A Secure Email System Based on Fingerprint Authentication Scheme

Zhe Wu[1], Jie Tian[1,3], *Senior Member*, *IEEE*, Liang Li[1], Cai-ping Jiang[2], Xin Yang[1]
[1]Center for Biometrics and Security Research, Key Laboratory of Complex Systems and Intelligence Science, Institute of Automation, Chinese Academy of Sciences. Graduate School of the Chinese Academy of Sciences, P.O.Box 2728 Beijing 100080 China
[2]The First Research Institute of Ministry of Public Security of P.R.C, Beijing 100044 China
[3]Life Science Center, Xidian University, Xi'an, Shaanxi, 710071, China

Abstract—**Most of secure email systems adopt PKI and IBE encryption schemes to meet security demands in communications via emails, however, both PKI and IBE encryption schemes have their own shortcomings and flaws and consequently bring security problems to email systems. This paper proposes a new secure email system based on a fingerprint authentication scheme which combines fingerprint authentication technology with IBE scheme. The system perfectly solves the existing problems encountered in email security protection implementations.**

Index Terms—**Secure email systems, PKI, IBE, fingerprint authentication scheme**

I. Introduction

With rapid developments of network and computer technologies, personal, enterprise, and governmental communications via emails become more and more widespread. The main reason why using emails is probably because they are convenient and time-saving. Individual privacies, commercial secrets, even country's intelligence information are being delivered through emails and thus contents in emails are more valuable than ever. Therefore, the security of emails has raised more concerns. Recently, many secure email systems are brought out and most of these systems are based on Public Key Infrastructure (PKI) or Identity-Based Encryption (IBE) schemes. However, implementing PKI, IBE or other information security techniques based on cryptography are facing a challenge of lacking the exact connection between cryptographic key and legitimate users. Besides, each scheme has its inherent shortcomings and flaws: In PKI scheme, certificates are not easily located; there needs strict online requirement; validating policy is time-consuming and difficult to administer; certificates leak data and users must pre-enroll; In IBE scheme, it is difficult in prove self-identity to Trust Authority (TA) and authenticate email sender's identity, etc. A number of great efforts [1]-[3] have been made to solve the problems mentioned above. However, none of these works are fully satisfactory and hence there isn't any satisfactory secure email system coming out yet.

Biometrics, which refers to distinctive physiological and behavioral characteristics of human beings, is more reliable indicator of identity than traditional authentication systems such as passwords-based or tokens-based ones [4],[5]. Fingerprint is the most widely used biometrics because of its uniqueness and immutability. In this paper, we propose a new secure email system based on a fingerprint authentication scheme which combines fingerprint authentication technology with IBE scheme. The novelty of this paper is introducing fingerprint authentication into security email system in order to solving the existing problems encountered in email security protection.

The rest of the paper is organized as follows. We briefly outlined the proposed system's fundamental scheme in section 2 and described the proposed secure email system implementing fingerprint authentication scheme in section 3. In section 4 and section 5, we presented manipulation instructions in details and analysed security issues, respectively. Finally in section 6, summary and conclusions are given.

II. Fingerprint Authentication Scheme

The proposed system's fundamental scheme combined fingerprint authentication technology with IBE scheme solves fatal problems which IBE scheme can not deal with alone. The adoption of fingerprint authentication technology can be considered referring to two aspects: fetching private key of identifier from Trust Authority (TA) and authenticating email sender's identity. For explaining the total scheme briefly, we present it by describing four algorithms: *Setup, Encryption, Decryption, Verification.*

A. Setup

TA initializes a secure area, constructs a supersingular elliptic curve satisfying Weil Diffie-Hellman (WDH) assumption and defines a bilinear map $\overline{e}$, a hash function H_1 and a map function H_2. TA chooses three secrets $s,u,v \in \mathbb{Z}_q^*$, one point $P \in G$ and computes three associated public keys P_{pub}, P_{FP_pub}, P_{online} where s, u, v are the master key of TA, fingerprint and online-services respectively. Besides, TA defines a signature function Sig, a verification function Ver, a fingerprint summary extraction function H which maps fingerprint template to fingerprint summary represented by bit string, a fingerprint summary matching function FPM, a standard symmetric encryption function such as AES and a standard hash function such as SHA-1, which are denoted by E and $Hash$ respectively. TA's identifier is also be defined in order to generate public/private key pair.

