An Identity Authentication Protocol Based on SM2 and Fingerprint USBkey

Zhang Lihua
School of Software, East China Jiaotong University, Nanchang, China
School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai, China

Dai Xichang and Shen Youjin
School of Electrical and electronic engineering, East China Jiaotong University, Nanchang, China

Abstract—In order to solve network security problem, we need identity authentication protocol to ensure legal user’s authority. Multi-factor identity authentication protocols have more merits than the common identity authentication protocol. This paper analyzes the shortcomings of existing network identity authentication methods, and proposes a new authentication protocol based on SM2 and fingerprint USBKey. The proposed scheme, which combines the fingerprint USBKey of fingerprint certificate with the National cipher algorithm SM2, constructs the multi-factor authentication model. And the scheme obtains many merits: 1) it adopts the challenge response authentication mechanism, and realizes the multi-factor mutual authentication; 2) it implements USBKey to verify the user and the remote server authentication by fingerprint features; 3) it can prevent eavesdropping attack, impersonation attack, replay attack and dos attack effectively. 4) it has better calculation and security performance than the existed schemes.

Index Terms—USBKey; SM2; Identity Authentication; Fingerprint

I. INTRODUCTION

The network identity authentication protocol is an important mean to solve the problem of increasingly serious network security problems. However, the common identity authentication schemes have many shortcomings. The static password authentication schemes are vulnerable to password guessing attack and dictionary attack, and passwords plaintext transfer are eavesdropped easily [2]. The dynamic password authentication’s time mechanism stepped out and synchronization events became complicated, because of the existence of time drifting [3-5]. The smart card authentication suffers smart card loss/replication attack [6-8]. A kind of identity authentication based on fingerprint characteristics is proposed by Ge Xiaomin et al [9], but in this scheme, the fingerprint characteristic is transmitted on the unsafe network, which will lead to the illegal invaders steal fingerprint image in the process of network transmission and conduct replay attack [10-12].

Because the existing network identity authentication has respective flaws and traits, scholars put forward some improved measures, that is mixing together static/dynamic password authentication, smart card certification, certification of USBKey, and biometric authentication methods, forming a multifactor authentication [13, 14]. But due to the complexity of the identity authentication and the diversity of network attacks, the authentication scheme for simple physical integration, cannot solve the problem of network identity authentication completely. The smart card authentication scheme based on ECC (Elliptic Curve Cryptography) and iris recognition was proposed by Shu-i Song et al [15], it is still difficult to resist the smart card loss/replication attack. As for the iris feature extraction is complex so that it is inconvenient for daily usage. The dynamic identity authentication scheme based on USBKey was proposed by Liu Huaila et al [16], because the generation of random numbers in the scheme has certain regularity, and USBKey still adopts a protective way of PIN number to control permission, leading to the security of the scheme is not high. In addition, for the security problems based on the commercial password, the State Cryptography Administration stipulates in 1 July 2011, the State Cryptography Administration stipulates that the commercial asymmetric cryptographic algorithm should use the SM2 elliptic curve cryptographic algorithms [17] what is released by the State Cryptography Administration. For the problems in network identity authentication and the existing research results. A fingerprint USBKey identity authentication scheme based on the national cipher algorithm SM2 is proposed in this paper. By putting a fingerprint authentication into the USBKey, using fingerprint instead of the PIN number to verify USBKey access, and the fingerprint is incorporated into the remote identity authentication for user. Through the SM2 asymmetric cryptographic algorithm to sign the interactive information in identity authentication, the security of data transmission is ensured. Adopting national cipher algorithm can make the scheme well applied in the business field.

This paper is organized as follows: In sect. 2, the SM2 and fingerprint USBKey is introduced, a novel identity authentication protocol is proposed in sect. 3, and the security analysis of the scheme is also demonstrated and discussed in sect. 4. Finally, some conclusions are drawn in sect. 5.
II. NATIONAL CIPHER ALGORITHM SM2 AND FINGERPRINT USBKEY

A. National Cipher Algorithm SM2

The identity authentication scheme proposed in this paper uses the national cipher algorithm SM2 [9] based on elliptic curve discrete logarithm problem. As public key cryptography algorithm, SM2 can complete the signature, key exchange and data encryption. The SM2 national cipher standard stipulated the signature, the calculation procedure of attestation and encryption, decryption calculation process. The national cipher algorithm SM2 has more clear advantages of security than the widely used cipher algorithm RSA based on factorization problem of large number, and it is much smaller in the same security, consequently, the calculation are faster, and the efficiency is higher. What's more, the SM2 applied in the commercial field could avoid backdoor attack hidden danger of foreign cipher algorithm procedure.

