网络与信息安全

适用于手机支付的身份认证机制

余小亮，卢达龙，吴 炜，王云峰

（厦门大学 信息科学与技术学院，福建 厦门 361005）

摘 要： 手机支付已经成为目前电子商务平台的主要支付手段，但用于手机支付的双重认证机制无法抵抗手机病毒感染、手机号码被复制、手机丢失带来的安全隐患。本文基于用户账户、密码、手机序列号 IMEI，借助于哈希函数、公钥密码等密码技术，设计了一个适用于手机支付的三级身份认证协议。经安全性分析，此机制具备安全性。

关键词： 手机支付；身份认证；哈希函数；公钥密码

中图分类号： TP391.41 **文献标识码：** A **DOI：** 10.3969/j.issn.1003-6970.2016.12.041

本文著录格式： 余小亮，卢达龙，吴炜，等. 适用于手机支付的身份认证机制[J]. 软件，2016，37（12）：192–196

An Authentication Mechanism for Mobile Payment

YU Xiao-liang, LU Da-long, WU Wei, WANG Yun-feng

(*School of information science and engineering, Xiamen University, Xiamen Fujian* 361005, *China*)

【Abstract】: Mobile payment has become one of the most widely used payment methods of e-commerce platform. However, the dual authentication mechanism used during mobile payment is not security if the cell phone used payment gets viruses. It is also not safe when mobile phone card is copied and mobile phone has been lost. An authentication mechanism for mobile payment is proposed based user name, user password and international mobile equipment identity. Hash function and public key cryptography are applied in the authentication protocol. The result of analysis shows that this authentication mechanism is secure.

【Key words】: Mobile payment; Authentication; Hash function; Public key cryptography

0 引言

互联网的飞速发展，方便了人们的生活，上网聊天、电子邮件、电子论坛等免费网络服务也逐渐成为人们生活的一部分[1]。网络交易的频繁进行极大地促进了手机电子商务的发展[2]。然而，由于网络本身的开放性，如何安全的进行交易成为人们所关注的问题[3]。网上交易的第一步是身份验证，它是保证交易系统安全的第一道门槛，也是一切安全技术的基础[4]。随着科技的快速发展，手机在电子商务中的作用不断突出，利用手机动态验证码进行身份验证的方式被越来越多的人接受并使用。

基于手机动态验证码的身份认证方式，在网上银行和淘宝、京东等电商平台上得到广泛的运用[5,6]。手机动态验证码认证方式的实质是将手机作为用户身份的标识，可是，如果用户的手机中毒、丢失或是手机号码被复制，都会使得动态验证码被非法盗用，那么盗用者就可以冒充用户通过身份认证进入到接下来的操作中。这就给用户的个人信息保护以及财产保护带来不安全的隐患。此外，2015 年 315 晚会还曝光了这样一个问题：公共场所的免费 WIFI 居然会偷钱。究其原因竟然是用户在 WIFI 中传输的信息都是以明文的形式直接传输的。

为了解决上述机动态验证安全问题，同时避免信息在 WIFI 中以明文进行传输的现象，本文基于随机数发生器、用户账户、密码、手机序列号 IMEI，借助于哈希函数[7]与公钥密码[8]等密码技术，设计了一个适用于手机支付的三级身份认证协议。经安全性分析，此方案可以抵制目前已知的各种攻击技术，即使是手机丢失或是手机号码被复制也具备安全性。

基金项目： 国家自然科学基金资助项目(61274133)

作者简介： 余小亮(1993–)，男，硕士，主要研究方向：数字集成电路设计及SLAM系统软硬件设计。

通讯联系人： 王云峰，博士，副教授，主要研究方向：数字集成电路设计及SLAM系统软硬件设计。

1 基于动态验证码的身份认证

为确保网络交易的安全性以及身份的可认证性，当今认证系统普遍采取了双重验证机制，即除了“用户名+密码”验证外，还附加使用手机动态验证码的验证方式[5]。认证过程如图 1 所示。

图中，请求方 A 向认证系统 B 请求通过身份验证，先要将自己的用户名和密码输入到认证系统 B 中，进行第一次身份认证；在通过第一次身份认证之后，认证系统 B 再向请求方 A 的手机上发送短信动态验证码，A 收到动态验证码后立即将其送回给认证系统 B，进行第二次身份认证。