1-4244-1330-3/07/$25.00 ©2007 IEEE.

Thus, the system's public parameters are

$$params = \{\overline{e}, P, P_{pub}, P_{FP\_pub}, P_{online}, H_1, H_2, Sig, Ver, E, Hash\}$$

B. Encryption

Assume A intends to send an email to B. A should register at TA. TA writes public params and A's personal params into A's Usb-Key$_A$, details will be introduced in section 3. When A writes an email, the encryption process is as following steps, M denotes the plaintext:

step 1 : Usb-key$_A$ authenticates A by capturing fingerprint summary on site b_A' and comparing b_A' with the fingerprint summary b_A stored in Usb-key$_A$. If authentication succeeds, A is allowed for next steps

step 2 : Usb-key$_A$ generates A's signature FPS_A automatically by using signature function Sig with A's onsite fingerprint summary b_A', onsite time and A's private key of fingerprint.

step 3 : A picks a random data $a \in \mathbb{Z}_q^*$, computes a symmetric key by function $\overline{e}$, then uses the symmetric key to encrypt the signature FPS_A by function E and obtains authentication data $AUTH_A$.

step 4 : A picks a random data $r \in \mathbb{Z}_q^*$, computes a session key K_{AB} by function $\overline{e}$, encrypts M by using function E with K_{AB} and obtains Enc_{AB}. A sends ciphertext $CIPH_1$ to B where

$$CIPH_1 = Enc_{AB} + Hash(Enc_{AB}) + AUTH_A + r \bullet P$$

C. Decryption

When receiving the email from A, B computes the session key K_{AB} with his private key of identifier and uses K_{AB} to decrypt Enc_{AB} to get M.

D. Verification

When B wants to verify A's identity, TA provides online identity authentication service. Receiving $AUTH_A$ sent from B, TA first encrypts it and obtains A's onsite fingerprint summary b_A', then verifies the signature FPS_A by verification function Ver. If Ver is true, TA matches b_A' with the registered fingerprint summary b_A stored in database by function FPM. TA returns the matching result to B after encryption and signature. Finally, B verifies A's identity.

III. Implementation

A secure email system generally consists of three parts: the Trust Authority (TA), email-server and email-client. We put more emphasis upon two main parts in our secure email system, *TA and Email-client*.

A. TA

In the proposed system, TA provides several functions: master key generation and preservation, user's fingerprint collection and transformation to fingerprint summary, fingerprint certificates generation, fingerprint certificates database management, user's private key of fingerprint generation, Usb-key issue, user's private key of identifier generation, user's identity authentication on line, etc. All these functions can be fulfilled in the form of TA's services toward users. TA has four main services: user registration, online secret-key distribution, online identity authentication and online identifier update as shown in Fig.1.

1. User registration:

A registers at TA taking his own identification such as driving licence, medical care certification or other certificates which can prove his real identity. TA verifies the legitimacy and will, if succeeds, continue the process described as following steps:

step 1 : TA captures A's fingerprint, and then transforms it to fingerprint template FPT_A. TA generates a basis set of pseudo random number R_A and computes fingerprint summary b_A by using fingerprint summary extraction function H with FPT_A and R_A.

step 2 : TA enrolls A's identifier: ID_A, which contains A's own string (like an email address) and an expiring date TI_A. TI_A is used to testify whether or not A's identifier has run out.

step 3 : TA computes A's fingerprint certificate C_A by function Sig with b_A, ID_A and TA's identifier. TA memorizes ID_A and C_A in the fingerprint certificate database.

step 4 : TA computes A's fingerprint identifier Q_{FP_A} and the private key of fingerprint D_{FP_A} which is used to sign the onsite fingerprint summary and the onsite time.

step 5 : TA writes the public params $\{P, P_{T\_pub}, P_{pub}, P_{online}, H, H_1, H_2, Sig\}$ and A's personal params $\{D_{FP\_A}, C_A, R_A, b_A\}$ into Usb-key$_A$, and hands over it to A.

