

The PKI authentication system with the integration of Biometric identification and non-symmetric key technology

LIU Shan

School of Economics and Management, BUPT, Beijing, China

E-Mail :l_i_u_sung@sina.com

Abstract—To deal with the threats to the PKI authentication system from the internet and the real world, based on the analysis of biometric identification and non-symmetric key technology, this paper presented a new PKI authentication system through the integration of Biometric identification and non-symmetric key technology, which assembled their advantages and made up their disadvantages to each other and formed a double-insurance for the E-commerce security. The most important of the system were the integration designs and measures for the private key ,also principles and the processes needed were introduced .

Index Terms—PKI, non-symmetric key, biometric identification

I. INTRODUCTION

E-commerce has brought great changes to the whole development process of society through raising awareness of management style. It is the result of the operation and management of technology innovation and integration. Nowadays the main problem of E-commerce is the security issues. To guarantee security issues of E-commerce, PKI technology as an effective solution is introduced , which is not only considered as the core of information security technology, but also the basic technology to solve the security of E-commerce.

PKI [1] is a kind of key management platform according to a certain established standards. It can provide all network applications with the public-key and encryption management necessary to the digital signatures and other key services. PKI authentication system mainly includes six aspects: certification(CA)、registered (RA) 、 certificates and certificates pool 、 key backup 、 recovery system and the PKI application interface system. PKI's main function is to guarantee the confidentiality of data transmission in E-commerce authentication and establish the trust relationship in transactions. It has the features of transparency、 ease of use, interoperability、 scalability 、 verifiable and wide range supports of applications and so on.

After many years of application and development, PKI technology has become a relatively mature information security solution that can realize good confidentiality、 integrity 、 non-repudiation for the information. It has solved many problems of E-commerce security. But there still exist many problems in the application of PKI technology. PKI bases on non-symmetric encryption

algorithm or Hash- algorithm, with the rapid development of computer 、 mathematics and other disciplines, public keys' crack gradually become possible; The Keys over rely on the centralized storage and management so that they become the targets easily; Furthermore, the biggest problem of PKI is that the private keys can easily be lost or stolen and result in the meaninglessness of entire PKI authentication system.

Through summary and improve the past research ,this paper emphasized that the integration of biometric identification and non-symmetric key technology could assemble both their advantages and make up their disadvantages to each other , form the double-insurance and cover the loophole for the security of E-commerce ,thus allow PKI authentication system to protect e-commerce more effective.

II. ANALYSIS TO NON-SYMMETRIC KEY TECHNOLOGY

Non-symmetric key[2], also known as public-key encryption, is to encrypt respectively by using two different keys: one is Known to the outside world, named "public key", the other can only be mastered by the owner , named "private key". Public key and private key have a close relationship to each other. The information encrypted by public key can only be decrypted by the corresponding private key. Non-symmetric key system can be shown as Fig.1[3].

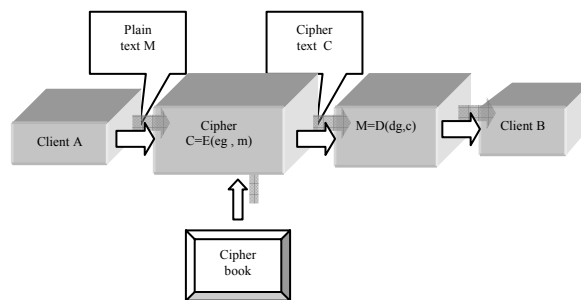


Figure 1. The system of non-symmetric key technology

For one of non-symmetric key's advantages-- simple key distribution, public key can be open to the public, every user only need memorize his private key respectively, so non-symmetric key decreases the number of keys with confidentiality. Since the private key exists in real world in implicit form, except for some the easy passwords with weak safety awareness , the

possibility of password stolen is very little. The main threat to the private key comes from the internet through the following methods[4] (1)password attack procedures: such as Crack、XIT、etc, which can attacks on Unix system; 10phtCract210、password NT, which can attacks Windows NT; other types of passwords attack procedures like ZipCract、NetCract; (2)password shield: that is, make use of some special procedures, skip directly into the system password. (3)theft of passwords: that is, the password is sent in plain text, in many networks, the message sent from the general browser to Web is also plain text, Thus the thieves can easily obtain a password. While some http, if not plain text, password crack is also very easy. (4)Trojan horse attacks: that is, under the circumstances of unawareness, the hackers install some special procedure to the user's compute in the network when the users download program or use the e-mail, accidentally carry out these special procedures. This procedure generally Records user information and sends it to the Internet or temporarily stands in hard drive, or has the function of directly access password of memory or disk, such as: B0, Net spy such as Trojans. Through the above measures, the password, ie, private key is stolen, furthermore, results in the meaninglessness of entire PKI authentication system.

