Non-Password Remote User Authentication Based on Biometric Technology

Rupali R. Dudhagi
Computer Science and Engg.
Asifia college of Engineering
Hyderabad, India

Vijayalaxmi L Udchan
Electronics and Telecommunication
Terna college of Engineering,Nerul,
Mumbai, India

***Abstract*—Unique identification of an individual is primary objective of web based applications.Password based remote user authentication using smart card are vulnerable to varoius attacks such as password guessing attack, ID-theft,stolen verifier attack.In this paper we present a Non-password remote user authentication which is based on biometric verification to achieve security and efficiency requirements.This scheme is secure against reply attack,imersonation attack,stolen smart card attacks and forgery attack.**

Keywords— authentication, smart card, biometrics, hash function,public key cryptography

I. INTRODUCTION

In 1981, Lamport [1] proposed a remote password authentication scheme that could authenticate remote users over an insecure channel.Lamport's scheme needs to store password table which makes Lamport scheme vulnerable to stolen –verifier attack. In 2000, Hwang and Li [3] proposed a new remote user authentication scheme using smart cards based on ElGamal's [4] cryptosystem. Hwang and Li's scheme only has to maintain a secret key without storing a password table in the system, but this scheme could not withstand masquerade attack. By using smart Cards ,there are several advantages over simple password based system.In smart card based remote user authentication system,a legal user login to the remote server with his/her unique identity by using smart card.Thus stolen verifier attack can be resisted.

Traditional User authentication scheme are categorised into Password based remote user authentication and Cryptographic key based remote user authentication. But,with the development of computer technology,peoples biometrics information can be used to convince their identities.Biometrics is an automated system of recognizing a person based on the person's physical or behavioral Characteristics. Biometrics are sorted into physiological(fingerprint,face iris,palm prints and hand geometry etc),Behavioral (signature,voice and key strokes etc) classes.A system used for biometric matching is called a Biometric System.The matching between one live record and one known stored record is called Aunthetication.Biometric based aunthentication system have many advantages over password based aunthetication system as follows:

- The personal biometric information can not be forgotten or easily gussed
- The personal biometric information is impossible to forge or distribute.
- The personal biometric information is hard to copy and share.

The Lee –Ryu –Yoo scheme[2] was also based on the ElGamal's public key crypto-system with two secret keys and password.The Lee-Ryu-Yoo scheme added more security by verifying the smart card owner's fingerprint.

In this paper we propose a Non-password remote user aunthetication scheme based on biometric technology and used public key cryptography.

The remainder of this paper is organized as follows.Section 2 shows the prposed scheme step by step.In section 3,we provide the relevant security analysis and concluded in section 4.

II. PROPOSED SCHEME

In this section ,we introduce detailed steps of the proposed system. In this proposed scheme we assumed public key and private keys of server are generated while registering the registration center using one of the public key cryptography. The proposed system consists of three phases:registration phase ,login phase,authentication phase.The notations used throughout this paper are as follows :

U	the user
S	the server
R	the registration center
ID	the identty of user U
B	the biometric information of user U
h(.)	a one-way hash function
$\oplus$	bitwise XOR operation
T	the timestamp
PR_s	the private key of server
PU_s	the public key of server
r	the random number selected by the registration centre R

A. Registration Phase

In this phase,the user U initially registers with the trusted registration center as follows-

1. First the user sends his /her identity ID and the related biometrics B to the registration center R over secure channel.

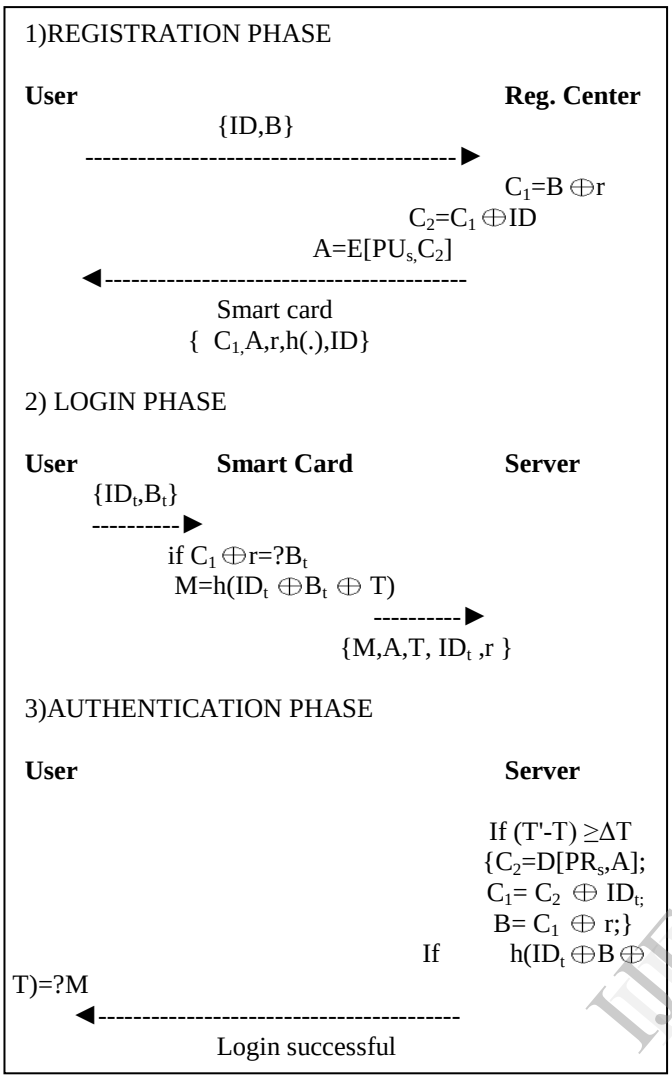

Figure 1 Proposed scheme

2. After receiving user ID and B, the registration center R computes
$C_1=B \oplus r$,$C_2=C_1 \oplus ID$,
$A=Encode[PU_s,C_2]$

