Using Multifactor Authentication for Secure Mobile Transaction

P. G. V. Suresh Kumar

Associate Professor, Department of IT & SC, AAiT, Addis Ababa University
Addis Ababa, Ethiopia

Abstract *--- Mobile device has successfully replaced traditional telephone to become the most popular wireless communication tools. Mobile devices provide various services fulfill almost all the user requirements as an effective communication and information delivering services. So there is a demand to communicate or exchange confidential information in a secure environment. In this paper, we introduce a security enhancement based multifactor authentication for secure mobile transaction that compromises cost, simplicity, security and performance of transaction. This proposal presents a biometrics authentication system as face recognition technology, a Public Key Infrastructure (PKI) such as an X.509 certificate both are used in the mobile device which help the mobile transaction.*

Keywords — *Public Key Infrastructure (PKI), Biometric, X.509 certificate, mobile device.*

I. INTRODUCTION

Mobile device servicing is having great influence in daily life but unfortunately most of the communication is insecure. The mobile devices can be accessed by other user in the case of mobile devices sharing or lost. There exist today three strong authentication that are something that you know (PIN, password), something that you have (smart card, authentication token) and something that characterizes you (biometric). Since Public Key Infrastructure (PKI) and biometric combine are a proven solution for secure communication encryption and authentication. These solutions bring sufficient protection to the users. There is possibility of losing the private key to the public when mobile device is lost so biometric will help in verification process for retrieving PKI certificate to overcome these issues. Public Key Infrastructure (PKI) which using pairing of key, for secure communication encryption and Biometric which using user authentication, for secure communication authentication. The key pair generation and distribution are performed by the Certificate Authority (CA). An authentication factor is a piece of information used to authenticate or verify a person's identity for security purpose. Multifactor authentication often a combination of two or three technique is used. PKI will provide the non-repudiation which is the concept of ensuring a party in a dispute cannot repudiate or refute the validity of a statement or contract. The most common authentication scheme today is based on passwords. The use of passwords as a means of authentication is not strong enough for services that require added security especially mobile device application, like e-commerce, online banking etc. Stronger authentications are required. In this paper, multifactor authentication service is proposed. If the mobile device was lost or stolen, the mobile user should inform() to expire key, but if the mobile user didn't inform about the lost or stolen mobile device, the application in most cases in which biometric technique in not used will accept only trails of PIN or password and after fourth trail, it will lock the application and the mobile user should go again through the registration process to renew the key but security breach if any unauthorized user guess and open the application in three trails of PIN/password so biometric techniques which we will propose in this paper and show in how to biometric technique help these type of security breaches. The demand for secure mobile transaction will become increasingly important because too many applications have been built for mobile devices. Besides that, the PKI and biometric technology is easy to understand and accept by public.

II. BIOMETRIC AUTHENTICATION TECHNIQUE

Biometric authentication uses the data taken from measurements of a person's body such as fingerprints, faces, irises, retinal patterns, palm prints, voice prints, hand-written signatures and so on to identify individuals. Such information is unique to the individual and remains throughout the life. In biometric technique, biometric data that is to be used for reference in comparison called as template data is registered in advance in the same way as when passwords are used. In the authentication processing, another biometric data that was input from a sensor is compared with the pre registered template data and calculated and matching. This matching helps for deciding whether this person is the authorized person or not. It is necessary to understand the recognition accuracy and incorporate it into the mobile device ECOM (The Electronic Commerce Promotion Council of Japan) proposed six kinds of evaluation Criteria,

