Improvement of Li-Hwang's Biometrics-based Remote User Authentication Scheme using Smart Cards

CHENG-CHI LEE
Department of Library and Information Science
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City, Taipei County 24205
Taiwan, R.O.C.
And Department of Photonics & Communication Engineering
Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung
Taiwan, R.O.C.
cclee@mail.fju.edu.tw

RUI-XIANG CHANG
Department of Photonics & Communication Engineering
Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung
Taiwan, R.O.C.
l123743151@yahoo.com.tw

LUNG ALBERT CHEN
Department of Multimedia Information Science and Applications
Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung
Taiwan, R.O.C.
achen@asia.edu.tw

Abstract: - Recently, Li and Hwang proposed an efficient biometrics-based remote user authentication scheme without storing the password tables. Their scheme uses random numbers to solve the problem of synchronized clocks. It also enables the user to freely choose or change their passwords. At the same time, they claimed that their scheme provides security, reliability and efficiency. However, we found that Li and Hwang's scheme is vulnerable to denial of service attacks. Therefore, in this paper we propose an improved scheme to solve this weakness.

Key-Words: - User authentication, password, biometrics, smart cards, security, cryptography.

1 Introduction

Password authentication is one of the mechanisms that have been widely used to authenticate a legitimate user. If the remote users want to login to a remote server for its resources and services, they must be authenticated by the remote server first. In 1981, Lamport [9] first proposed a remote user authentication scheme by using a one-way hash chain and password table. However, if the password table is stolen by an adversary, all of the remote users must change passwords and/or re-register. Furthermore, it is inconvenient for the server to maintain the password tables, because the size of the password tables is determined by the number of users. Later on, in 1990, Hwang et al. [3] proposed a non-interactive password authentication scheme using smart cards instead of maintaining the verification table. In 2000, Hwang and Li [4] proposed a remote user authentication scheme using smart cards based on ElGamal's public key cryptosystem. Unfortunately, their scheme was found to be vulnerable to impersonation attacks and heavy on computation cost. Many remote user authentication schemes have subsequently been proposed for the client-server environment [4, 5, 7, 12, 13, 14]. However, these schemes are all based on the password or the cryptographic keys.

It is well known that simple passwords are vulnerable to password guessing attacks [2]. This is due to the fact that people tend to use easy-to-remember passwords. In general, the cryptographic keys are long and difficult to memorize. The remote server maintains the

cryptographic keys in a secure place and uses it to verify the remote users. The security of the place storing the cryptographic keys has then become an issue. It will be a disaster if the cryptographic keys are lost or stolen. Biometrics keys are proposed to overcome this issue, which can be used for user authentication and as cryptographic keys for cryptographic applications as well. A smart card is used to store the hash value of the biometrics keys and is used for verification purpose. Biometric data contains unique personal information, such as fingerprint, face, voice, and/or retina scan, … etc.

In 2002, Lee et al. [10] proposed a fingerprint-based remote user authentication scheme adopting El-Gamal public key cryptosystem using smart cards. However, Lin and Lai [11] pointed out that Lee et al.'s fingerprint-based remote user authentication scheme is vulnerable to masquerade attack. Then Lin and Lai proposed a flexible biometrics remote user authentication scheme. Unfortunately, Khan and Zhang [6] showed that Lin and Lai's flexible biometrics remote user authentication scheme is vulnerable to the server spoofing attack and cannot provide mutual authentication. Then they proposed improved scheme to address these weaknesses. Recently, Li and Hwang [8] proposed an efficient biometrics-based remote user authentication scheme without storing the password tables. Their scheme uses random numbers to solve synchronized clocks problem and enables the user to freely choose or change their passwords. In the meanwhile, they claimed that their scheme provides security, reliability, and efficiency. However, we found that their scheme is susceptible to the denial of service attack and cannot achieve session key establishment.

Denial-of-Service (DoS) attacks [16] can disrupt the availability of the authentication between the legitimate user and remote server. This would prevent legitimate user from gaining access to the remote server. To launch a DoS attack, the adversary could simply keep on sending fake messages to the remote server. In response, the remote server performs many expensive cryptographic operations, such as modular exponentiations. The remote server resources therefore would be depleted from it's normal operations, and will not be able to respond to the valid requests from legitimate users. Protection against DoS attacks is an essential requirement in the remote user authentication scheme.

