移动支付的安全方案研究

施小华，王志坚
（河海大学 计算机及信息工程学院，江苏 南京 210098）

摘 要：移动支付系统按照交易额的数量可分为宏支付和微支付。在宏支付中，由于交易数额较大，系统对安全性要求较高，因此，设计出一种安全的支付方案是系统成败的关键。介绍了宏支付的概念和移动支付的安全性要求，总结了移动交易的模式，并且在该模式下、在考虑移动支付的安全性要求的情况下，设计出了一种安全有效的支付方案。随后，对方案在秘密性、完整性、可认证性以及不可否认性等安全性方面和方案的实用性进行了分析，证明了方案的有效性。最后，为方便在后续研究中更深入探讨，指出了工作的局限性和它可以进一步完善的地方。

关键词：移动支付；宏支付；支付方案；安全性
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1673－629X(2007)04－0108－05

A Secure Payment Scheme for Mobile Payment System

SHI Xiao-hua, WANG Zhi-jian
(College of Computer and Information Engineering, Hohai University, Nanjing 210098, China)

Abstract: The mobile payment system has the distinction between a macro and a micro one, due to the amount of payment. In the former case, because of the multitude of monetary transfer, strong securities are desired. Therefore, a secure payment scheme is crucial in the design of a good system. In this paper, introduced the concept of macro－payment, presented the security aspects that a mobile payment system has and that its designer needs to be constantly conscious of and consider carefully in design process. Summed up the mode of a mobile transaction, under which designed a macro－payment scheme, bearing always in the mind the security restraints presented earlier. Following this is analysis of the scheme in its validity and usefulness. The result reached is that the scheme is quite satisfactory with respect to securities which include privacy, integrity, authentication, non－repudiation, and usefulness. In the end, to facilitate further research along the line, pointed out the area which research has mainly addressed in achieving the securities. To expand this area to consider other possibilities to make the scheme work safely alike under other conditions will undoubtably be improvement to the work.

Key words: mobile payment; macro－payment; payment scheme; security

1 移动支付中的宏支付

移动支付系统按照交易额的数量分为宏支付和微支付[1]。现存的移动支付系统大部分都是微支付。在微支付系统中，交易的费用是从用户的话单中扣除的，不涉及到银行的直接参与。而在宏支付系统中，用户用手持设备购物时，银行是直接参与者之一，用户的交易费用是从与用户手持设备绑定的银行账户中扣除的。由于交易数额较大，宏支付对安全性要求较高，因此，设计出一种安全的宏支付方案十分关键。文中从密码学的角度在应用层为宏支付设计出了一种安全方案来解决宏支付中的安全问题。

收稿日期：2006－07－08

作者简介：施小华(1979－)，男，湖北公安人，硕士研究生，主要研究方向为信息安全；王志坚，教授，博士生导师，主要研究方向为网络计算机应用技术、信息安全、网络软件系统集成技术。

2 移动支付方案的安全性标准

安全方案的目标是保证在安全方案执行完毕时能实现其安全性质。安全方案的安全性质主要有以下几个方面[2]。

2.1 可认证性

认证是最重要的安全性质之一，所有其它安全性质的实现都依赖于此性质的实现。认证是分布式系统中的主体进行身份识别的过程。有三种认证方法：

① 主体使用只有验证者与其共享的密钥加密消息，验证者使用同一密钥解密消息验证主体的身份。

② 主体使用其私钥对消息签名，验证者使用主体的公钥验证签名以验证主体的身份。

③ 主体通过可信第三方来证明自己的身份。

2.2 秘密性

秘密性是指保护协议消息不被泄漏给未被授权的人，即使是攻击者了解消息的格式，他也无法从消息内

容中得到有用的信息。保证秘密性最直接的办法是对消息进行加密,将消息从明文变成密文,没有密钥的人是无法解密消息的。

2.3 完整性

完整性是指保护协议消息不被非法篡改、删除或替代。最常用的方法是封装和签名,即用加密或 Hash 函数产生一个摘要附在传送消息后,作为验证消息完整性的依据。用户收到消息后用同样的 Hash 函数产生一个摘要和收到的摘要进行对比来判断消息在传输过程中是否保证了完整性。