1) The National Cipher SM2 Signature Algorithm

Assuming the both sides of communication for A and B, A sends the message M to B. Its national cipher SM2 signature algorithm is as follows:

(1) The elliptic curve is defined as \( E(F_p) \), A is the base point that order is \( n \) on elliptic curve. The user A chooses the private key \( d_A \) to calculate the public key \( P_A = d_A G \). \( H() \) is the Hash function. \( Z_A \) is the hash value about identifiable logo of User A, part of the elliptic curve system parameters and public key of User A.

(2) Signature: A calculates \( \overline{\text{M}} = Z_A \mid M \), \( e = H(\overline{\text{M}}) \), then calculate the point on the elliptic curve i.e \( (x_1, y_1) = kG \) (\( k \) is random number), finally, calculates \( r = (e + x_1) \mod n \), \( s = ((1 + d_A) - 1) \cdot (k - r \cdot d_A) \mod n \).

The signature pair for the message \( M \) is \((r, s)\), A send \((r, s)\) and message \( M \) to B.

(3) Verification: After receiving \((r, s)\) and message \( M \), B calculates \( t = (r + s) \mod n \), \( (x_1, y_1) = sG + tP_A \).

Then B calculates \( e' = H(Z_A \mid M) \), \( R = (e', x_1) \mod n \).

And B verifies whether \( R \) is equal to \( r \). If equal, the signature verification was passed, Otherwise, the validation fails.

2) The National Cipher SM2 Encryption Algorithm

Assuming the public and private key pair for B is \((d_B, P_B)\), A uses the public key of B to encrypt message \( M \) whose length is \( l \), then A decrypts the encrypted cipher text. The process of encryption and decryption as follows:

(1) Encryption: A calculates \( (x_2, y_2) = kP_B \), and calculates the cipher text \( C = C_1 \mid C_2 \mid C_3 \), in which \( C_1 = kG(x_2, y_2) \), \( C_2 = M \oplus t \) (\( t = KDF(x_1, y_1, l) \), \( KDF() \) is Key derivation function), \( C_3 = H(x_2 \mid M \mid y_2) \). A sends C to B.

(2) Decryption: B calculates \( d_B C_1 = (x_2, y_2) \), \( t = KDF(x_1, y_1, l) \), finally outputs plaintext \( M = C_2 \oplus t \).

B. The Fingerprint USBkey

The scheme of fingerprint USBkey identity authentication, which combines SM2 cipher algorithm and fingerprint identification technology with USBkey to construct a new type of fingerprint USBkey. The fingerprint USBkey is a kind of USB interface equipment, which is a collection of fingerprint sensor, information security fingerprint processing chip, information security chip, and embedded COS, etc. The fingerprint sensor and the fingerprint processing chip construct the fingerprint processing module of fingerprint USBkey, and the information security chip with the embedded COS constructs the information security module. Its structure is shown in figure 1.

The fingerprint USBkey built-in SM2 cipher algorithm, stores user private key and digital certificate including template of fingerprint characteristic, etc. The fingerprint USBkey can be used for digital signature and encryption/decryption arithmetic. Because of the fingerprint USBkey stores the user key in the key storage area of USBkey, which is unable to export USBkey, all encryption/decryption and signature are carried out in USBkey, ensuring the safety of the private key.

We use the fingerprint characteristic to improve the traditional USBkey with the method of PIN protection, to prevent the PIN code being stolen or being stolen by Trojan, and make USBkey form one-to-one correspondence relationship with the user entity identity, to realize USBkey entity authentication for user. Furthermore, we use the certificate from the user's fingerprint characteristics, to implement the remote service entity authentication for the user.

In order to make the user's fingerprint characteristic not to be tampered with or copied, we use the trusted certificate authority (CA) to generate digital certificate including the fingerprint characteristics with the user's public key bindings. And we promulgate the only corresponding certificate serial number i.e \( fID \). Upon the USBkey initialization, the digital certificate is solidified in USBkey, the fingerprint characteristic certificate contains the user's fingerprint characteristic \( Temp \), which is used for the USBkey access authentication and for remote authentication. The specific process is as follows:

(1) Using fingerprint feature instead of PIN, to implement USBkey about user entity authentication. When user uses USBkey every time, the user must input the fingerprint firstly, then the user's fingerprint characteristic is generated by fingerprint processing chip,
and it is matched with the fingerprint characteristic Temp. Only the feature matching is successful, the user can access USBkey.

(2) Using fingerprint characteristic to implement the remote service entity authentication for the user. When the remote authenticating, the fingerprint feature matching is successful, releasing the sequence number \( f_d \) corresponding to the fingerprint characteristics for remote authentication.