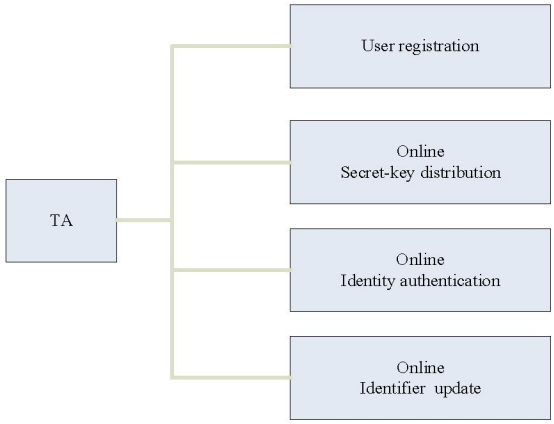

Fig.1. TA's four main services

We integrate fingerprint sensor and USB token into one device called Usb-key. The Usb-key is able to capture and process fingerprint image. There is an independent time

system in the Usb-key, the onsite time will be generated and signed in sender's signature. User's Usb-key is used for storing fingerprint identifier, private key of fingerprint and other relative params. Besides, it also contains fingerprint summary matching algorithm and Identity-Based Signature algorithm (Sig and Ver), and be able to be protected against duplication of private key of fingerprint.

2. Online secret-key distribution:

When ***B*** receives an email form ***A***, he can connect with TA online to fetch his private key of identifier for ciphertext decryption. The process is as following steps:

step 1 : ***B*** applies to TA requesting private key of identifier. ***B*** chooses a random data $c \in \mathbb{Z}_q^*$, computes the symmetry secret key and generates a session key. ***B*** encrypts the service type, his fingerprint signature FPS_B and session key with the symmetry secret key by using function E and obtains C_{pri}. At last, ***B*** sends $CIPH_2$ to TA where $CIPH_2 = C_{pri} + Hash(C_{pri}) + c \bullet P$

step 2 : TA authenticates ***B***' identity. TA receives $CIPH_2$ from ***B***, computes symmetry secret key with the master key of online-services, decrypts C_{pri} and obtains service type and the session key. TA exacts ***B***'s onsite fingerprint summary from FPS_B to verify FPS_B by function Ver and then computes function FPM to authenticate ***B***'s identity.

step 3 : TA sends ***B***'s private key of identifier to ***B***. TA encrypts ***B***'s private key of identifier with the session key by function E and obtains C_{back}. TA sends $CIPH_3$ to ***B*** where $CIPH_3 = C_{back} + Hash(C_{back})$

step 4 : ***B*** obtains his private key of identifier from TA by decrypting $CIPH_3$.

3. Online identity authentication:

The process has been described in Section 2. ***B*** sends ***A***'s authentication data to TA. TA authenticates ***A***'s identity and returns matching result to ***B***.

4. Online identifier update:

Assume ***B*** wants to update his identifier, he could apply to TA online for relevant service. Like online secret-key distribution service, step1, ***B*** computes C_{pri} which also contains ***B***'s new string. Then ***B*** sends $CIPH_2$ to TA. After authenticating ***B***'s identity, TA provides update service requested by ***B***. TA recomputes ***B***'s identifier and fingerprint certificate, encrypts them with the session key and obtains C_{update}, then returns $CIPH_4$ to ***B*** where $CIPH_4 = C_{update} + Hash(C_{update})$.

B takes new identifier and fingerprint certificate instead of the old ones in Usb-key$_B$.