In this paper, we propose an improved scheme to overcome these weaknesses. The paper is organized as follows: in Section 2.1, we review Li and Hwang's biometrics-based remote user authentication scheme. The security flaws of Li-Hwang's al.'s scheme is presented in Section 2.2. Section 3 contains our proposed, improved scheme. In Section 4, we discuss the security and the efficiency of our scheme. Finally, the conclusion is in Section 5.

2 Review of Li-Hwang's Scheme

In this section, we brief the Li-Hwang's scheme and show the security weakness of their scheme.

2.1 Li-Hwang's Scheme

In this section, we review Li-Hwang's biometrics-based remote user authentication scheme. Their scheme contains four phases: registration phase, login phase, verification phase, and password change phase. There are three main participants in Li-Hwang's remote user authentication scheme: the user (C_i), the remote server (S_i), and the registration center (R_i). Ri is assumed to be trustworthy in this case. Table 1 lists the notations used in Li-Hwang's scheme.

Table 1. The notations used in Li-Hwang's scheme

Notations	Descriptions
C_i	A client
ID_i	The identity of C_i
PW_i	Password shared between C_i and S_i
S_i	The remote server
R_i	The registration center
B_i	Biometric template of the user
R_C	A random number chosen by the user
R_S	A random number chosen by the server
Xs	The secret key maintained by the server
$h()$	A one-way hash function
$\oplus$	The bitwise XOR operation
$\|\|$	String concatenation operation
$\Rightarrow$	A secure channel
$\rightarrow$	A common channel

2.1.1 Registration Phase

Before the remote user *Ci* wants to access the systems, he/she needs to register with *Ri*. The steps of the registration phase are as follows:

Step R1. $C_i \Rightarrow R_i$: ID_i, PW_i, B_i

C_i first inputs his/her personal biometrics B_i on the specific device and freely chooses his/her identity ID_i and PW_i. Then C_i sends $\{ID_i, PW_i, B_i\}$ to the registration center R_i for registration, through a secure channel.

Step R2. After received these message from C_i, R_i computes

$$f_i = h(B_i), \quad (1)$$

$$r_i = h(PW_i||f_i), \quad (2)$$

$$e_i = h(ID_i||Xs) \oplus h(PW_i||f_i), \quad (3)$$

where *X*s is secret information generated by the server.

Step R3. $R_i \Rightarrow C_i$: ID_i, f_i, e_i, $h(.)$

R_i issues a smart card and sends it to C_i through a secure channel. The smart card contains $\{ID_i, f_i, e_i, h(.)\}$.

2.1.2 Login Phase

After receiving the smart card from R_i, C_i can use it when he/she wants to login S_i. The steps of the login phase are as follows:

Step L1. C_i inserts his/her smart card into a smart card reader and provides the personal biometrics B_i input for the specific device. Then the smart card computes $h(B_i)$ and checks whether $h(B_i)$ is the same as f_i. If they are the same, C_i passes the biometrics verification and continues the login phase. Otherwise the smart card terminates the login request.

Step L2. C_i inputs PW_i, and the smart card computes

$$r'_i = h(PW_i||f_i), \quad (4)$$

$$M_1 = e_i \oplus r'_i = h(ID_i||Xs), \quad (5)$$

$$M_2 = M_1 \oplus R_C, \quad (6)$$

where R_C is a random number generated by the user.

Step L3. $C_i \rightarrow S_i$: ID_i, M_2

Finally, C_i sends the message $\{ID_i, M_2\}$ to the remote server.

2.1.3 Verification Phase

After receiving the login request sent from C_i, S_i performs the following tasks to authenticate the user's login request.

Step V1. After receiving the login request, S_i verifies ID_i and computes

$$M_3 = h(ID_i||Xs), \quad (7)$$

$$M_4 = M_2 \oplus M_3 = R_C, \quad (8)$$

$$M_5 = M_3 \oplus R_S, \quad (9)$$

$$M_6 = h(M_2||M_4), \quad (10)$$

where R_S is a random number generated by the remote server.