III. THE ANALYSE TO THE BIOMETRIC IDENTIFICATION

Biometric identification[5] mainly refers to the authentication technology according to human's biometric characteristics. Biometric characteristic usually is unique (different with others), it can be measured or can be automatically identified and verified. The core of biometric identification is how to obtain these biological characteristics, convert them into digital information and store them in a computer, then use a reliable matching algorithm to complete the process of verification and personal identification. The common biometric identification methods are like fingerprint、iris、face、voice print、hand-written signatures.

Logically speaking, the Biometric identification can be divided into Registration modules and Identity Module[6]. In the Registration stage, the legitimate user's biometric characteristics are scanned by the sensor firstly, and turn into the digital descriptions of the characteristics. In order to speed up the matching and reduce storage requirements, the digital descriptions are further processed by the feature extraction procedure and turn into the compressed digital description, known as templates. Biometric template can be deposited into a common database system or magnetic cards or smart cards portable for the individuals.

In the recognition stage, the sensor captures the user's biometric characteristic and converts them into digital format. The characteristic are further processed by feature extraction procedure to generate the same format with the template description when the feature extraction results are transmitted to the feature matching process. The comparison between the templates determine

whether it is the identity of legitimate users. The two stages can be shown as Fig. 2.

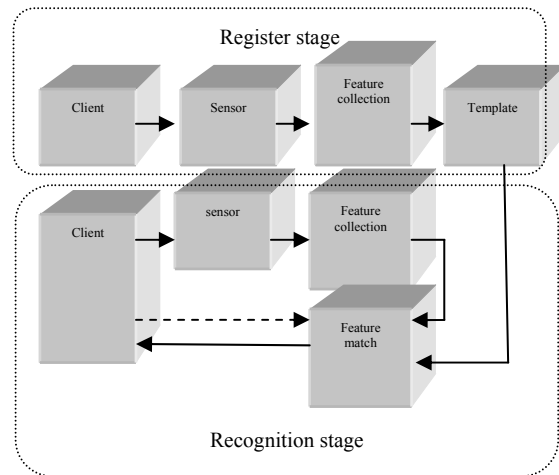


Figure 2. The system of Biometric identification

The system can be made with reference to Mambo's agent signature algorithm.

System parameters are as follows:

- p for large prime numbers,
- q is a prime factor of p - 1,
- $g \in \mathbb{Z}^* p, gq = 1 \pmod p$

A. Registration

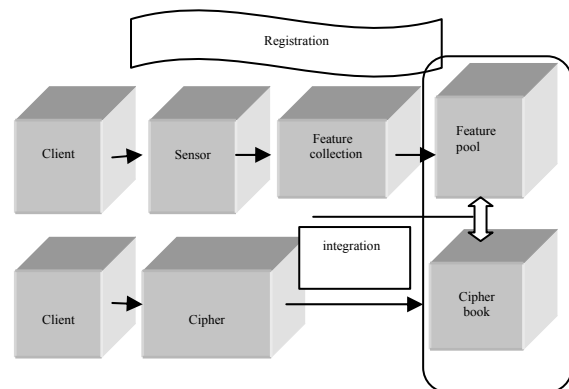


Figure 3. The system of Registration

The user Center registers in register center. RA authenticate users. After authentication, CA preserves the biometric features (such as finger print) and the cipher book provided by user. They can be used after user authentication, also can be used to prevent repudiation. Meanwhile the user's private key for signature is also generated in the card.

The cards randomly selected $SA \in \mathbb{Z}_{q-1} \setminus \{0\}$ for the user smart card key.

Calculated $SA \equiv g SA \pmod p, FA \equiv f A \pmod p$

The user's key for $\delta \equiv (fA + SA SA) \pmod q$

The corresponding public key for verification: c

Save the private key and the smart card to ensure that private information will not be read out. In order to verify the public key, CA approach for the user digital

certificate, which contains the public key information VA.

B. Application and verification

Just as Fig.3 shown, first the visitor must use the sensor with biometric identification. After the card reader collects digital descriptions, It transmit them to feature extraction module, further transmit to the smart card to carry out the logic match and feature match. If both match, visitor have the qualification to visit the material.