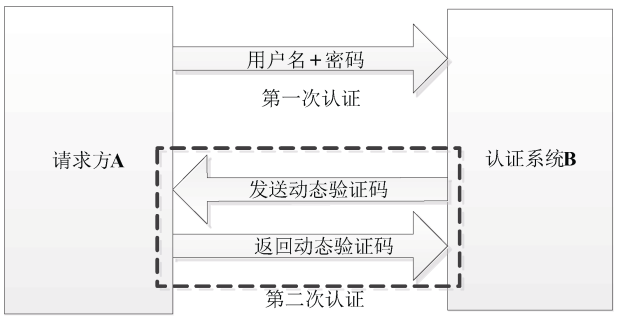

图 1 双重认证机制

在这个认证过程中，第一次认证确保请求方 A 在账号或是密码没有被窃取的情况下可以安全完成身份认证；但是，如果 A 的账号和密码被有心人士 C 窃取，那么可能存在 C 冒充 A 通过身份认证，然后发送虚假信息或接收信息等。而第二次认证通过向 A 的手机发送动态验证码，C 无法获得动态验证码，也就无法完成第二次认证。因此，利用账号+密码和手机动态验证码双重认证的方式，使得身份认证过程更加安全。

但是现实生活中双重认证机制应用于手机上存在以下缺点：（1）如果手机中毒导致账户、密码和认证动态码泄露会使攻击者具备与手机用户同样的操作权限，给手机用户带来经济损失；（2）如果手机丢失，同样受到账户、密码和认证动态码泄露威胁；（3）攻击者通过监视等非法手段获得用户名和密码后非法复制手机号码就可以伪装成手机用户。

2 三级身份认证方案

为了解决手机支付双重认证的安全问题，对电子商务中的身份认证协议进行了设计，提出了三级身份认证机制。请求方和认证方之间利用公钥加密体制进行信息传递，并利用 SHA-256 算法生成动态验证码。三级身份认证中各个变量含义如表 1 所示。

表 1 三级认证机制中各个参数

变量名	含义
A	需要认证的一方（请求方或手机）
B	认证系统（认证方，电子商务平台）
name_A	A 的登录账户
secret_A	A 的登录密码
Phone_A	A 的电话号码
Mail_A	A 的电子信箱
IdB	平台 B 的 Id 号
K_d_A	A 的个人私钥
K_e_A	A 的公开密钥
K_d_B	B 的个人私钥
K_e_B	B 的公开密钥
Mca1	用于第二级认证的动态验证码
Mca2	用于第三级认证的动态验证码
Tab1	用于第二级认证的时间戳
Tab2	用于第三级认证的时间戳
R1	用于第二级认证的随机数
R2	用于第三级认证的随机数

第一级认证流程如图 2 所示，步骤如下：

步骤 1：请求方 A（或手机 A）向认证系统 B 发出请求，想要进行身份认证。

步骤 2：B 系统接收到请求后，允许认证。

步骤 3:A 使用自己的自己私钥 K_d_A 利用公钥密码对登录账户名 name_A 和登录密码 secret_A 进行加密，生成密文 K_d_A（name_A||secret_A），然后再用 B 的公钥 K_e_B 对 K_d_A（name_A||secret_A）进行加密，生成密文 K_e_B（K_d_A（name_A|| secret_A））送给认证系统 B。

步骤 4：B 收到密文 K_e_B(K_d_A(name_A||secret_A))之后，先用自己的私钥 K_d_B 将密文解密，得到 K_d_A(name_A||secret_A)，再用 A 的公钥 K_e_A 对(K_d_A(name_A||secret_A))进行解密，得到 A 的账号名 name_A′，密码 secret_A′，并将其与认证系统 B 中保存的对比账号名 name_A 和密码 secret_A 进行比对，如果 name_A= name_A′，secret_A= secret_A′时，则第一级身份认证成功；如果有一个不相等，则身份认证失败。