B. Email-client

Email-client is the terminal unit of the proposed system and manipulated by user directly. It must have a visual and friendly user interface. Besides the basic functions as a normal email-client, the proposed email-client provides four more functions: local login authentication, email encryption and decryption, intercommunication with Usb-key and intercommunication with TA.

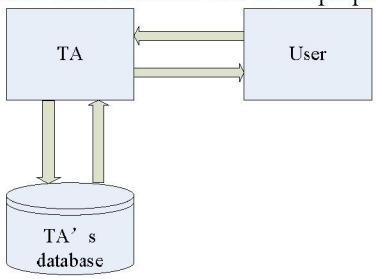

Fig.2. Interaction between TA and User's email-client

Local login authentication. When the user wants to login the email-client, he needs pass the local login authentication with his Usb-key. Usb-key authenticates the user's legitimacy by comparing onsite fingerprint summary with the fingerprint summary stored in Usb-key. Whether or not the user can login the email-client depends on the authentication result. If one doesn't have an Usb-key or the Usb-key doesn't belong to him, he will be rejected by the email-client.

Encryption and decryption. The processes of encryption and decryption can be completed by email-client automatically. Users only need to choose special function options provided in the user interface of the email-client to finish process strictly according to the proposed scheme mentioned in section 2.

Intercommunication with Usb-key. When intercommunicating with Usb-key, the email-client will send special commands to Usb-key which will then return corresponding response to email-client helping to achieve relevant functions.

Intercommunication with TA. As shown in Fig.2, the intercommunication with TA includes three aspects: private key of identifier distribution, email sender's identity authentication and identifier update. There are functional options displayed in the user interface, which are corresponding to special services with TA. Under the guidance of the email-client, the user can choose these options to achieve the corresponding functions expediently without understanding concrete principles. The communications between user and TA are encrypted in case of wiretapping.

IV. MANIPULATION

A secure email system's interaction diagram is given in Fig.3. For illustrating the manipulation of the proposed system, we propose the following steps:

step 1 : ***A*** registers at TA and obtains his Usb-key$_A$.

step 2 : ***A*** uses Usb-key$_A$ to login the email-client system, writes the email, selects encryption option in the user interface, and then sends the email via internet.

step 3 : ***B*** registers at TA and obtains his Usb-key$_B$.

step 4 : ***B*** receives the email from email-server via internet. The email-client will notice ***B*** whether he has his

private key of identifier or not. If ***B*** has the key, he can choose "decryption" option to decrypt ciphertext to plaintext. If not, the "decryption" option is disabled, ***B*** can select "secret-key distribution" option to connect with TA online for the private key of identifier. After TA authenticates his identity, ***B*** obtains his private key of identifier, and "decryption" option becomes available. Thus ***B*** decrypts the ciphertext and reads the plaintext.

step 5 : If ***B*** wants to verify sender's identity: whether or not is ***A***, he can choose "online identity authentication" option and email-client will automatically send ***A***'s authentication data to TA. After receiving TA's authentication result, email-client will notice ***B*** the result.

step 6 : identifier update: If ***A***'s identifier has been expired, the email-client will notice ***B*** this information though checking the time signed in ***A***'s signature in the email. If ***A*** wants to update his identifier, he can choose "identifier update" option to ask TA for identifier update service online. When TA sends the updated data to ***A***, the email-client will write the data into ***A***'sUsb-key$_A$ and notice ***A*** identifier update is completed.

V. Security Analysis

We mainly emphasize security analyses after we introduce the fingerprint authentication scheme to the proposed secure email system. We will explain how the proposed system solves several security issues respectively which need to be most concerned. We are assuming ***C*** is an attacker.

(1) ***C*** pretends ***B*** to ask TA for ***B***'s private key of identifier.

It is a big issue that other secure email systems based on IBE scheme haven't solved perfectly yet. In our system, fingerprint authentication is used to overcome such serious problem. ***B*** extracts his onsite fingerprint summary and signs it with his private key of fingerprint. ***B*** sends TA his signature after encryption. TA uses ***B***'s signature to authenticate ***B***'s identity. If ***C*** pretends ***B*** to ask TA for ***B***'s private key of identifier, he needs ***B***'s private key of fingerprint. However, ***B***'s private key of fingerprint is stored in Usb-key$_B$ which is unreadable. ***C*** could not fabricate it. So, ***C*** cannot pass TA's identity authentication and therefore fails to get ***B***'s private key of identifier.

