易时，VASP 不能获知移动用户的身份信息，所以方案为移动用户提供了有限的匿名性。

结论 本文设计了一种新的移动微支付方案，它是基于 GSM 移动环境的。本方案通过将计算、存储和通信量转移到静态的网络主机上以达到移动电话的负荷最小化，整个支付过程移动电话发送和接收的信息非常简单，且避开了复杂的公钥运算，减少了延时并消除了因通信失败而造成的不完全支付的可能性。在支付过程中，交易信息都使用共享密钥进行了加密，移动用户隐私和支付信息的安全都得到了很好的保护。与其它移动微支付方案相比，由于本方案完全没有使用公开密钥算法，因而效率大大提高。此外，方案还为移动用户提供了有限的匿名性。

参考文献

1 Buttyán L. Removing the Financial Incentive to Cheat in Micropayment Schemes. IEE Electronics Letters, 2000,36 (2): 132～133

2 Adachi N, Aoki S, Komano Y, et al. The Security Problems of Rivest and Shamir's PayWord Scheme. In: Proc. of the IEEE Intl. Conf. on E-Commerce (CEC'03), 2003. 126～129

3 Yen S, Lee C, Ho L. PayFair: a prepaid Internet micropayment scheme promising customer fairness. IEE Proc. of Comput. Digit. Tech., 2001, 148(6): 207～213

4 Kalden R, Meirick I, Meyer M. Wireless Internet Access Based on GPPS. IEEE Personal Communications, 2000, 7(2): 8～18

5 Wrona K, Zavagli G. Adaptation of the SET Protocol to Mobile Networks and to the Wireless Application Protocol. In: Proc. European Wireless 99, Munich, Germany, Oct. 1999. 193～198

6 Stern J, Vaudenay S. SVP: a Flexible Micropayment Scheme, Financial Cryto'97, Springer-Verlag, 1997. 161～171