第一级认证类似双重认证机制，存在一些安全隐患，因此 A 通过第一级身份认证后，可以在系统 B 中进行一些基本操作：比如浏览网页、添加或删

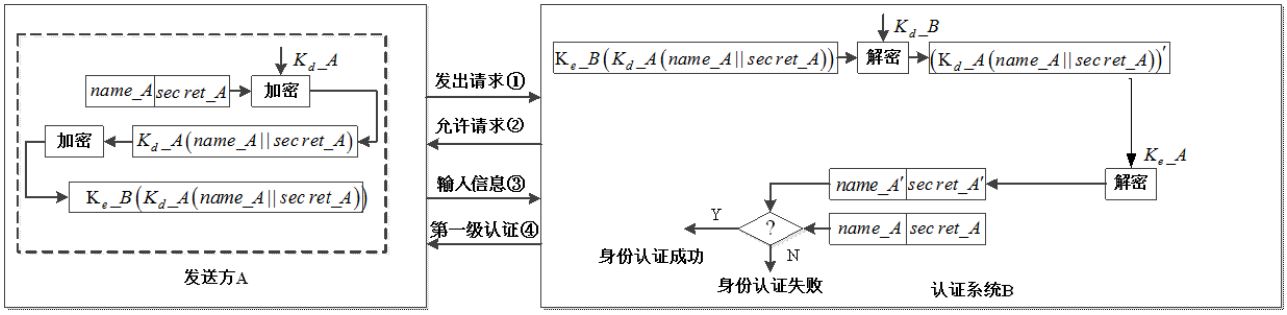

图 2　第一级认证

减收藏等，如果 A 想要完成下一步支付操作时，那么就需要对 A 的身份进行第二级认证。

第二级认证需要在通过了第一级认证基础上才能进行，认证流程如图 3 所示，步骤如下：

步骤 5：请求方 A 向认证系统 B 发出请求，想要进行第二级身份认证。

步骤 6：B 接收到 A 的请求后，立即做出响应。利用 SHA-256 算法生成动态验证码 Mca1，并用 A 的公开密钥 K_e_A 对 Mca1 进行加密，得到密文 K_e_A（Mca1），然后以手机短信的形式向 A 发送密文 K_e_A（Mca1），并开始倒计时 1 分钟，同时保存 Mca1 以待稍后的比对验证。

步骤 7：A 收到密文 K_e_A(Mca1)后，先用自己的私有密钥 K_d_A 对 K_e_A(Mca1)进行解密，得到动态验证码 Mca1′，然后用 B 的公钥 K_e_B 将 Mca1′、A 手机的 IMEI_A、A 要进行的操作编码 Op 进行加密，得到密文 K_e_B(Mca1′‖IMEI_A||OP)，并立即送到交易系统 B 中。

步骤 8：B 收到 A 发送的密文 K_e_B(Mca1′‖IMEI_A||OP)之后，先用自己的私有密钥 K_d_B 对密文进行解密得到 Mca1′、IMEI′、Op，接着将 Mca1′、IMEI′前保存的 Mca1、IMEI 进行对比，如果都相等，就表明 A 通过第二级身份认证，允许 A 在 B 平台上进行 Op 操作，否则 A 就无法通过第二级身份认证，B 平台拒绝 A 所有操作请求。

步骤 6 中 Mca1 是由哈希函数 SHA-256 来产生的。用来产生 Mca1 的 SHA-256 种子如图 4 所示。需要指出的是，由于经过 SHA-256 算法后生成的摘要是 256 位，而实际中使用的验证码是 4 位、6 位或是 8 位的数字或字母组合，因此需要对最后的结果进行相应的截取。具体操作如下：先将哈希种子 Seed 进行 SHA-256 算法计算，生成 Seed 的摘要，即 Hv256，然后根据需要，分别截取 Hv256 的高 16 位、高 24 位和高 32 位，以分别生成 4 位、6 位和 8 位的动态验证码 mca_4、mca_6 和 mca_8。

在第二级身份认证过程中，通过认证手机号码与 IMEI 号，可以防止号码被复制的攻击方式，但无法抵抗手机丢失带来的安全隐患。因此可以允许通过第二级认证的用户进行一些例如小额支付、提交订单等损失不大的操作。如果用户想完成更加敏感的交易操作，保证交易的安全，就需要进行第三级身份认证。第三级身份需要在通过了第一、第二级认证的基础上，通过计算机才能进行，第三级认证如图 5 所示，具体步骤如下：

