

5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017)

# A Three-factor Two-way Identity Authentication Scheme in Mobile Internet

Mingwen Wang<sup>1, a</sup>, Dongming Tang<sup>2,b</sup>

<sup>1</sup>School of Mathematics, Southwest Jiaotong University, China <sup>2</sup>School of Computer Science and Technology, Southwest University for Nationalities, China <sup>a</sup>wangmw@swjtu.edu.cn, <sup>b</sup>tdm\_2010@swjtu.edu.cn,

Keywords: cryptography, scheme, authentication, biometric, mobile.

# Abstract.

Mobile devices such as smartphones, tablet computers are widely used over the past years. In such mobile Internet environment, how to authenticate a mobile user is a crucial problem. However the single factor based authentication methods are not suitable for high security level applications. Based on Dodis's fuzzy extractor method, a three-factor two-way authentication scheme is proposed in this paper. Password, fingerprint and digital certificate are combined to realize a two-way identity authentication. Compared with the existing mobile user authentication methods, the proposed method is more secure, lightweight and suitable for high security level mobile applications.

# Introduction

With the rapid development of mobile communication infrastructure, most of the online applications can be performed by mobile devices, especially smartphones. Similar to Internet, mobile Internet is also suffered a lot of security risks and threats. Hence, the research of mobile Internet security becomes more and more urgent [1]. In mobile Internet, generally the first secure step is to authenticate the identity of the user. In general, there are three authentication methods: knowledge based authentication, possession based authentication, and biometric based authentication [2]. Static password and dynamic password are two typical authentication knowledge [3], however static password is easy to break and dynamic password is suffered by the risk of the loss of the smartphone [4]. For possession based authentication, a token is provided to the user based on their credentials. After that the user can access the protected online applications by using the token, however the smart card based token may confront the risk of lost and stealing [5]. Biometric based authentication is another type of authentication method. Typical biometrics includes fingerprint, face, palm, iris, voice, finger vein, et al. A typical biometric based authentication algorithm is proposed in [6].

For authentication in mobile Internet, password based authentication is still the most widely used authentication method, however this method is not very secure. Token based authentication has the high security, however it is not very convenient to take the token. Biometric based authentication solved the problem of convenient carrying, however it needs additional biometric device to sample the biometric data. Due to these reasons, the combination of biometric identity and cryptography is becoming a hot research area in recent years. The concept of fuzzy identity based encryption (FIBE) is first introduced by Sahai and Waters [7]. A certain amount of error tolerance in the identities was allowed in the FIBE schemes, so the biometrics could be used in the cryptography easily.

Considering that the function of fingerprint authentication has been included in a lot of type of smart phones at present, we try to combining the fingerprint authentication and the digital certificate based authentication to enhance the security level of the mobile applications. Our proposed authentication method is a three factor authentication method with high security level. Moreover, it is a two-way authentication method, which means not only the user would be authenticated by the server, but also the server would be authenticated by the user.



## Preliminaries

**Fuzzy Extractor Method.** A scheme of turning biometric data to cryptographic keys is proposed by Dodis et al [8]. An algorithm called by fuzzy extractor is proposed to extract a uniformly random string U from biometric data b in a noise-tolerant way.

Suppose the input biometric data be b' and b, if b' is close enough to b, the string U can be reproduced exactly. In order to reproduce U from b', the fuzzy extractor outputs a nonsecret string V and keep U secret.

Let *M* be a matrix with finite dimensions. Let the length of output string *U* be *l* and the minimum noise-tolerant distance be *t*. A distance function is defined as:  $M \times M \rightarrow Z^*$  and an  $(M, m, l, t, \varepsilon)$ -fuzzy extractor is defined by a pair of randomized procedures *Gen* and *Rep*, where:

1. On input  $b \in M$ , the generation procedure *Gen* outputs an extracted string  $U \in \{0,1\}^l$  and a helper string  $V \in \{0,1\}^*$ .