Smart card can calculate fA and $SA \equiv g SA \pmod p$ and use the signature key $\delta \equiv (fA + SA) \pmod q$, make use of signature key and DSS signature algorithm for messages signature. After the output of signature information, signature key was destroyed. If the key did not match several times, smart card is locked. Other users can use user A's digital certificate to verify public key. the $SA \equiv g SA \pmod p$, Also Other users can use the user A's digital certificate to verify the public key to verify the signature. Verification process with the use of standards is same to the standard DSS algorithm.

C. Change and write-off

If the user's smart card is lost, he can change the cipher book of private key in the CA center. and if the user no longer need digital certificates, after verified the CA Center write off the preserved feature information and cipher book.

Biometric identification based on the human biometric characteristics in real world. It can effectively avoid the problems of key theft from network. But it is too easy to be imitated by the others in real world. moreover every method of biometrics identification have their pros and cons ,for example ,the common and convenient methods used in PC , i.e. fingerprint 、voiceprint 、hand signature ,their benefits and defect can be shown as Table I .

TABLE I.

THE BENEFITS AND DEFECTS OF BIOMETRIC IDENTIFICATION

TYPE	Benefits	Defects
Finger print	Without interference; low Error rate ; capacity to record deterrent documents of fraud	Wear finger; sense of privacy violations
Voice print	Voice can be easily accepted for public as a unique identifier ; hands-free environment; Receiving less prone unauthorized access	difficult for computer systems to analyze voice system; Voice changes with emotional control; Acceptable problem; High complexity; System is the lack of capacity of the distinction between real identification and pre-recorded voice
Hand written Signatu re Analys is	Quick and easy to use; Any pen to write down clear lines can be used; Easy integration into existing equipment	Performance and reliability is relatively low; Laptop users may have portability questions.

IV. THE INTEGRATION MEASURES

From Fig.3, the general process of PKI integration system ,we can see that the most important part of the system is the integration between the “feature pool “and the “cipher book” and the integration ’s chief aim is to compensate the traditional private key ’s shortage and keep out the threat for the whole system from the loophole of private key.

We can generalize the measure of integration between the biometric and cipher book into following three types .

A. Integration between Biometric identification and ordinary password

TABLE II.

THE DESIGN OF INTEGRATION FOR THE BANK ATM KEYBOARD

Index finger	Middle finger	Ring finger
1	2	3
4	5	6
7	8	9
0	.	00

Take the password keyboard¹ of Bank ATM machine as example. Assumed that the password was 200905, then entered the correct password in the figure at the same time, The correspondent Fingerprints are required to input: middle finger(2)、index finger (0) 、 index finger (0) ring finger (9)、index finger (0) 、 middle finger (5) ,Shown as Table II .

Take the computer keyboard as another example . The use of right hand and left hand can also reflect the integration between the finger prints and the passwords as Table III ²shown.

TABLE III.

THE DESIGN OF INTEGRATION FOR THE PC KEYBOARD

Left hand					Right hand				
⑤	⑤	④	③	②	②	③	④	⑤	⑤
1	2	3	4	5	6	7	8	9	0
Q	W	E	R	T	Y	U	I	O	P
A	S	D	F	G	H	J	K	L	
Z	X	C	V	B	N	M			

Thus we can conclude that the recognition stage includes two match parts ,one is password match ,the other is finger print match just as Fig.4 shown.

1 Footnote : with reference to the ATM keyboard of China bank
 2 Footnote: ②、③、④、⑤ refer to the fingerprints of index finger 、 middle finger 、 ring finger、 little finger respectively

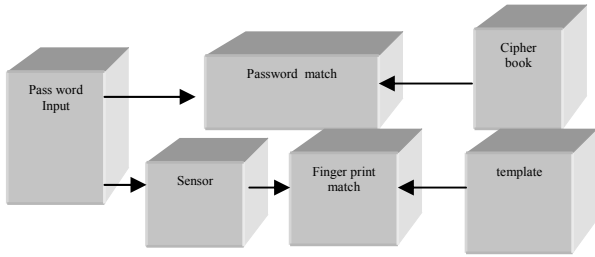


Figure 4. The logic match and feature match of the integration system

B. Integration with biometric identification and Non-duplicate password

Biometric can also integrate with non-duplicate password, took the voice print for example, voice print [7] can be either random voice or special voice according to the text. As we know, non-duplicate password [8] is produced from cipher book at random, while it requires the client answer with the right password and correspondent voiceprint just as Fig. 5 shown.

