Advances in Engineering Research, volume 123
2nd International Conference on Materials Science, Machinery and Energy Engineering (MSMEE 2017)

An Identity Authentication Scheme Based on OTP for Mobile Payment

Keqiang Xie[a)], Shizhun Jia[b)], Limei Fu*[c)]

Software Quality Engineering Research Center, CEPREI, Guangzhou 510610, China.

[a)]xiekq@ceprei.com
[b)]Jiasz@ceprei.com
[*c)]fulimei1002@126.com

Abstract. With the development of intelligent terminal and Mobile Internet technology, Mobile payment has become one of the important means of commerce. However, security problems are still challenging mobile payment. Identity authentication is the basic security issue in mobile payment. In this paper, a mobile identity authentication scheme MIAS based on One-time password (OTP) and Elliptic curve encryption (ECC) is presented. Biometric information about user' fingerprint is introduced as an important authentication factors. This paper analyzes the security of novel scheme and prove it by SVO logic.

INTRODUCTION

With the growing maturity of Mobile Internet and rapid development of business applications, mobile intelligent terminals are becoming more and more powerful and widely used. Now mobile financial services such as mobile payment are growing quickly.

The security of mobile payment has drawn more and more attentions. Identity authentication is in the core positon of security mechanism of mobile payment application, because if without effective authentication of the user's identity, the integrity and confidentiality of user information will not make any sense [1]. At present, the authentication mechanism of mobile payment application is mainly based on simple user password and SMS, which are vulnerable to be attacked and password is easily to be intercepted in wireless communication [2, 3] .Also, some authentication methods based on biological characteristics (e.g. fingerprints) are proposed, however, it is vulnerable to replay attack too[4, 5]. Besides, identity authentication mechanism of public key authentication system it must be perfect Certification authority (CA) system as the basis and need a legitimate impartial third party certification, which cost is too high and technology is too complex for mobile payment environment.

OTP has higher security by one time padding. OTP authentication technology does not require third-party certification, with low calculation workload and cost, can be implemented easily and more suitable for mobile payment environment. How, it has some weakness.

In this paper, a bidirectional identity authentication scheme MIAS based on OTP and elliptic curve algorithm for mobile payment is designed, which solve the weakness of OTP and improve authentication security.

The remainder of this paper is structured as follows. In second section related work is briefly summarized. The improved authentication scheme is described in detail in third section. The security of the scheme is analyzed in fourth section and fifth Section concludes this paper with some feature work.

RELATED WORK

OTP and Its Safety Analysis

In 90s, Bellcore established the S/Key one-time password system based on MD4 and MD5 hash function [6]. The S / Key one-time password system divided into server and client: the client calculate one time password according to the secret pass phrase and the challenges information received from the server; the server produce challenge information, check a one-time password response sent by the client, store the last successful authentication password and the serial number in the data record, and the server must let users can conveniently and safely change their secret pass phrase. OTP improve the security by add uncertain factors in login process, so that each login password is not the same.

However, OTP has some weakness, OTP only supports server to authenticate client, cannot prevent client dipeptide by fake server; the attacker can obtain a series of password by using decimal attacks and then posing as legal client. Since client initiating authentication, the random number and secret pass phrase are transmitted in plaintext without encryption protection, OTP cannot resist Man-in-the-Middle Attack [7].

Elliptic Curve Cryptography

At present, three kinds of public-key cryptosystems are recognized as safe and effective. These cryptosystems are divided into: IF type public-key cryptosystem based on the integer factorization problem, such as the RSA system; DLP public key cryptosystem based on discrete logarithm problem of finite multiplicative group, such as DSA; ECDLP cryptography system; the discrete logarithm problem of algebraic curve finite additive group based on elliptic curve cryptosystems, such as ECC[8].

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). ECC requires smaller keys compared to other cryptography to provide equivalent security. For example, ECC with 210bits is equal to RSA with 2048bits [9]. While ECC is easy to implement with hardware and software, so that ECC is suitable for mobile payment authentication environment.

THE SCHEME OF MIAS

This section introduces the scheme of the MIAS. MIAS includes 2 parts: registration stage and authentication stage.