2. The reproduction procedure *Rep* takes an element  $b' \in M$  and a bit string  $V \in \{0,1\}^*$  as inputs. The correctness property of fuzzy extractors guarantees that if  $dis(b,b') \le t$  and U, V were generated by  $(U,V) \leftarrow Gen(b)$ , then Rep(b',V) = U. If dis(b,b') > t, then the output of *Rep* cannot be guaranteed.

3. The security property guarantees that for any distribution b on M of min-entropy m, the string U is nearly uniform.

By the fuzzy extractor, one can extract some randomness U from b and then successfully reproduce U from any string b' that is close to b.

**Formal Model of Asymmetric Encryption Scheme.** A generic asymmetric encryption scheme consists of the following three algorithms.

• Setup: is a probabilistic polynomial-time (PPT) algorithm that takes as input  $1^{l}$  and outputs a pair of keys (x,k), where x is a private key and k is a public key. Here l is a security parameter.

• Encryption: is a PPT algorithm that takes as input a plaintext message m, the message receiver's public key k, outputs a ciphertext  $c \leftarrow E_k(m)$ .

• Decryption: is a PPT algorithm that takes as input a received ciphertext c, the receiver's private key x, and outputs a recovered plaintext  $m \leftarrow D_x(c)$ .

Typical asymmetric encryption schemes include RSA scheme, ECC scheme, SM2 scheme et al.

**Formal Model of Digital Signature Scheme Tables.** A generic digital signature scheme consists of the following three algorithms.

• Setup: is a PPT algorithm run by a PKG that takes as input  $1^{l}$  and outputs a pair of keys (x,k), where x is a private key and k is a public key. Here l is a security parameter.

• Sign: is a PPT algorithm that takes as input a message m, the signer's private key k, outputs a signature of message  $m: s \leftarrow Sig_k(m)$ .

• Verify: is a PPT algorithm that takes as input a received signature s and message m, the signer's public key k, and outputs 1 or 0: 1 or  $0 \leftarrow Ver_k(m, s)$ . If the result of verification is 1, the signature will be accepted, otherwise the signature will be rejected.

Typical signature schemes include RSA signature scheme, ECC signature scheme, et al.

#### The Proposed Identity Authentication Scheme

**System Architecture.** As shown in figure 1, the system is composed of three roles: mobile user(MU), application Service Provider(ASP), and authentication server(AS). Note that we don't distinguish the mobile user and mobile client strictly. The typical process is as follows:

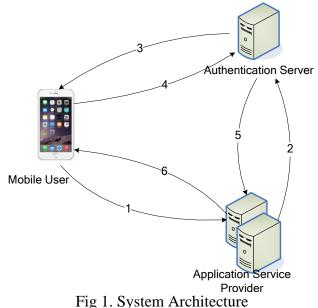
Step 1: The mobile user requests to access an application.

Step 2: The ASP requests the AS to authenticate the MU.

Step 3 and step 4: Two-way authentication is performed between the AS and MU.

Step 5: The AS reply to the ASP the authentication result of the MU.

Step 6: According to the authentication result by the AS, the ASP accept or reject the request of the MU.



**The Details of the Scheme.** The main authentication process is performed between the MU and the AS. For simplicity, we just illustrate the authentication scheme between the MU and the AS. Our scheme consists of three modules as follows.

**Register.** If a mobile user wants to be a valid user of a secure application in Internet, he must register in advance. In the register process, the user MP should present his identity information to the authentication server AS to register, and apply the digital certificate from AS. The main processes are as follows:

1) Based on the public key generation algorithm, a pair of keys  $(x_s, k_s)$  of AS are generated, where  $x_s$  is the private key of AS, and the corresponding public key is  $k_s$ . After that, AS chooses a strong collision-resistant secure Hash function  $h(\cdot)$ . Finally, AS publishes its public key  $k_s$  and the Hash function  $h(\cdot)$  to all potential users.