2.4 不可否认性

不可否认性又称不可抵赖性,是指通信主体能通过提供对方参与协议交换的证据来保护自身合法利益,即协议主体必须对自己的行为负责,不能也无法事后抵赖。不可否认性又分以下两种:

(1)消息源不可否认(non - repudiation of origin),亦即不可否认协议向接收方提供不可抵赖的证据,证明收到消息的来源的可靠性;

(2)消息宿的不可否认(non - repudiation of receipt),亦即不可否认协议向发送方提供不可抵赖的证据,证明接收方已收到了两种消息。主体提供的证据通常以签名消息的形式出现,从而将消息与消息的发送者进行了绑定。

3 移动交易过程

移动支付系统应有用户(手持设备)Client、商家 Merchant、移动支付平台 MPP、银行端处理设备 Settlement 等组成部分。它们是移动交易过程的主要参与者。移动交易过程为:

① Client 挑选商品,按固定格式形成订单。选择完毕后连同手持设备 ID(如手机号)发送给商家。

② 商家对该订单和手持设备 ID(如手机号)进行加密、签名后通过安全 Internet 通道如 SSL 发送给 MPP。

③ MPP 收到消息后确认消息的来源,如果消息确实来自指定商家则进行消息处理(如加密签名)后发送给移动用户即 Client。

④ Client 收到 Welcome 消息后输入 PIN 码同意使用移动支付系统,然后确认所买的商品、消费额、商家标示及消息来源,如果消息正确,则同意支付。消息处理后传送给 MPP。

⑤ MPP 确认消息正确后向银行发起转账请求。

⑥ 银行处理支付。

⑦ MPP 收到转账成功的消息。

⑧ 商家收到支付成功的通知。

⑨ Client 收到电子发票或收据。

⑩ 商家为客户提供服务。

其中③④两步是手持设备与支付平台间在无线环境下的通信,必须保证客户对交易支付的确认信息的安全性。移动支付平台对商家的认证也很重要,以防商家的假冒行为,但这是基于 Internet 的有线环境的,因此较易做到。在以上过程中,移动运营商仅起信息传媒的作用。

从上可见,对移动支付系统的安全威胁主要来自两方面:

a. 冒充用户或冒充手持设备。用户 A 在选购商品完毕后,冒充用户 B,希望商品的费用从用户 B 的银行账户中支付;

b. 冒充商家。商家 B 冒充商家 A,希望用户支付给商家 A 的费用转到自己的账户中。实施这些威胁所采用手段有窃听、重放等。

4 支付方案描述

4.1 符号说明

C_{client}:客户端(即手持设备端)Client 的证书;

S_{client}:客户端(即手持设备端)Client 的私钥;

P_{client}:客户端(手持设备端)Client 的公钥;

$C_{merchant}$:商家 Merchant 端的证书;

$S_{merchant}$:商家 Merchant 端的私钥;

$P_{merchant}$:商家 Merchant 端的公钥;

C_{MPP}:移动支付平台 MPP 的证书;

S_{MPP}:移动支付平台 MPP 的私钥;

P_{MPP}:移动支付平台 MPP 的公钥;

C_{bank}:银行处理端 Settlement 的证书;

S_{bank}:银行处理端 Settlement 的私钥;

P_{bank}:银行处理端 Settlement 的公钥;

CA:所有证书的同一颁发单位(实际上不同的证书可能由不同的 CA 颁发,但这些 CA 可同属一个根 CA,证书的认证可通过证书链完成);

H(Information):Information 的 H 函数摘要;

$H(Information)_{SK}$:用私钥 SK 签名 Information 的 H 函数摘要形成的数字签名;

$(Information)_K$:用密钥 K 对 Information 加密;