III. PROTOCOL OF IDENTITY AUTHENTICATION

The fingerprint USBkey identity authentication protocol based on SM2 includes phase of user registration, remote authentication, password, fingerprint characteristics change and log off. The main body of the remote authentication includes user, fingerprint USBkey, the remote server and the access control center(ACC) of the remote server. The server provides a remote application server for User, ACC conducts authentication control for user access to the server. Only the legitimate authenticated users are allowed to access to the server. And ACC is responsible for authenticating and issuing the digital certificate that containing fingerprint characteristics.

A. Application for User Registration

Before the user registers to ACC, ACC uses SM2 algorithm to generate the key pair i.e \((x, K_r)\) (\(x\) is private key of ACC and \(K_r\) is its public key), and by using the SM3 algorithm to generate the Hash function \(h()\). ACC publicizes \(K_r\) and \(h()\) to all registered users. The user registration process is shown in figure 2.

The detailed description as follows:

(1) User requests to access server for ACC, and sends \((ID, PW)\) to ACC.

(2) After receiving \(M_1\), ACC employs \(K_r\) in the message \(M_1\) to achieve the result of decryption i.e \(H_1, H_2\) and Temp, as well calculates \(H_2 = h(Temp)\). Then ACC verifies whether \(H_2\) is equal to \(H_1\). If it is equal, the digital certificate \(Cert\) including fingerprint is issued for user’s ID. In addition, \(Cert = E_{K_r}(Temp | f_d)\) | \(ID\) | \(Sing\), Certificate including the encrypted fingerprint features and fingerprint sequence number \(f_d\), the user’s public key, the signature of the ACC etc. The ACC add user list \(U\), which includes \(Cert\), \(H_1\), ACC sends \(Cert\) to USBkey.

(3) USBkey downloads \(Cert\) to digital certificate storage area of USBkey. By the form of encrypting fingerprint characteristic certificate, which can prevent the illegal user from being tampered with the fingerprint characteristics of USBkey effectively.

B. Remote Authentication Process

The remote authentication process is shown in figure 3.

The specific process as follows:

(1) User inputs \((ID, PW)\) into USBkey. After receiving \((ID, PW)\), USBkey calculates \(H_1 = h(ID, PW)\), and verifies whether \(H_1\) is equal to \(H_i\), if it is equal, ACC will calculate \(M_2 = E_{K_r}([n, h(ID, PW)]\) \( (n\) is random number \). Then ACC will send \(M_2\) to USBkey of user.

(2) Fingerprint USBkey employs its own private key \(x\) and public key \(K_r\) of ACC to \(M_2\) after receiving \(M_2\) for obtaining \(h(ID, PW)\) and \(n\). Fingerprint USBkey then verifies whether \(h(ID, PW)\) is equal to \(H_1\) in fingerprint USBkey. If equal, the fingerprint USBkey pass the certification for ACC.

(3) Fingerprint USBkey prompts the user to input fingerprints, after the user inputs fingerprint, USBkey extracts fingerprint image feature and exploits fingerprint template in the certificate of fingerprint characteristic to compare with the user’s fingerprint. If success, it indicates
that the user has access to the fingerprint USBkey, implementing the USBkey entity authentication for the user.

5) After passing entity authentication, USBkey calculates \( M_5 = E_k \{ E_{x} (n, c, f_d) \} \mid ID \) (c is random number) and sends it to ACC.

6) After receiving \( M_5 \), ACC finds out sequence table \( U_i \) of users and obtains the public key \( K_s \) of USBkey via \( ID \), and employs its own private key \( x_s \) and \( K_s \) to decrypt \( M_5 \) for obtaining \( n', c \) and \( f_d \). ACC then verifies whether \( n' \) is equal to \( n \) and \( f_d \) is equal to \( f_d' \). If equal, USBkey passed certification.

C. The Phase That Password and Fingerprint Characteristics Change and Log Off

If users need to change the new ID, password and fingerprint template, identity authentication has to be conducted among user, fingerprint USBkey and ACC/Server, the ID password and fingerprint template have to change after the identity authentication. The specific process is as follows:

1) The change of user ID and password: Inputting new \( (ID', PW') \) into USBkey, and USBkey calculates \( H_1 = h(ID', PW') \), \( M_4 = E_{x} (H_1, ID) \mid K_s \mid ID \), afterwards, sending ACC the \( M_4 \) to update user's sequence table, and calculates the new digital certificate to fingerprint USBkey, updating the certificate.

2) The change of user fingerprint template: USBkey achieves user's fingerprint image to generate a new template \( Temp' \) of fingerprint characteristic, and calculates \( M_5 = E_{x} (H_1, H_2, Temp') \mid K_s \mid ID \) to ACC. Depending on \( M_5 \), ACC calculates the new digital certificate containing the fingerprint characteristics and sends it to USBkey. USBkey downloads the digital certificate to the storage area of USBkey certificate.