Step V2. $S_i \rightarrow C_i$: M_5, M_6

S_i sends the message $\{M_5, M_6\}$ to C_i.

Step V3. After receiving these messages from S_i, C_i computes $h(M_2||R_C)$ and checks whether $h(M_2||R_C)$ is the same as M_6. If they are the same, C_i authenticates S_i successfully. Otherwise C_i terminates this session.

Step V4. C_i computes

$$M_7 = M_5 \oplus M_1 = R_S \text{ and} \quad (11)$$

$$M_8 = h(M_5||M_7). \quad (12)$$

Step V5. $C_i \rightarrow S_i$: M_8

C_i sends the message $\{M_8\}$ to S_i.

Step V6. After receiving the message from C_i, S_i computes $h(M_5||R_S)$ and checks whether $h(M_5||R_S)$ is the same as M_8. If they are the same, S_i authenticates C_i successfully. Otherwise S_i terminates this session.

The login and verification phase of Li-Hwang's scheme are summarized in Fig. 1.

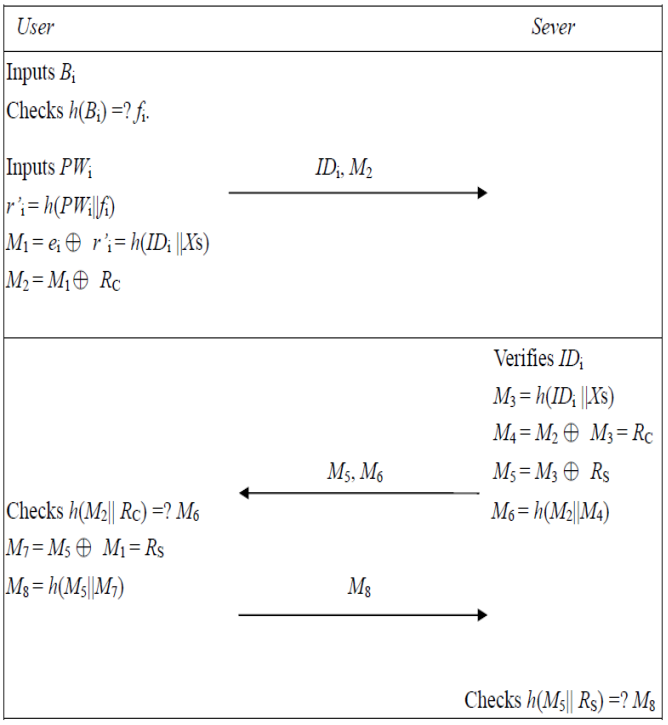

Fig 1. Login and verification phase of Li-Hwang's scheme

2.1.4 Password Change Phase

In this phase, C_i can change his/her password any time when he/she wants. The steps of the password change phase are as follows:

Step P1. C_i inserts his/her smart card into the smart card reader and then inputs his/her biometric template B_i on the specific device.

Step P2. The smart cared computes $h(B_i)$ and checks whether $h(B_i)$ is the same as f_i. If they are the same, C_i passes the biometrics verification. Otherwise the smart card terminates this login request.

Step P3. C_i inputs the old password PW_i and the new password PW_{inew}. Then the smart card computes the following:

$$r'_i = h(PW_i||f_i), \quad (13)$$

$$e'_i = e_i \oplus r'_i = h(ID_i||Xs), \quad (14)$$

$$e''_i = e'_I \oplus h(PW_{inew}||f_i). \quad (15)$$

Step P4. Then the smart card replaces the e_i with e''_i.