2) On obtaining the public key  $k_s$  of AS and the Hash function  $h(\cdot)$ , the mobile user begin to register. Since the fingerprint recognition module has become a standard module in modern smart phones, we add fingerprint factor to authenticate a user. Firstly, on obtaining the mobile user MU's fingerprint data b, the mobile client computes  $Gen(b) \rightarrow (U,V)$  and lets U be the user's private key  $x_c$ . The corresponding public key is  $k_c$ . The mobile user sets ACC and PWD as the login account and corresponding password of the application of the mobile Internet, and computes  $M1 = E_{k_s}(ACC || PWD || k_c || h(x_c))$ , where || denotes the concatenation operation. Finally, the mobile user sends M1 to the authentication server over a public channel.

3) On obtaining the message M1, the authentication server AS uses its private key  $x_s$  to decrypt the message  $D_{x_s}(M1) = ACC || PWD || k_c || h(x_c)$ . After that AS check the validity of ACC and PWD. If the verification fails, AS will ask the MU to send a new message, otherwise AS will issue the digital certificate  $Cert = E_{k_c}(PWD || K_c || K_s || Sig_{x_s}(PWD || K_c || K_s))$ . Finally, AS saves ACC, h(PWD),  $k_c$ ,  $h(x_c)$  in the user information database and sends *Cert* to the mobile user MU.

4) On obtaining the message *Cert*, the mobile user MU uses its private key  $x_c$  to decrypt the message  $D_{x_c}(Cert) = PWD || K_c || K_s || Sig_{x_c}(PWD || K_c || K_s)$ . And verify the digital signature

Advances in Engineering Research, volume 141



 $Sig_{x_s}(PWD || K_c || K_s)$  of the certificate. If it succeeds, MU saves the certificate to its mobile client and the register process is over.

Authentication. If a registered user wants to access a mobile Internet application, the following steps would be performed.

1) The mobile user MU inputs his/her account name *ACC* and the corresponding password *PWD* on the login page of the mobile Internet application.

2) On obtaining ACC and PWD, the authentication server AS computes h(PWD) and compares it with the information in the local database. If they are not equal, the access request will be rejected, otherwise transfers to step 3.

3) The mobile user inputs his fingerprint to the mobile client. Using the fingerprint data b' and locally stored help data V, the mobile client computes  $Rep(b',V) \rightarrow U$ . The correctness of fuzzy extractor method guarantees that the string U is the private key of the mobile user, namely  $x_c$ . The mobile client computes  $M2 = E_{k_s}(E_{x_c}(r1))$ , where r1 is a random number, and sends the message M2 to authentication server AS.

4) On obtaining the message  $M_2$ , AS firstly decrypt  $M_2$  by its private key  $x_s$  and the public key  $k_c$  of the mobile user. Then AS selects a different random number  $r_2$  and computes  $M_3 = E_k (h(x_c) || r_1 || r_2)$ . Finally AS sends the message  $M_3$  to the mobile client.

5) On obtaining the message M3, the mobile client decrypts the message  $D_{x_c}(M3) = (h(x_c))' || r1' || r2$ . For received  $(h(x_c))'$  and r1', the equations  $(h(x_c))' = h(x_c)$  and r1' = r1 will be checked. If any of the two equations does not hold, the authentication fails. Otherwise the mobile client accepts that AS is the valid server. After that, AS computes the message  $M4 = E_{k_c}(r2)$  and sends it to AS.

6) On obtaining the message M4, AS decrypts the message  $D_{x_c}(M4) = r2'$  and judges if the equation r2' = r2 holds. If it holds, AS accepts the user is the valid user and allows it accesses the Internet application, otherwise the access will be rejected.

By the above steps, the authentication processes for the mobile user MP and the authentication server AS are finished.

**Cancellation.** If a mobile user does not want to use his digital certificate anymore, he can request to cancel the certificate. The cancellation steps are as follows:

1) The mobile user MU computes his cancellation request of the digital certificate  $Dele = E_{k_{x}}(ACC || PWD || Sig_{x_{x}}(ACC || PWD))$  and sends it to the authentication server AS.