which include resistance to attack. These standards have been proposed as requirements for personal authentication by means of biometrics. In this paper, our system focuses on these evaluation criteria Threat countermeasures, Accuracy of authentication and Ease of use. Using statistical or pattern- recognition techniques, biometric verification systems claim to discriminate between the performance of a given individual and the rest of the population. Because biometric data are real-world data and are somewhat variable, all biometric tests are prone to two kinds of error - false acceptance and false rejection. The lower threshold for false rejection (i.e. the higher the probability of false rejection), the higher the threshold for false acceptance, and vice-versa. The equal error rate is therefore the key figure for evaluation of biometric authentication mechanisms; most biometric techniques are now subject to equal error rates around 1%, since the meaning of an error rate is entirely dependent on the set of data used to procure it. While it is clear that the error rates of biometric techniques could never approach those of the PKI system, it is essential to remember that the domain of proof is not the same, in that biometrics purports to provide evidence of real-world states of affairs. For example, ordinary visual recognition is assumed to be reliable, but mathematical proofs of its reliability would be very difficult to construct but now a days all mobile devices are inbuilt of these types of features. Both types of technique employ to establish the link to the transaction. It is accepted that if such techniques are used, then the integrity of this link can be mathematically proved with a very high degree of probability. The degree of probability is itself demonstrable mathematically. The mobile identifies its owner through face recognition and offline/online PIN/password necessary to activate the certificate during the mobile transaction process. So if the mobile is stolen or lost the main factor of biometric technique will not start the mobile application process.

III. PUBLIC-KEY ENCRYPTION TECHNOLOGY AND X.509 CERTIFICATE

Public-key encryption uses an asymmetrical encryption key pair. An encryption uses one key of the pair, and decryption use the other key of the pair. Each user is issued a pair of keys. One key of the pair is called the public key which is known by everyone and the other key called the private key which is kept secret. When used for encryption, the data to be sent to another party is encrypted by using the public key of the recipient and then transmitted to that party. The receiver then uses their own private key to decrypt the data when it is received Fig. 1.

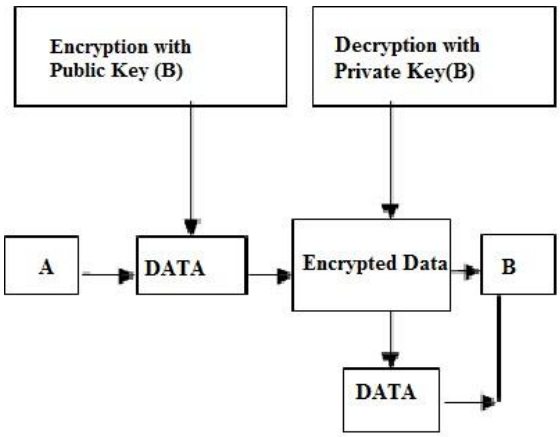

Fig. 1: Encryption/Decryption Process

If the secrecy of the private key is maintained, the secrecy of the data is guaranteed. When used for digital signing, the data that is to be signed is first compressed by using a unidirectional and collision-free conversion function that is called a hash function. The signer then sends the data encrypted with the signer's own private key together with the original data. The receiver uses the sender's public key to decrypt the encrypted data, compresses the original data with the hash function, and checks for consistency in the hash values. This process can validate the owner's public key without corrupting the signed data.

The standardized X.509 certificate is the ISO/IEC/ITU standard form of the digital signature used to guarantee the integrity of this public key An X.509 certificate was standardized as an authentication function in the X.500 directory service.

We built our authentication system according to the X.509 certificate, because our system will be used widely in mobile environments as mobile commerce. The structure of an X.509v3 digital certificate is as follows: certificate{Version, Serial Number, Algorithm ID, Issuer, validity (Not before, Not after), Subject, Subject Public key Info (Public Key Algorithm, Subject Public key), Issuer Unique Identifier, Subject Unique Identifier, Extensions}, Certificate Signature Algorithm, Certificate Signature. In the X.509 system, a trusted party issues a certificate binding a public key to a particular distinguished name. X.509 also includes standards for certificate revocation list implementations. The IETF-approved way of checking a certificate's validity is the online certificate status protocol. There are lots of risks to implement PKI technique only in the mobile device to do the mobile transactions such as who is using my key? How secure is the verifying mobile device? How secure are the certificate practices?

IV. MULTIFACTOR AUTHENTICATION SYSTEM

A multifactor authentication that employs a

Combination of public-key encryption technology and biometric authentication technology is shown in Fig. 02.