PIN + PIN:PIN 对自己的填充;

A\\B:消息 A 与消息 B 的级联;

Order:订单。

4.2 支付方案描述

(1)商家→MPP。

I: $\{SHA(Order)_{Smerchnant}\}$ \\ Order

$$\backslash\backslash ID\backslash\backslash N_{RAND}$$

其中 ID 为手持设备的 ID。N_{RAND}为大随机数,作为抵制重放攻击的策略。SHA[3]是安全散列算法,以防止穷举法攻击。消息 I 通过安全通道由商家发送到 MPP。因为商家和 MPP 之间是基于 Internet 的有线通道的,所以保证消息 I 的安全性不成问题。其中 Order 中应包含商家信息、用户的购物单、用户的 ID 等信息,MPP 会检查 Order 中商家和签名的商家是否一致。

(2)MPP→Client。

首先 MPP 和 Client 在 MIDP2.0 规范下通过 HTTPS 保证端到端的安全[4]。

MPP 收到消息 I 后验证商家的签名来判断商家的身份并验证数据 Order 的完整性。如果正确则提取出 ID 和 N_{rand},否则返回错误信息给商家。接着从本地数据库中检索 ID 来验证 ID 的合法性。如合法则运行 InitServlet 产生会话密钥(SessionKey)和随机数 challenge 。会话密钥有两个:一个用于 MPP 端加密而 Client 解密;一个用于 Client 加密而 MPP 端解密。MPP 用 Client 的 PIN 对自己的填充对 SessionKey 加密后伴随着 Welcome 界面发送给 ID 用户并要求用户输入 6 位 PIN 码同意使用支付系统。同时存储 N_{RAND}。

$$II:\left\{\begin{array}{l}[SHA(Order\backslash\backslash challenge)]_{Smpp}\\ \backslash\backslash Order\end{array}\right\}_{SessionKey}$$

$$III:(SessionKey)_{PIN+PIN}$$

以上的加密过程可采用安全性能较高的 AES[5]算法。

上面 InitServlet 函数的功能包括:

(a) 产生 128 位的随机数 challenge;

(b) 为客户创建新的 HTTP session;

(c) 存储 challenge 到会话变量里;

(d) 产生 128 位的加密/解密会话密钥(SessionKey);

(e) 存储(d)产生的会话密钥到数据库 Client 的条目里;

(f) 从数据库检索 Client 的 PIN 码;

(g) 用 PIN 码填充自己后加密会话密钥;

(h) 将(g)的结果伴随着 Welcome 界面发送给 ID 用户并要求用户输入 6 位 PIN 码同意使用支付系统。

(3)Client→MPP。

Client 输入 PIN 码后通过解密 III 得到 SessionKey,用 SessionKey 初始化 AES,解密 II 验证 MPP 的签名以及 Order 的完整性。如正确则证明消息确实来自 MPP。用户检查 Order 后,如同意支付则生成 Confirm 确认信息并将其签名附上 challenge,ID 和 PIN 信息用会话密钥加密后发送给 MPP;如 Client 输入 PIN 码不正确或得到消息不完整则返回相应信息。

$$IV:\left\{\begin{array}{l}[SHA(Confirm)]_{Sclient}\backslash\backslash confirm\\ \backslash\backslash challenge+1\backslash\backslash ID\backslash\backslash PIN\end{array}\right\}_{SessionKey}$$

其中 ID 和 PIN 码是为了进一步验证用的,challenge+1 是为了防止重放攻击。

(4)MPP→Settlement。

MPP 收到 IV 后进入认证阶段:

① 首先 MPP 从数据库中取出用于对 IV 进行解密的 SessionKey 来初始化 AES,解密 IV,如果解密不成功则返回相应的错误信息给 Client。