2) On obtaining *Dele*, the authentication server AS decrypts the message  $D_{x_{n}}(Dele) = ACC \parallel PWD \parallel Sig_{x_{n}}(ACC \parallel PWD)$ .

Furthermore the signature  $ACC \parallel PWD$ ,  $Sig_{x_c}(ACC \parallel PWD)$  will be verified. If the signature verification does not pass, then the cancellation fails. Otherwise AS searches the records by the keyword ACC in its user database and modifies the state of the user's certificate to "Cancelled". Finally AS sends the results of the cancellation request to MU.

3) On obtaining the successful cancellation message, the mobile client deletes the stored digital certificate in the mobile phone and the cancellation process is finished.

## **Security Analysis**

Different from most of the existing identity authentication schemes in mobile Internet, our proposed scheme is a three-factor authentication. Firstly, the account name ACC and password PWD will be verified. Secondly, the fingerprint data will be verified in order to generate the correct private key of the mobile user. Finally, the digital certificate of the mobile user will be used in the



interactive authentication process between the mobile user and the authentication server. So the proposed scheme has a high security level, and it is hard to break it.

Moreover, the proposed scheme is a two-way authentication scheme. As shown in previous section "Authentication", by a random value r1, the identity of the authentication server will be verified by the equations  $h(x_c)' = h(x_c)$  and r1' = r1. On the other hand, the identity of the mobile user will be verified by the combination of the account name and password, the biometric data, and the digital certificate based authentication process.

Because the contents in the messages M2, M3 and M4 are simple random numbers r1, r2 and  $h(x_c)$ , the network traffic is low. So the proposed scheme is suitable to use in the mobile Internet.

#### Conclusions

A three-factor two-way identity authentication scheme is proposed in this paper. Password, fingerprint and digital certificate are used to authenticate a mobile user, and the identity of the authentication server is also be verified by the mobile user, so it is an identity authentication scheme with high security level. Moreover, the proposed scheme has a lightweight protocol, so it is suitable to use in the mobile Internet.

## Acknowledgements

The authors would like to thank the National Natural Science Foundation of China under Grant No. 61373009, the Science and Technology Support Project of Sichuan province under Grant No. 2015GZ0089 for financial support.

#### References

- [1] Hualin Sun. Secure signature authentication algorithm in mobile Internet. International Journal of Security and its Applications. Vol 10(3):31-40(2016).
- [2] Uaman Shafique, Asma Sher, Rahim Ullah, et al. Modern authentication techniques in smart phones: security and usability perspective. International Journal of Advanced Computer Science and Applications. Vol 8(1): 331-340(2017).
- [3] S Akram, D Manjunath, AS Nagesh, et al. A survey on knowledge-based authentication. International Journal of Emerging Technologies and Innovative Research. Vol2(4): 1194-1201(2015)
- [4] M Balduzzi, C Platzer, T Holz, et al. Abusing social networks for automated user profiling. In Recent Advances in Intrusion Detection: 13th International Symposium, vol 6307: 422-441(2010)
- [5] P Neamatollahi, Y Sedaghat, M Naghibzadeh. A simple token-based algorithm for the mutual exclusion problem in distributed systems. Journal of Supercomputing: 1-18(2017)
- [6] J Moon, Y Choi, J Jung, D Won. An Improvement of Robust Biometrics-Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. Plos One. Vol 10(12): e0145263(2015).
- [7] A Sahai, B Waters. Fuzzy identity-based encryption. Advances in Cryptology, EUROCRYPT 2005, LNCS 3494, Springer-Verlag: 457-473(2005)
- [8] Y. Dodis, L. Reyzin, A. Smith. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In Advances in Cryptology, EUROCRYPT 2004, in: LNCS 3027, Springer-Verlag: 523-540(2004)