步骤 9：请求方 A 向认证系统 B 发出请求。

步骤 10：B 接收到 A 的请求后，立即做出响应。利用 SHA-256 算法生成动态验证码 Mca2，并用 A 的公开密钥 K_e_A 对 Mca2 进行加密，得到密文 K_e_A(Mca2)，然后以电子邮件的形式把密文 K_e_A(Mca2)发到 A 的指定邮箱 Mail_A 中，并开始倒计时 5 分钟，同时保存 Mca2 以待稍后的比对验证。

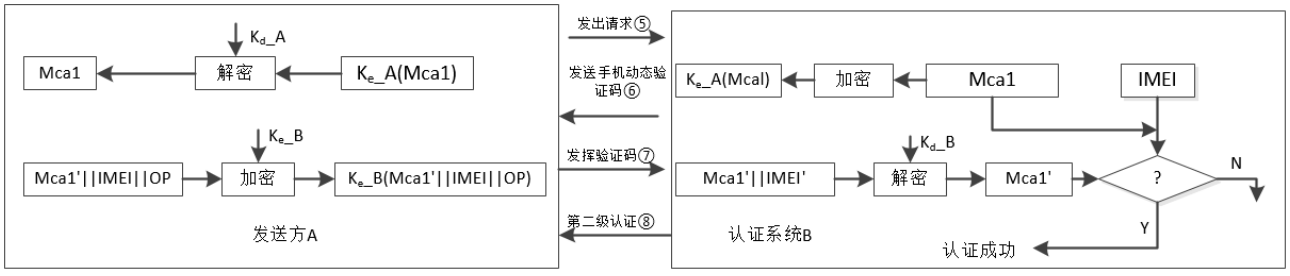

图 3　第二级认证

Phone_A	name_A	IdB	Tab1	R1

图 4　第二级认证动态码的 SHA-256 种子 Seed

步骤 11：A 通过计算机先登陆指定邮箱 Mail_A，取出密文 K_e_A(Mca2)，然后用自己的私有密钥 K_d_A 对 K_e_A(Mca2)进行解密，得到动态验证码 Mca2′，接着用 B 的公钥 K_e_B 将 Mca2′进行加密，得到密文 K_e_B(Mca2′)，并立即送到交易系统 B 中。

步骤 12：B 收到 A 发送的密文 K_e_B(Mca2′_ 之后，先用自己的私有密钥 K_d_B 对密文进行解密得到 Mca2′，接着将其与之前保存的 Mca2 进行对比，如果对 Mca2 和 Mca2′的值相等，就表明 A 通过第三级身份认证，但如果 Mca2 和 Mca2′的值不相等，A 就无法通过第三级身份认证。

步骤 10 中 Mca2 也是由哈希函数 SHA-256 来产生的，除种子不同外，其产生过程同 Mca1 产生过程相同。用来产生 Mca2 的 SHA-256 种子如图 6 所示。

3　安全性分析

在三级认证系统中，每级认证都必须在上一级身份认证通过后，才能进行下一级的身份认证，因此安全性是逐级递增的。平台可以根据安全性赋予不同的操作权限，实现便利与安全的折中。例如小额支付可以分配给第二级认证，不需要通过计算机登录邮箱进行验证；而大额支付必须通过第三级认证，最大程度的保证资金安全。

认证过程中传递的信息都是经过公钥密码加密后再进行传递的，因此，可以有效地避免信息在公共 WIFI 中明文传输的缺陷，使得信息不会被攻击者在信息传递过程有效获得。

第一级身份认证过程中，A 的登录账户与登录密码首先通过 A 的私钥进行加密，在冒充者不知道 A 的私钥的前提下，因此即使冒充者知道 A 的账号和密码，也无法冒充 A 通过身份认证；此级认证无法抵抗重传攻击，即如果手机中毒，冒充者可以获得认证信息，然后重传认证信息获得认证通过；因此认证只具备一般安全性，平台可以不授权任何操作权限或只授权不会造成任何损失的操作。

第二级身份认证首先通过时间戳与随机数抵抗重传攻击，即每次认证请求的认证信息都不相同，因此无法通过重传信息获得认证通过。此外，由于认证还需验证手机的 IMEI 号，因此冒充者即使通过病毒植入获得了 A 的登录账户、登录密码、私钥，也无法通过复制手机卡的方式冒充 A。