Where r is random unique to R and ciphertext A of C_2 is generated using public key of server and then R stores the data { C_1,A ,r ,h(.), ID}into a smart card and issues to U.

B. Login Phase

This phase is invoked whenever the user U asks service from server S

1. The user U inserts his or her smart card into card reader and inputs his or her identity ID_t and the personal biometrics B_t at time t.
2. The system checks whether the format of ID is correct or not .If the format is incorrect,the system rejects request.
3. The smart card checks $C_1 \oplus r=?B_t$ to verify the user U's biometrics on the specific device.If it holds,U passes the biometrics verification;the scheme is aborted.
4. The smart card computes $M=h(ID_t \oplus B_t \oplus T)$ where T is the current timestamp of the login device.
5. Next smart card sends message {M,A,T, ID_t ,r } to the server S.

C. Authentication Phase

After transmission delay,the server receives the login message from the smart card of user at T', the server S perform

1. If (T'-T) ≥ΔT, where ΔT denotes the expected valid time interval for transmission delay, the server rejects the login request.
2. Decodes the A using own private key PR_s,it gets $C_2=Decode[PR_s,A]$;
3. Computes $C_1= C_2 \oplus ID_t$;
4. Computes $B= C_1 \oplus r$;
5. Checks $h(ID_t \oplus B \oplus T)=?M$ if holds S confirms the identity of U;otherwise rejects the user's login request.

III. SECURITY ANALYSIS

In this section, security analysis of this scheme is summarized.The proposed scheme is designed using public key cryptography,XOR operation and one hash function which can withstand the possible well known attacks as follows-

1. The proposed scheme is based on public key cryptography and biometrics verification in registration phase.It's difficult for the intruder to calculate private key for decoding A.It's also difficult for the intruder to obtain public key ,user ID and his/her biometrics simultaneously to generate A.
2. Replay attack can be prevented by checking time stamp at Step 2 in the authentication phase. An intruder may try to modify T to achieve the replay attack. It does not work unless he/she also modifies M to a correct value.
3. In case the intruder can wangle the legal user's smart card, he/she still cannot pass the biometrics verification in login phase.Unfortunately, it is obvious that intruder can not pass the ver ification $C_1 \oplus r=?B_t$,so that proposed scheme can withstand such a stolen smart card attack.
4. In practice,it is likely that the user U_i uses the same ID to access several servers for his/her convenience.Even If an insider of a remote system obtains ID,a remote system does not maintain any verifier table through which a dishonest party can steal the user login data.

Thus the proposed scheme can resist the replay attacks,stolen smart card attacks,guessing attacks,insider attacks,forgery attacks.

IV. CONCLUSION

In this paper,we proposed non-password remote user authentication scheme which uses biometric technology.The proposed scheme need cost two one-way hash function.The performance of our system is much cheaper than the hash based system since the implementaion uses public and privte

key ,random number,xor operation and less number of hash functionThis scheme is more practical with biometric technlogies.In addition ,proposed scheme can withstand to some attacks.Therefore proposed scheme is actually secure and practical for real network applications such as digital library,online exams and mobile applications.

REFERENCES

[1] L. Lamport, "Password authentication with insecure communication,"*Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1993

[2] K. Lee, S.R. Ryu, K.Y. Yoo, Fingerprint-based remote user authentication scheme using smart cards, Electronics Letters 38 (12) (2002 June) 554 – 555.

[3] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000 February) 28 – 30.

[4] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Informa-tion Theory IT-31 (4) (1985 July) 469 – 472.

[5] A. K. Awasthi, and S. Lal, "A remote user authentication scheme using smart cards with Forward Secrecy," IEEE Transactions on Consumer Electronics, vol.49, no.4, pp.1246-1248, Nov. 2003.

[6] T. Hwang, Y. Chen, C.S. Laih, Non-interactive password authentications without password tables, IEEE Region 10 Con-ference on Computer and Communication Systems, IEEE Computer Society, 1990 (September), pp. 429 – 431.

[7] N.-Y. Lee and Y.-C. Chiu. Improved remote authentication scheme with smart card. Computer Standards and Interfaces, 27(2):177–180, 2005.

[8] C-H Lin,Y-Y Lai "A flexible biometrics remotebuser authentication scheme" Computer Standards and Interfaces, 27(2004) 19–23.

[9] C-L Chen,Lin,Wang,Y-L chen ,An Improvement on Hsiang and Shih's Remote User Authentication Scheme Using Smart Cards IEEE Computer Society 2011,53-57