② 取 Client 的公钥验证签名的有效性。如无效则返回 Client 相应的错误信息。

③ 提取 Confirm 进行 SHA 运算,用结果和收到的摘要进行比较,验证数据(Confirm)的完整性,如不相符则返回 Client 相应的错误信息。

④ 提取出 ID\\challenge+1\\PIN。依次和数据库中的 PIN 和 ID 比较验证一致性,同时验证 Client 发来的 challenge 和会话变量里存储的 challenge 的一致性。

⑤ 此时根据签名的有效性可以判断 Confirm 确实来自指定的客户端,根据 SHA 结果可以判断 Confirm 在传输过程中没有被篡改过,再次验证 challenge 可以判断消息是否被重放。PIN 和 ID 起到辅助验证的作用。

MPP 认证 Client 后,向 Settlement 发出支付处理请求。

$$V:\begin{array}{l}\{SHA(Request)\}_{Smpp}\\ \backslash\backslash Request\backslash\backslash N_{Rand}\end{array}$$

其中 Request 应包含客户 ID、商家 ID、转账金额、交易代码、交易时间戳等等信息。

(5)Settlement→MPP。

Settlement 收到消息 V 后:

① 验证 MPP 的签名的有效性,如无效则返回 MPP 相应的出错信息。

② 用 SHA 散列 Request 后将散列结果和收到的摘要进行比较,如不一致则返回 MPP 相应的出错信息。

③ 通过 Request 里的交易时间戳判断是否是重放。

经过上面的过程可以验证:消息 V 确实来自指定的 MPP 且非重放。这样可以防止假冒 MPP 的情况。

Settlement 根据 Request 提供的信息进行支付处理,如处理成功则返回转账成功的消息给 MPP,否则返回 MPP 相应的出错信息。

$$VI:\{SHA(ResMPP)\}_{Sbank}\backslash\backslash ResMPP$$

$$\backslash\backslash N_{Rand}+1\backslash\backslash$$

$$\left\{\begin{array}{l}\{SHA(ResMerchant)\}_{Sbank}\\ \backslash\backslash ResMerchant\end{array}\right\}_{Pmerchant}$$

$$\backslash\backslash$$

$$\left\{\begin{array}{l}\{SHA(ResClient)\}_{Sbank}\\ \backslash\backslash ResClient\end{array}\right\}_{Pmerchant}$$

其中 ResMPP 应包含客户 ID、商家 ID、账户处理结果、交易代码、交易时间戳等信息,并用银行的私钥签名。ResMerchant 是银行给 Merchant 的收据,用银行的私钥签名后用 Merchant 的公钥加密。ResClient 是银行给 Client 的收据,用银行的私钥签名后用 Client 的公钥加密。对 MPP 来说,其只知道支付是成功的而看不到 Merchant 和 Client 的帐户信息,从而保证了 Merchant 和 Client 的帐户的私密性。Settlement 应存储一些最近的交易以备客户查询。

(6)MPP→Merchant。

●MPP→Client。

MPP 收到 VI 后:

① 验证 Settlement 的签名的有效性,如无效则返回 Settlement 相应出错信息。

② 用 SHA 散列 Response 后将结果和收到的摘要进行比较,如不一致则返回 Settlement 相应的出错信息。

③ 通过收到的($N_{Rand}+1$)与 N_{Rand}的差是否为 1 来判断是否是重放。

通过上述过程可以确定消息确实来自 Settlement,判断支付已经成功。此时 MPP 需要通知商家和用户。

●MPP→Merchant。

$$VII:\left\{\begin{array}{l}\{SHA(ResMerchant)\}_{Sbank}\\ \backslash\backslash ResMerchant\end{array}\right\}_{Pmerchant}$$

其中 ResMerchant 应包含 Merchant 的帐户信息和账户处理信息。

●MPP→Client。

$$VIII:\left\{\left\{\begin{array}{l}\{SHA(ResClient)\}_{Sbank}\\ \backslash\backslash ResClient\end{array}\right\}_{Pcliem}\right\}_{SessionKey}$$

其中 ResClient 应包含 Client 帐户信息和账户处理信息。MPP 将从消息 VI 中提取出的相应信息用与 Client 之间的 SessionKey 加密后发给 Client。