Registration Stage

In the registration process, users using the server generate secure elliptic curve generated by the user's public key, private key, then the user with the server public key exchange, the last user to register the server's public key encryptions

The ID and password (*PW*) are chosen by the user during the registration, before registration, the server generates secure elliptic curve (ECC) parameters, and selects its private key (*KSS*) as well as public keys (*KSR*). When user applies for registration, the server sends ECC parameters with *KSR* to user, user selects its own private key (*KUS*) and public key (*KUR*). When registration, MIAS follows the following steps:

(1) User applies for registration by send a message to server. The server generates ECC parameters, and selects *KSS* as well as *KSR*.

(2) Sever sends ECC parameters with *KSR* to user, then user saves *KSR* and selects *KUS* as well as *KUR*.

(3) User inputs registration user's ID (*UID)* and *PW*, create fingerprint feature information code (*FP*), then user encrypts *PW*, *KUR*, *UID* and *FP* with *KSR*, sends the information to server. The server decrypts and saves the information, check whether registrant successfully.

(4) Server saves user's information, creates random seed character string *SR* and saved as *SR'*, then encrypts server's ID (*SID*) and *SR* with *KUR*, which be sent to user. User decrypts information and saves *SID* and *SR*.

Then registration stage complete.

Fig.1 shows the whole stage and E means encryption.

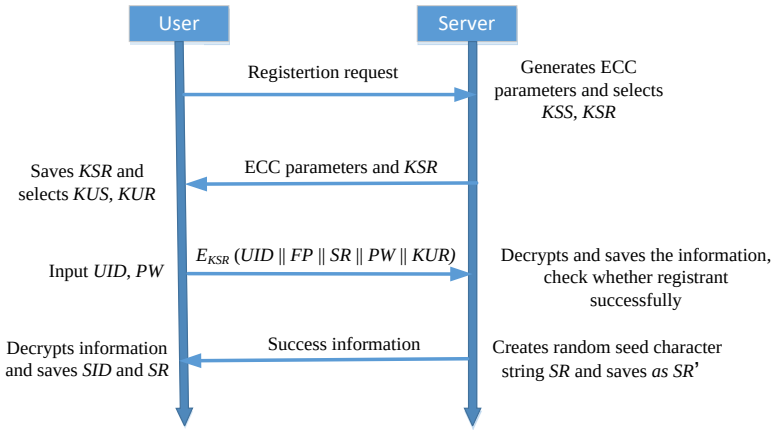

FIGURE 1. The registration stage.

Authentication Stage

The authentication process follows the following steps:

(1) User enters the *UID* and *PW*, creates random seed character string *UR and saves as UR'*, press finger creates *FP*, calculates the hashed value of *PW* and *FP* according to $a=H(FP \| SR \| PW)$. Then *UID*, *UR*, *a* are encrypted by *KSR* and the result $M1=E_{KSR}(UID \| H(FP \| SR \| PW) \| UR)$ is sent to server.

(2) *M1* is received in Server and decrypted by *KSR*, the server checks whether the corresponding *FP* and *PW* exit , if does not exit then authentication end, else calculates *b* according to $b= H(FP \| SR' \| PW)$, if $a=b$, user is validated to be legal, else the authentication end.

(3) If user is validated to be legal, server calculates *c* according to $c=H(FP \| UR)$. *SID and c* are encrypted by *KUR* and the result $M2=E_{KUR}(SID \| H(FP \| UR))$ is sent to server.

(4) User decrypts *M2* by *KUS*, obtains *SID* and *c*, then compare *SID* and *SID'*, if *SID* does not equal *SID'* then reject authentication, else compute *d* according to $d=H(FP \| UR')$. If $c=d$, server is validated to be legal, else is illegal.

Fig.2 shows the whole process of authentication stage.

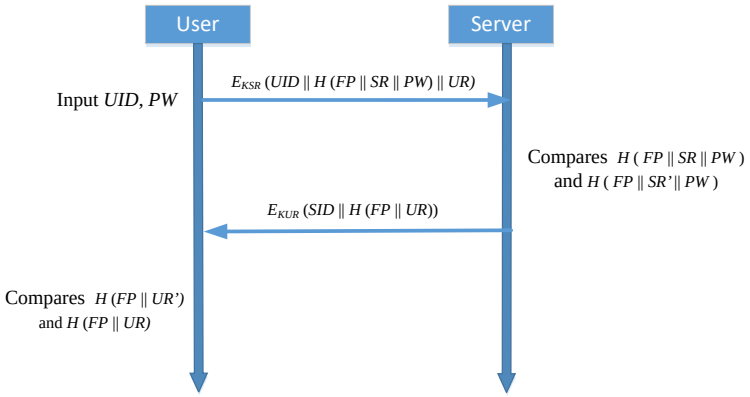

FIGURE2. The authentication stage.