IV. PERFORMANCE ANALYSIS

A. Security Analysis

For the identity authentication technology is proposed in this scheme, analyzing its ability about resist attacks and security.

1) The Security Identity Authentication Among Subjects

Analysis: The mutual authentication relationship among user, fingerprint USBkey and ACC/Server is shown in Figure 4.

> Figure 4. The mutual authentication relationship among subjects

The figure 4 shows that the fingerprint USBkey and ACC/Server implement two-factor authentication for User, and fingerprint USBkey conducts the entity authentication for user, improving the security of the identity authentication. Utilizing the user's fingerprint characteristics and the random number achieves the two-way authentication between fingerprint USBkey and the ACC/Server. The employment of fingerprint characteristics and USBkey realize the bidirectional authentication between the user and the ACC/Server indirectly. By using password, fingerprint and USBkey formed the multifactor authentication scheme, the security is strong.

2) Anti Hacking Attacks

Analysis: In the process of the mutual authentication for User and the ACC, assuming that the attacker \( C \) monitored authentication data of User and ACC. Attacker monitored \( M_2 = E_{K_s} \{ E_{x} (n, h(ID, PW)) \} \) in the process (2) of authentication phase, however, as a result of lacking of private key \( x_s \) of user, it's impossible for \( C \) to decrypt arithmetic, as well get \( n, h(ID, PW) \) to implement attack. In the process (3) of authentication phase, attacker \( C \) monitored \( M_3 = E_{K_s} \{ E_{x} (n, c, f_d) \} \mid ID \). However, the attacker \( C \) cannot achieve the purpose of hacking attacks for lacking of private key \( x_s \) of ACC.

3) Anti-Repeat Attacks

Analysis: Due to the User and the ACC for identity authentication, all of the authentication information uses the random number, such as \( (n,c) \), ensuring the freshness of information so that the attacker can't do replay attack.

4) Anti Counterfeiting Attacks

Analysis: The attacker \( C \) in the identity authentication of user and ACC, faking certification entity that is User or ACC, But the attacker \( C \) is without the private key of authentication on both sides, so \( C \) can't make fake attacks for identity authentication. When the attacker \( C \) fakes User to proceed identity authentication, because there is no User's fingerprint, \( C \) cannot use fingerprint USBkey, even cannot use fingerprint USBkey to achieve identity authentication with sever. When the attacker counterfeits the ACC, he can acquire \( M_5 = E_{K_s} \{ E_{x} (n, c, f_d) \} \mid ID \), but without the private key of ACC, he is unable to obtain certificate.

5) Anti Dos Attacks

Analysis: The certification request what is sent to the ACC must contain the correct \( f_d \) i.e the serial number of user’s fingerprint characteristics. Only responding the next identity authentication, the ACC has to testify \( M_3 = E_{K_s} \{ E_{x} (n, c, f_d) \} \mid ID \), or will close certification sessions immediately to resist DOS attack effectively.

According to above analysis, this scheme and security contrastive analysis of literature mentioned in the introduction is shown in Table 1.

B. Performance Analysis

The results of identity authentication scheme compared with the efficiency of the scheme are presented in table 2. Using the secret algorithm SM2 to encrypt authentication messages, improves the security and efficiency of authentication protocol.
V. CONCLUSION

Using the fingerprint USBkey to store user’s private key can protect the security of private key. Utilizing the fingerprint characteristics to replace the PIN number of USBkey can resist password attacks, because PIN number is stolen easily, and can carry out USBkey to the entity authentication of the user. Building digital certificate about fingerprint characteristic can prevent illegal users from tampering with the fingerprint characteristics of USBkey. Introducing fingerprint to remote identity authentication can realize remote server to the entity authentication of users. All in a word, this scheme based on SM2 and fingerprint USBkey has high security and efficiency.

ACKNOWLEDGMENT

The author would like to thanks for the financial support by scientific research project fund of Jiangxi province (GJJ14371) and the aids from East China Jiaotong University. The authors would like to thanks the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

Zhang Lihua received the BS degree in Electrical Engineering from the East China Jiaotong University, Nanchang, China in 1994, and the MS degrees from the school of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang, China in 2003. He received the PhD degree from the Beijing University of Aeronautics and Astronautics, Beijing, China in 2011. He is currently an associate professor in the School of Software at East China Jiaotong University, Nanchang, China. His current research interests include information security, security protocol design in wireless mesh networks and wireless sensor networks, identity authentication and mobile communication. He is a member of the IEEE and ACM.