(7) Merchant 和 Client 对消息的处理。

Merchant 收到消息 VII 后用私钥解密,验证银行签名,查看收据并存储收据。

Client 收到消息 VIII 后用会话密钥解密,再用私钥解密,验证银行签名,查看收据并存储收据。

5　支付方案的安全性与实用性分析

下面从秘密性、完整性、可认证性、不可否认性来分析方案的实用性。

5.1　秘密性

该安全方案能保证数据的秘密性。首先 Client 和 MPP 之间采用会话密钥加密,且 AES 的加密采用 128 位密钥。同时 MIDP2.0 规范支持 HTTPS,因此可形成 Client 与 MPP 之间的安全信道。而 MPP 和 Settlement 之间、商家和 MPP 之间是在 Internet 环境下通信的,运算能力和空间都不受限制,因此也能保证他们之间的数据秘密性。

5.2　完整性

该方案的散列函数都是采用 SHA－1[3](安全散列算法)函数,它形成的消息摘要比 MD5 摘要长 32 位。使用强行技术,产生任何一个报文使其摘要等于给定报文的摘要的难度对 SHA－1 是 2^{160}数量级操作,产生具有相同报文摘要的两个报文的难度是 2^{80}数量级的操作。这样,SHA－1 对强行攻击有很大的强度。因此使用 SHA－1 算法配合签名算法有很好的安全性,从而能保证数据的完整性。

5.3　可认证性

首先,方案中 Client 和 MPP 之间端到端的认证是通过主体使用只有验证者与其共享的会话密钥加密消息来完成的。两者之间的会话密钥具有随机性,且各自加密和解密采用了不同的密钥,因此能达到 Client 和 MPP 之间良好的认证效果。消息内容中的签名有助于加强认证。

其次,假设有冒充商家存在,根据方案的第(1)步,有三种情况:

① 商家 B 有能力伪造含有 B 信息的 OrderB 并用自己的私钥进行签名,即它能产生消息

$$\{SHA(OrderB)_{SmerchantB}\}\backslash\backslash OrderB$$

但是商家 B 不知道用户 ID,因此无法冒充商家 A;

② 商家 B 能够获得含有商家 A 信息的 OrderA,并且知道用户 ID,这时商家 B 用自己的私钥签名后发给 MPP 消息

$$\{SHA(OrderA)_{SmerchantB}\}$$
$$\backslash\backslash OrderA\backslash\backslash ID\backslash\backslash N_{RAND}$$

MPP 收到消息后会检查 Order 含有的商家信息与签名的商家是否一致。这样 MPP 就会发现商家的冒充行为;

③ 在①的基础上,如果商家 B 知道用户 ID,这时,商家 B 会发送给 MPP 消息

$$\{SHA(OrderB)_{SmerchantB}\}$$
$$\backslash\backslash OrderB\backslash\backslash ID\backslash\backslash N_{RAND}$$

MPP 收到检查消息后,会把 OrderB 发送给指定 ID 用户,此时用户能发现商家的冒充行为。

由此可见,方案具有抵制商家冒充行为的能力。

再次,若有用户冒充,则冒充攻击可能出现在方案的第(2)步或者第(3)步,有三种情况:

*用户 B 在购物完毕后使用用户 A 的 ID,这时 MPP 产生的 SessionKey 用用户 A 的 PIN 码加密后发给用户 A,此时用户 B 在不知道用户 A 的 PIN 码的情况下,无法进行下一步操作;

*用户 B 能够窃听或截取到消息 II 和 III,但无用户 A 的 PIN 码无法得到 SessionKey;

*用户 B 能够窃听或截取到消息 IV,但不能解密用 SessionKey 加密的内容,同时 Challenge 又抵制了重放攻击。因此只要用户的手持设备的 ID 不被窃取,用户就可不必担心自己被冒充。