2.2 Denial of Service Attack on Li-Hwang's Scheme

In this section, we will demonstrate that Li-Hwang's scheme is vulnerable to a denial of service attack. In the

real world, denial of service attack has increased dramatically in the recent years. A denial of service attack presents when an adversary tries to occupy some resources by making them busy to answer legitimate requests, or to deny legitimate users accessing the remote server. In their scheme, they claimed that their scheme does not store all the random values between the users and remote server. However, any adversary has the ability to perform the denial of service attack, because the remote server only checks the identity of the user in Step V1 and needs to spend many cycles computing necessary information. If the identity of the user is valid, the remote server computes $\{M_3, M_4, M_5, M_6\}$ and responses $\{M_5, M_6\}$ back to the user. Then the user verifies the remote server by checking $h(M_2 || R_C) =? M_6$ and responses $\{M_8\}$ to the remote server. After receiving the message $\{M_8\}$ from the user, the remote server checks $\{M_8\}$ to verify the user. This means that the remote server needs to compute $\{M_3, M_4, M_5, M_6, M_8\}$ to verify the user. It wastes many CPU resources in the remote server.

In general, when a user communicates with the remote server and sends the login requests to the remote server for some resources, an adversary can record the user's login request in Step V1. Because the login message is sent in the form of plaintext through a public network, any user, including the adversary, can intercept the message from the public network. Then an adversary can replay the intercept message $\{ID_i, M_2\}$ to the remote server. The fake login request will be rejected in Step V6, because the remote server chooses a new random number R_S in Step V1 and uses this new random number R_S to verify M_8. However, if an adversary replays a large amount of fake login requests to the remote server, then the remote server needs to compute $\{M_3, M_4, M_5, M_6, M_8\}$ every time, in the verification phase, to verify these fake login requests. Then the remote server's CPU resources will soon be fully loaded. To launch such an attack, a large amount of fake login message is enough to serve the purpose. Under that situation, the remote server is too busy to answer other legitimate requests, and an adversary can perform a denial of service to paralyze Li-Hwang's remote user authentication scheme.

Besides, we found that Li-Hwang's scheme does not provide session key establishment. In verification phase, mutual authentication is achieved between the user and remote server without establishing the session key. Messages are therefore not encrypted and sent between the user and remote server in an unsecure domain. We think that the session key establishment is an essential requirement and the entire remote user authentication should meet this requirement. Therefore, we propose an improved scheme to address the denial of service issue and also achieve the goal of session key establishment. More detail is illustrated in the next section.

3 Our Improved Scheme

In this section, we propose an improvement on Li-Hwang's scheme, which keeps the merits of the original scheme and can survive the denial of service attack; at the same time, it achieves the session key establishment requirement. To defend the denial of service attack in Li-Hwang's scheme, we assume that the remote server needs to verify the user's login request in the early phase. We present our improved scheme in the four phases: registration phase, login phase, verification phase, and password change phase. There are also three main participants in our improved remote user authentication scheme: the user (C_i), the remote server (S_i), and the registration center (R_i). The improved scheme is described as follows.

3.1 Registration Phase

This phase is the same as the Section 2.1.1.

3.2 Login Phase

After receiving the smart card from R_i, C_i can use it when he/she wants to login S_i. The steps of the login phase are as follows:

Step L1. C_i inserts his/her smart card into the smart card reader and then inputs the personal biometrics B_i on the specific device. Then the smart card computes $h(B_i)$ and checks whether $h(B_i)$ is the same as f_i. If they are the same, C_i passes the biometrics verification. Otherwise the smart card terminates this login request.

Step L2. C_i inputs PW_i, and the smart card computes

$$r'_i = h(PW_i || f_i), \quad (16)$$

$$M_1 = e_i \oplus r'_i = h(ID_i || Xs), \quad (17)$$

$$M_2 = M_1 \oplus R_C, \quad (18)$$

$$M_3 = h(R_C), \quad (19)$$

where R_C is a random number generated by the user.

Step L3. $C_i \rightarrow S_i$: ID_i, M_2, M_3

Finally, C_i sends the message $\{ID_i, M_2, M_3\}$ back to the remote server.

3.3 Verification Phase

After receiving the login request sent from C_i, S_i performs the following tasks to authenticate the user's login request. The steps of the verification phase are as follows:

Step V1. After receiving the login request, S_i verifies ID_i and computes

$$M_4 = h(ID_i || Xs), \quad (20)$$

$$M_5 = M_2 \oplus M_4 = R_C, \quad (21)$$

$$M_6 = h(R_C). \quad (22)$$

The remote server checks if M_6 is the same as M_3. If they are the same, the remote server authenticates the user successfully. Otherwise the remote server terminates this session. Once the user is authenticated, the remote server computes

$$M_7 = M_4 \oplus R_S, \quad (23)$$

$$SK = h(R_C \| R_S \| ID_i \| S_i), \quad (24)$$

$$M_8 = h(SK \| M_5), \quad (25)$$

where R_S is a random number generated by the remote server.