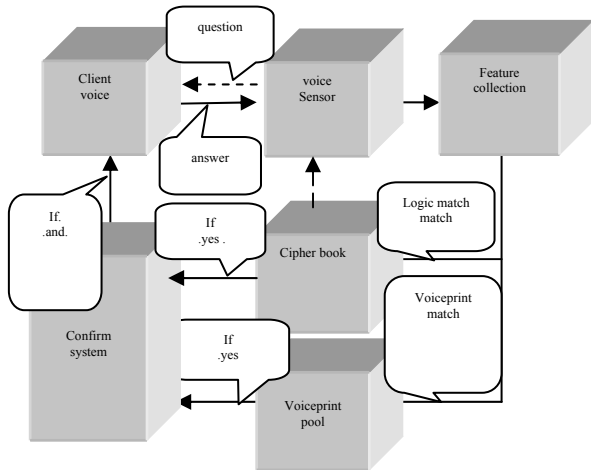


Figure 5. The process that voice print integrates with the non-duplicate password

C. Integration between two or more biometric identification methods

Biometric technology greatly resolves passwords forget and identity theft problems[9]. As more and more electronic transactions are brought out, the protection demand of these transactions related to private and sensitive information is increasing. Series of biometric identification technology are sure to be used in the field of security as the mainstream strength [10]. It is worth noticing that there is no competition between the biometric technology, not even a kind of biometric technology game over other technologies. Various of biometric identification technology form cooperation projects. Two or more biometric identification methods [11] integrated in a smart card to be use in the identification can be more powerful, and it was verified that Some measures had been realized in some countries. For example If the authentication system of the gate, we can choose fingerprint and face information of the smart card to use in PKI authentication, Just as Fig. 6 shown.

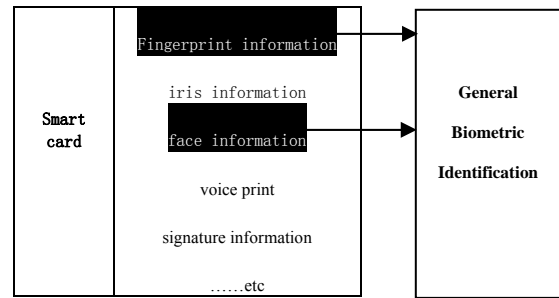


Figure 6. General Biometric Identification of two or more methods

V. THE COMMON PRINCIPLE AND PROCESS

Those above designs and measures of integration must be realized through the rapid development of computer and network, also the following principle and processed are in need.

Step 1: Before design the PKI system, list all the threats the system may encounter from the network and the real world through the method of brainstorming.

Step 2: In accordance with the encryption needs and the threats' feature, select suitable biometric characteristic for the preparation of integration with non-symmetric key technology;

Step 3: Design the PKI authentication system based on the integration of biometric identification and non-symmetric key technology.

Step 4: Verification and amendment

VI. SUMMARY

Through the biometric feature match and password logic match, or more than two biometric feature matches, which assembled the advantage of Biometric and non-symmetric key technology, The PKI authentication lower the possibility of private loss or invalidity, thus guarantee high lever of security for the E-commerce.

REFERENCES

- [1] FAN Jie, JIA Wei, ZHAOWei-dong, The Application of PKI Technology in E-commerce security and its security analysis, SCI-tech Information development and Economy, 2008, volume(18):119-120.
- [2] TAN Xia, Data encryption techniques of e-commerce security, Science and Technology Information, 2008(11):pp75.
- [3] YANQiang, HUTao, LVTingjie, e-commerce security [M] Machinery Industry Press, 2007(5):pp75.
- [4] FENG Xiao-ling edit, E-commerce security [M] Foreign Economic and Trade University Press, 2008(3):29-30.
- [5] QIMing, E-commerce security and encode [M] High education press :pp116-138.
- [6] LIU Pei-Shun, WANG Jian-bo, HeDake, PKI authentication system combining with Fingerprint, computer Engineering, 2005(3):pp59-60.
- [7] Wang, CHEN Junlong, ZHANG Hongxian, based on the audio than the voiceprint recognition technology, Foshan Institute of Science and Technology (Natural Science Edition) Vol.26 No.4 :pp1-5.

- [8] FENG Xiao-ling ,editor, E-commerce security, Foreign Economic and Trade University Press, March ,2008.
- [9] XI Xian-ming, JU Chengdong, LIU Kewen, e-commerce security and the law ,January, 2009.
- [10] Ping Zhong, A modern e-commerce security strategy ,mall modernization, Total section 559 :pp67-68,December 2008.
- [11] Yi Jing, PKI security in e-commerce applications ,entrepreneurs world • theory version ,:pp69-7,Apirl,2008.