由上面三种情况可知,方案能够抵制用户冒充的攻击,即能够认证用户。

5.4 不可否认性

不可否认性和认证性紧密相连。该方案每条消息摘要都经过了主体的数字签名,它们将作为不可否认的证据提供给对方,因此可以有效地防范客户和银行的事后抵赖行为。特别是商家和客户的电子收据能有效地抵制银行的抵赖行为。

5.5 可用性

综上所述,该方案较完备地考虑了移动支付系统的安全性需求,加之其可适应无线环境和手持设备的受限性,将大部分计算性功能从手持设备端转移到服务器端完成,另外 J2ME 平台提供了对 HTTPS 的支持,因此该方案是适用于构建实用的移动支付系统的。

6 进一步工作

实用的移动支付系统在技术上涉及到许多方面,文中所提出的方案着重考虑了无线环境下的安全性,但是有线环境下的安全性同样需要谨慎设计。另外,如何提高系统的吞吐量,使得当用户数量增加时,对用户的响应仍然相对及时,使用户不感觉到系统的延时仍需进一步研究。

参考文献:

[1] Mobile payment forum, Ltd. Mobile payment forum white paper[EB/OL]. 2002 - 12. http://www.mobilepaymentforum.org/info/mpf_docs/mpf_whitepaper.pdf.

[2] 冯登国. 密码学原理与实践[M]. 北京:电子工业出版社, 2003.

[3] Stallings W. 密码编码学与网络安全[M]. 杨 明,胥光辉等译. 北京:电子工业出版社,2002.

[4] Forum Nokia. MIDP 2.0 Introduction, Version 1.0[EB/OL]. 2003 - 03. http://forum.nokia.com.cn/sch/index.html.

[5] Daemen J, Rijmen V. AES Proposal: Rijndael, AES Algorithm Submission, National Institute of Standards and Technology (NIST) AES[EB/OL]. 1999. http://csrc.nist.gov/CryptoToolkit/aes/.

(上接第 107 页)

对进入的包进行检查看是否进行了 IPsec 保护,如果未受保护则查询 SPD - I 数据库决定是丢弃或是转发,同样如果丢弃则进行审计事件,如果通过就和普通数据包一样处理;如果受到 IPsec 保护,首先进行查找 SAD 数据库 ,查询有无与之相匹配的 SA 实体。如果没有丢弃该包,并进行审计事件;如果有与之匹配的 SA 实体,按照协商好的协议进行 IPsec 处理。进入和外出处理都考虑到嵌套 SA 的处理,如果需要则按上述流程处理。

4 结束语

主要讲述了 IPsec 在无线应用场景下的实现过程。而下一代网络将是一个混合异构网络,以高速固网为中间骨干网,边缘有多种有线和无线接入网络组成[8]。移动终端也将是下代网络的重要组成。如何保证这些设备在各种接入网络间安全自由切换,实现“无缝移动”,IETF 专门成立 MOBIKE 工作组,研究 IPsec 与移动 IP 之间的集成和互操作问题。IPsec 的发展目标将是保证未来各种网络之间的安全和平共处。

参考文献:

[1] 李成友,曹 伟. IPsec 研究与虚拟专用网技术[J]. 计算机工程,2002(2):246 - 248.

[2] Kent S, Seo K. RFC4301. Security Architecture for the Internet Protocol[S]. 2005.

[3] Kent S. RFC4302. IP Authentication Header[S]. 2005.

[4] Kent S. RFC4303. IP Encapsulating Security Payload(ESP) [S]. 2005.

[5] 龙艳彬,王丽军. IPsec 的分析与改进[J]. 计算机应用,2005(2):390 - 393.

[6] Kaufman. RFC4306. Internet Key Exchange (IKEv2) Protocol[S]. 2005.

[7] 徐 敏,罗汉文. 无线局域网安全问题研究[J]. 通信技术,2002(7):65 - 66.

[8] 叶润国,冯彦军. IPsec 在移动无线场景下的互操作问题[J]. 北京航空航天大学学报,2004(11):1057 - 1061.