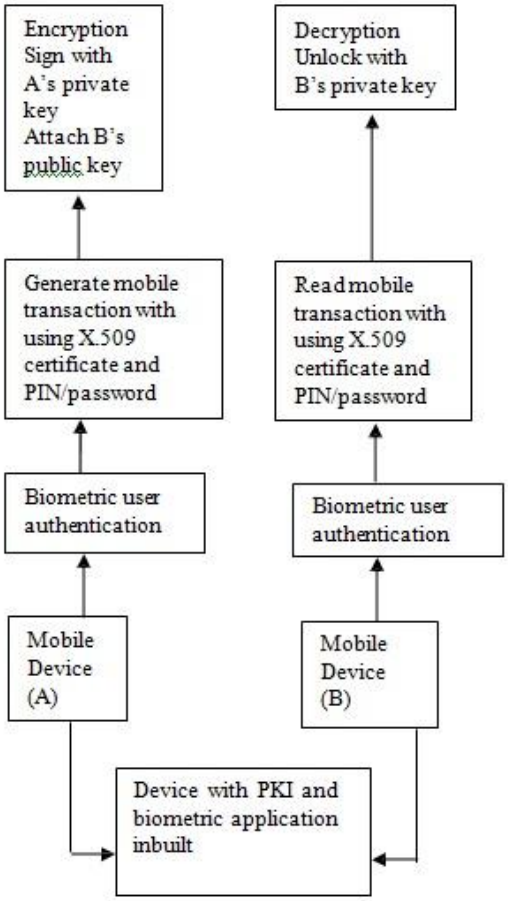

Fig. 2: Multifactor authentication technique in mobile device

We proceed with some assumptions to make our system simpler and easy to use.

- Mobile device is assumed to have good quality of camera inbuilt to detect face easily.
- Mobile device has enough inbuilt memory to store the template data of biometric and X.509 certificate and also other services of the own application.

One time registration process: The authorized user registered him by using face recognition technique on its mobile device and this template is kept on the same mobile device.

Matching process: The process matches the biometric face data of a user inputted to the mobile device and a template which was already stored on that mobile device.

Deciding process: The decision for grant to access the mobile device depends on the match successes or fail. That is the biometric data corresponds to the template which leads to unlock the mobile device.

Multifactor authentication process: The user can get the certificate from the trusted party after one time registered process is completed.

Step 1: The user logon to the mobile device providing face recognition technique.

Step 2: Matching and deciding process will go on depending upon providing match is success or fail. This shows the user has authenticate or not.

Step 3: The user can now use the certificate which was already requested to get from the trusted authority after providing PIN/password to access the certificate which leads the multifactor authentication system.

Our multifactor authentication system provides authentication, confidentiality, integrity, non-repudiation security mechanism. And also to prevent social engineering technique since attacker can get the information about PIN/password of the certificate but it can not biometric information .

V. Conclusion

It is impossible for an unauthorized person to alter the template or the PIN/password and the matching process. The authentication by face recognition is possible on the mobile device which has sufficient memory and as well as good pixel camera inbuilt. The mobile device authenticates without the network since all authentication process done on the mobile device itself therefore improves ease of operation and reduces authentication time. Since face recognition and X.509 certificate of PKI technology with PIN/password are combined and make multifactor authentication system to guarantee the validity of the template.

ACKNOWLEDGEMENT

We would like to convey our gratitude to Sri. P. Bhaskara Rao, Retd. Teacher, India, Prof. Tyaga Raju, Nune Srinivas, faculty of SECE, Mrs. Pendem Padmaja, India, a special thanks to Mr. P.V. Subrahmanyeswara Rao, Miss Ramya Krishna and Daniel Abea Head ITSC under School of ITSC in AAiT Addis ababa University, Ethiopia befor their technical support to realize the this proposal discussed in this paper.

References

[1] Special Issue on Automated Biometric Systems, Proc. of the IEEE, Vol. 85, No. 9 (1997).

[2] A. Jain et al., eds.: BIOMETRICS Personal Identification in Networked Society, Kluwer Academic Publishers (1999).

[3] ECOM (The Electronic Commerce Promotion Council

of Japan) Personal Authentication Technology Study WG: Standards for Evaluation of Personal Authentication (First Ed.), ECOM Report, H9- WG06, http: //www. ecom. or. jp/about wg/wg06/h9doc/wg06-list.htm (1998).

[4] W. Ford, et al: Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Prentice Hall (1997).

[5] C. Ellison and B. Schneier, Ten risks of PKI, Computer security journal, Vol. 16, No. 1 (2000).