Step V2. $S_i \rightarrow C_i$: M_7, M_8

S_i sends the messages $\{M_7, M_8\}$ to C_i.

Step V3. After receiving these messages from S_i, C_i computes

$$M_9 = M_7 \oplus M_1 = R_S, \quad (26)$$

$$SK = h(R_C \| R_S \| ID_i \| S_i), \quad (27)$$

$$M_{10} = h(SK \| R_C). \quad (28)$$

C_i checks if M_{10} is the same as M_8. If they are the same, C_i has successfully authenticated the remote server. Otherwise C_i will terminate the session.

Step V4. C_i computes $M_{11} = h(SK \| M_9)$.

C_i sends the message $\{M_{11}\}$ to S_i.

Step V5. After receiving the message from C_i, S_i computes $M_{12} = h(SK \| R_S)$ and checks whether M_{12} is the same as M_{11}. If they are the same, S_i authenticates C_i successfully. Otherwise S_i terminates this session. After achieving mutual authentication between C_i and S_i, they can use SK to encrypt/decrypt messages for secrecy communication.

The login and verification phases of our improved scheme are summarized in Fig. 2.

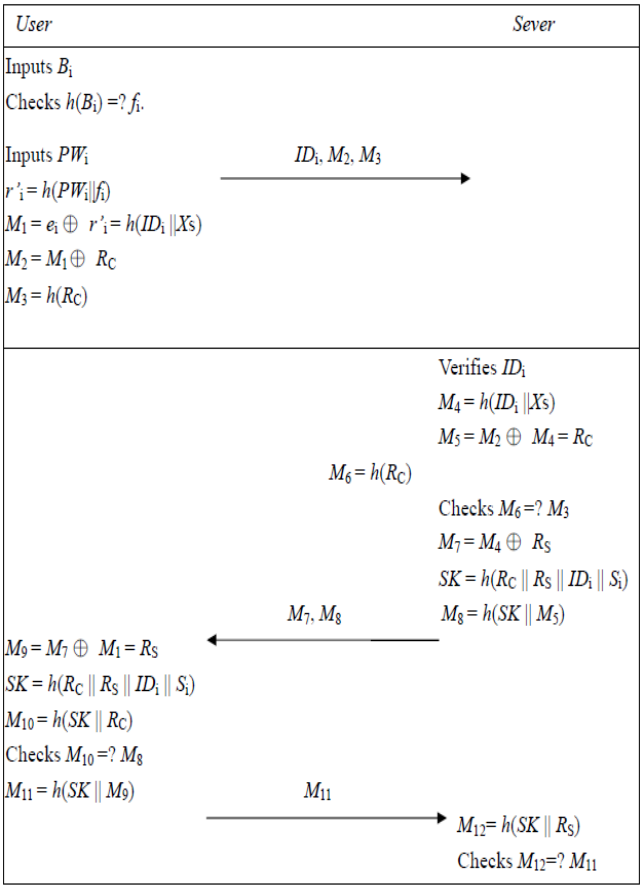

Fig 2. Login and verification phase of our improved scheme

3.4 Password Change Phase

This phase is the same as that in Section 2.1.4.

4 Security Analysis and Comparisons

Li-Hwang's scheme was compared with other schemes in these literatures [1, 6, 11, 12, 15], in terms of security analysis, performance comparisons, and functionality comparisons. Therefore, in this section, we will focus on only the comparison between the enhanced security of our proposed scheme and Li-Hwang's scheme, in terms of functionality and computations costs.

4.1 Security Analysis

In this section, we discuss the security of our improved scheme. We demonstrate that the improved scheme is secure against various attacks and can achieve session key establishment and mutual authentication as well.