第三级身份认证通过向 A 的绑定邮箱发送动态验证码进行认证，请求方必须先通过计算机登录自己的邮箱，才能获得加密后的动态验证码。这样即使冒充者通过病毒植入获得了 A 的登录账户、登录密码、私钥，并且还获得了 A 的手机，也无法通过此级认证。只有在 A 手机中毒、计算机也中毒，同时手机又被攻击者获得的前提下才能被冒充，发生这样情况的概率是非常低的，几乎是不可能发生。

4　结束语

针对手机支付身份认证的潜在威胁，本文基于随机用户账户、密码、手机序列号 IMEI，借助于哈希函数、公钥密码等密码技术，设计了一个适用于手机支付的三级身份认证机制。在认证的过程中，公钥密码用来保护信息在传输通道的安全，时间戳与随机数用来防止攻击者的重传攻击，手机的 IMEI 号用来防御手机卡被复制的危险，而第三级的电子信箱验证保证即使在手机丢失的前提下也不会被攻击者假冒。在使用此认证机制时，应根据需要授权不同级别认证允许的操作，实现便利与安全的折中。

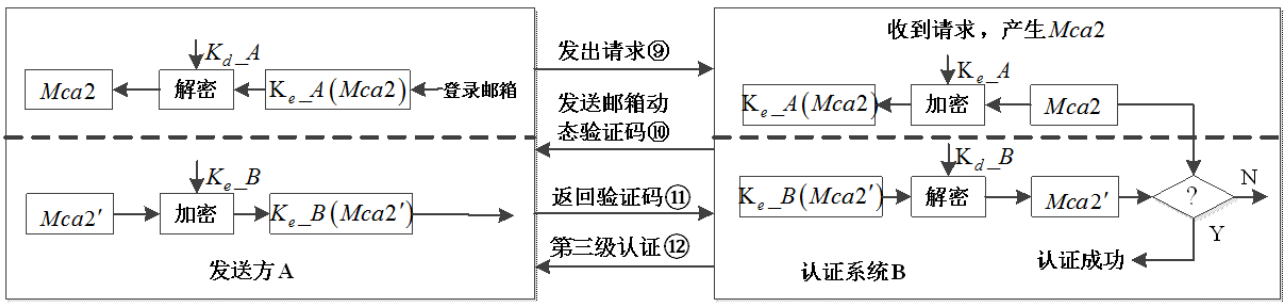

图 5　第三级认证

Mail _ A	*name_A*	*IdB*	*Tab* 2	*R* 2

图 6 第三级认证动态码的 SHA-256 种子 Seed

参考文献

[1] Kahri F, Bouallegue B, Machhout M, et al. An FPGA implementation and comparison of the SHA-256 and Blake-256[C]//International Conference on Sciences and Techniques of Automatic Control and Computer Engineering. IEEE, 2013: 152-157

[2] Shafiq S, Khiyal M S H, Khan A. Development of Mechanism of Integrity in M-Commerce using Joint Signature Scheme[J]. International Journal of Computer Theory & Engineering, 2012, 4(3): 332-336

[3] 郝舒欣，赵耿，徐刚，等. 一种新的基于Chebyshev多项式的身份认证方案[C]//Asia-Pacific Conference on Information Network & Digital Content Security. 2010.

[4] 王斌君，王靖亚，杜凯选，等. 验证码技术的攻防对策研究[J]. 计算机应用研究, 2013, 30(9): 2776-2779.

[5] 彭州. 基于手机动态验证码的网络支付风险分析[J]. 金融科技时代, 2015(1): 61-62.

[6] 马阳明. 基于可信硬件的智能手机短信加密方案[J]. 计算机与现代化, 2016(4): 29-35.

[7] 赵耿，闫慧，童宗科. 基于Chebyshev多项式的公钥密码系统算法[J]. 计算机工程, 2008, 34(24): 137-139

[8] GARC A R, ALGREDO-BADILLO I, MORALES-SANDOVAL M, et al. A compact FPGA-based processor for the Secure Hash Algorithm SHA-256[J]. Computers & Electrical Engineering, 2014, 40(1): 194-202