ANALSYSIS ON THE SCHEMES

Security Analysis on the Scheme

The scheme is based on the difficulty of solving elliptic curve discrete logarithm and OTP authentication technology.

(1) Realizes two-way authentication. In scheme the realization of two-way authentication is mainly based on one-time factor. When the server calculates $b=H$ ($FP \| SR' \| PW$)and the a=H (FP || SR || PW) sent by user are same, that the client is legal; and when the client is calculated calculates $d=H$ (FP || UR') and the $c=H$ (FP || UR) sent by the server are same, the server that is legal, if any one of them is not the same, it means that one side cannot be authenticated, the authenticate failed.

(2) Resists against replay attacks and small-number attacks effectively. Due to the random strings generated in each authentication are different, the so the information intercepted by the attacker is not valid for the next use, which can prevent replay attacks and small-number effectively [10].

(3) The password, ID and random strings are in the form of encrypted message with high security during the transmission in the network.

Formally Analyzed Based on Logic SVO

SVO logic is a kind of trust logic method which can be used for formal analysis of protocol. It can discover the vulnerabilities and security flaws in protocol design effectively. It play an important role in security analysis of authentication protocol. It absorbs the advantages of some logic system such as BAN logic, GNY logic, AT logic, at the same time, it has very simple inference rules and axioms. Therefore, it has become a widely used method in formal logic analysis.

Some relevant inferential rules of SVO logical proof include [11, 12]:

(R1) The MP rule: $\psi(\psi \supset \varphi)|\text{-}\ \varphi$

(R2) The Nec rule: $(|\text{-}\varphi) \supset P$ believes φ

A6: $(PK_\sigma$ (Q, k)) $\wedge R$ received $X \wedge SV(X, k, Y) \rightarrow Q$ said Y

A9: P received $(X_1,\ldots, X_1) \rightarrow P$ received X_i (i=1,…,l)

A10: P received $\{ \mid X \mid \}_k \wedge P$ sees $\tilde{k} \rightarrow P$ received X

A17: P says $(X_1,\ldots, X_1) \rightarrow P$ *said* $(X_1,\ldots, X_1) \wedge P$ says X_i (i=1,…,l)

A18: P controls $\varphi \wedge P$ says $\varphi \rightarrow \varphi$

A19: fresh $(X_i) \rightarrow$ fresh $(X_1,\ldots, X_1)$ (i=1,…,l)

A21: fresh(X) $\wedge$ P said $X \rightarrow P$ says X

A22: P received $X \supset P$ sees X

The formal analysis of MIAS based on SVO logic is as follows.

The initial assumption is as follows:

P1: S believes fresh (SR)
U believes fresh (UR)

P2: U believes PK_σ (S, KSS)
S believes PK_σ (U, KUS)

P3: U believes PK_φ (S, KSR)
S believes PK_φ(U, KUR)

P4: U believes $SV(\{SID, H (FP, UR)\}_{KUR,})$

P5: S believes $SV(\{UID, H (FP, SR, PW), UR\}_{KSR,})$

P6: U believes S controls PK_σ (S, KSS)
S believes U controls PK_σ (U, KUS)

P7: U received $(\{SID, H (FP \| UR)\}_{KUR})$

P8: S received $(\{UID, H (FP, SR, PW), UR\}_{KSR})$

The understanding of scheme is as follows:

P9: U believes (U received $(\{SID, H (FP, UR)\}_{KUR})$)

P10: S believes (S received $(\{UID, H (FP, SR, PW), UR\}_{KSR})$)

The target of protocol is as follows:

T1: U believes S says H (FP, UR)
U believes U sees H (FP, UR)
T1: S believes U says H (FP, SR, PW)
S believes S sees H (FP, SR, PW)
The detailed analysis of the scheme is as follows:
R1: U believes U received $\{SID, H(FP, UR)\}_{KUR}$
(According to A9, P9, MP)
R2: S believes S received $\{UID, H(FP, SR, PW), UR\}_{KSR}$
(According to A9, P10, MP)
R3: U believes S said $\{SID, H(FP, UR)\}_{KUR,}$
(According to R1, A6, P2, P4)
R4: S believes U said $\{UID, H(FP, SR, PW), UR\}_{KSR,}$
(According to R2, A6, P2, P5)
R5: S believes U said H (FP, SR, PW)
(According to R4, P3, A17, MP, Nec)
R6: S believes U says H (FP, SR, PW)
(According to R5, A19, A21, P1, Nec)
R7: S believes S received $\{UID, H(FP, SR, PW), UR\}$
(According to A9, A10, P3, P10, MP)
R8: S believes S sees H (FP, SR, PW)
(According to R7, A22, MP)
R9: U believes S said H (FP, UR)
(According to R4, P3, A17, MP, Nec)
R10: U believes S says H (FP, UR)
(According to R6, A19, A21, P1, Nec)
R11: U believes U received (SID, H (FP, UR))
(According to A9, A10, P3, P9, MP)
R12: U believes U sees H (FP, UR)
(According to R11, A22, MP)

R6 and R8 show the Protocol target T1 has been proved, R10 and R12 show the Protocol target T2 has been proved.

CONCLUSION

This paper introduces the characteristics of OTP which is suitable for mobile payment and the security risk of OTP. We have improved OTP by ECC and presented a novel identity authentication scheme. This paper expounds the process of scheme and analyze its security, proves the scheme by SVO analysis. The novel scheme realize two-way authentication between user and server, prevents imitate attacks, replay attacks and small-number attacks effectively. Authentication protocol optimization will be the next step work.

ACKNOWLEDGMENTS

The work was supported by Science and Technology Major Planning Project of Guangdong Province, China (No. 2016B010110004).

REFERENCES

1. Zhiyuan Hu. Password cracking and encryption technology [M]. Beijing: China Machine Press, 2003.
2. Yu Zheng, Dake He and Mingxing He, “An authentication scheme in mobile terminal users based on trusted computation”, Chinese Journal of Computers, Vol.29, No.8, pp.1255– 1264, 2006.
3. Mu Yang, Runtong Zhang and Yi Yang, “New OTP authentication scheme for m-commerce based on one time password”, Computer Security, Vol.28, No.B06, pp.71–72, 75, 2008.
4. Ji Dongyao, Wang Yumin, “An Authentication and Micropayment Protocol for Mobile Computing Network”, Acta Electronica Sinica, Vol.30, No.4, pp.495–498, 2002.

5. Ping Han, Yanqin Zhu, Xizhao Luo, “Identity authentication scheme using OTP in wireless LAN”, Computer Engineering, Vol.34, No.14, pp.161–162, 165, 2008.
6. L. Law, A. Menezes, M. Qu, et al. An efficient protocol for authenticated key agreement. Designs, Codes and Cryptography, 2003,28:119—134.
7. Ao Jinghai, Wang Qin, Zhi Fenhe, “Design and Implementation of Mobile Identity Authentication Mechanism Based on OTP”, International Conference on Information Management, Innovation Management and Industrial Engineering, vol. 02, no. , pp. 248-251, 2010.
8. Zhou Yu, Wang Xiaodong, Cao Xiaohua. “Application of elliptic curve cryptosystem in mobile e-commerce security”. Journal of Ningbo University (Science and Technology) Vol.21, No.2, pp. 145-149, 2008.
9. Sangram Ray and G.P.Biswas, “Design of Mobile Public Key Infrastructure (M-PKI) using Elliptic Curve Cryptography”, Int. Journal on Crypt. And information security (IJCIS), Vol.3, No.1, March. 2013.
10. Xiaomin, et al. “MOTP: An Identity Authentication Scheme for M-Commerce”, Chinese Journal of Electronics Vol.22, No.1, pp. 146-150, 2013.
11. Lei Xinfeng, and Xue Rui. Logic method of cryptographic protocol analysis. Science Press, 2013.
12. Wang Zengguang, Chen Liyun, Lu Yu and. “Design and analysis of WiFi authentication model based on OTP”, Control technology. Vol.35, No.7, pp. 98-101, 2016.