(2) ***C*** pretends ***A*** to send an email to ***B***.

When writing an email, ***A*** needs to sign his onsite fingerprint summary and the onsite time with his private key of fingerprint and put the signature in the email. When ***B*** gets the email from ***A***, he sends ***A***'s signature to TA to verify ***A***'s identity. If ***C*** pretends ***A*** to send ***B*** an email, he has to use ***A***'s private key of fingerprint. The same as (1), ***C*** could not fabricate it and so, ***B*** can confirm ***A***'s identity accurately.

(3) ***B*** pretends ***A*** to send email to other users like ***D*** or TA.

If ***B*** uses ***A***'s signature and ***A***'s fingerprint certificate to pretend ***A*** to communicate with other users like ***D*** or TA .They can check the onsite time, which is generated by Usb-key$_A$ and signed in signature, to avoid being cheated.

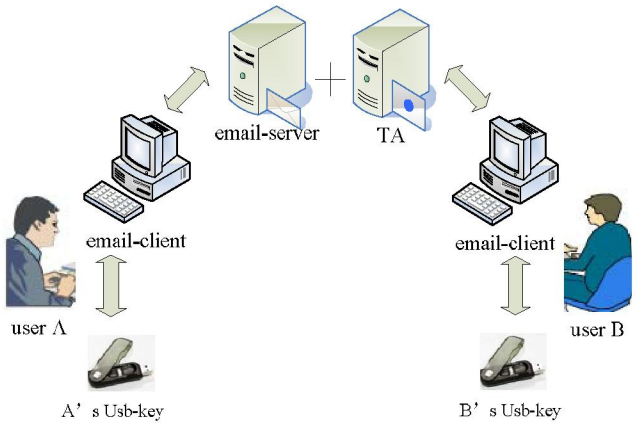

Fig.3. Secure email system interaction diagram

VI. Conclusions

In this paper, we presented a new secure email system based on a fingerprint authentication scheme which combines fingerprint authentication technology with IBE scheme. The novelty of this paper is introducing fingerprint authentication scheme into security email system in order to solve existing problems encountered in email security protection using IBE scheme alone. We briefly described the proposed scheme and put the main emphasis on the system implementation. In order to show the proposed system's security performance, we analysed serveral common but serious security issues and presented the solutions to these issues by the proposed system.

In the system, we use Usb-key to keep secret data and help completing relevant encryption process. Usb-key can only be used by its legitimate owner. Thus the system successfully combines cryptographic key with legitimate users.

Acknowledgment

This paper is supported by the Project of National Science Fund for Distinguished Young Scholars of China under Grant No. 60225008, the Key Project of National Natural Science Foundation of China under Grant No. 60332010 and 60575007, the Project for Young Scientists' Fund of National Natural Science Foundation of China under Grant No.60303022, and the Project of Natural Science Foundation of Beijing under Grant No.4052026, Chair Professors of Cheung Kong Scholars Programme, the Program for Changjiang Scholars and Innovative Research Team in University and the CAS Hundred Talents Program.

References

[1] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.

[2] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceeding of the International Conference on Advances in Cryptology, pages 213-229. Springer-Verlag, 2001.

[3] Mont. M. C and Bramhall. P. IBE applied to privacy and identity management. Trusted Systems Laboratory. HP Laboratories Bristol, 2003.

[4] Jie Tian, Liang Li, Xin Yang, "Fingerprint-based identity authentication and digital media protection in network environment," Journal of Computer Science and Technology, Sept.2006, Vol 21, No.5..

[5] Umut Uludag, A.K.Jain, "Biometric Cryptosystems: Issues and Challenges", Proceeding of IEEE, 2004.