4.1.1 Resistance to Impersonation Attacks

Suppose that the adversary wants to masquerade as a legitimate user accessing the remote server. Then he/she needs to send a valid login request to the remote server. However, the adversary has no way to create a valid login request, because he/she cannot compute $M_1 = h(ID_i \| Xs)$ and $M_2 = M_1 \oplus R_C$ without server's secret key Xs. The adversary doesn't know the server's secret key Xs, which is embedded in M_1, and M_1 is a one-way hash function. It can successfully prevent the adversary from performing a masquerade user attack to our improved scheme.

Besides, suppose that the adversary wants to masquerade as a remote server to fool a legitimate user for his/her personal information. Then he/she must response a valid verification request to a legitimate user. If the adversary intercepts the legitimate user's login request $\{ID_i, M_2, M_3\}$ in Step L3, he/she must response a valid authentication request $\{M_7, M_8\}$ to the legitimate user. However, there is no way for the adversary to compute $M_4 = h(ID_i \| Xs)$ in order to obtain $M_5 = M_2 \oplus M_4 = R_C$, since the adversary doesn't know the server's secret key Xs. Neither can the adversary compute $M_7 = M_4 \oplus R_S$, $SK = h(R_C \| R_S \| ID_i \| S_i)$ and $M_8 = h(SK \| M_5)$ and response with a valid authentication request $\{M_7, M_8\}$ to the legitimate user. Therefore, the adversary cannot

impersonation as a remote server to cheat the legitimate user in our improved scheme.

4.1.2 Resistance to Denial of Service Attacks

Usually, the remote user authentication scheme uses a single server to support many legitimate users simultaneously. If the remote server handles too many invalid login requests, or too many computationally expensive cryptographic operations, the resources of the remote server could be exhausted. Then the remote server will not be able to respond to valid requests from legitimate users, and legitimate users cannot employ this server's service. Therefore, protection against denial of service attacks is an essential requirement in the remote user authentication scheme. The adversary could employ some methods to force the remote server to deny the legitimate user's login request. However, it cannot work in our improved scheme, because the remote server can control the amount of incoming login requests in the verification phase. Besides, our improved scheme only uses XOR operations, string concatenation operations and one-way hash functions. The remote server doesn't need to compute many computationally expensive cryptographic operations. Therefore, our improved scheme is more secure against denial of service attacks.

4.1.3 Resistance to Password Guessing Attacks

Password-based authentication scheme is very vulnerable to password guessing attacks, because of the fact that people often use simple or easy to remember passwords carrying low-entropy. In general, the regular password guessing attacks can be categorized into three classes. Sometimes, they are called on-line and off-line password guessing attacks, respectively. Another kind is called undetectable on-line password guessing attack. An on-line password guessing attack is when the adversary verifies his/her guess in an on-line process. If the guess is incorrect, the remote server can detect a failed guess. On the other hand, an off-line password guessing attack is when the adversary intercepts valid message and verifies his/her guess in an off-line process. And an undetectable on-line password guessing attack is when the adversary tries to verify his/her guessed passwords in an on-line process, but the remote server cannot detect a failed guess.

If the adversary wants to perform password guessing attacks to guess user's passwords, it cannot work in our scheme. Because user's password doesn't embed in login message or authentication message, the adversary cannot perform an on-line or off-line password guessing attack. It means that the adversary only obtains user's biometrics value f_i and secret parameter $r_i = h(PW_i||f_i)$ to perform an off-line password guessing attack. However, user's biometrics value f_i and secret parameter r_i are secret storing in the smart card, any user, including illegal ones, cannot obtain those secret parameters. Therefore, our improved scheme is secure against password guessing attacks.

4.1.4 Resistance to Stolen Smart Card Attacks

If the adversary obtains a user's smart card, he/she could employ it to masquerade as a legitimate user to access the remote server for some resources. This attack therefore should be considered in the smart card based scheme. We assume that the adversary has stolen the smart card in some way, and then he/she tries to use it to login to remote user. However, when the adversary inserts the smart card into the smart card reader, he/she must input the personal biometric B_i on the specific device. Since the adversary doesn't know the personal biometric B_i, he/she cannot pass the biometric verification. Even if the adversary passes the biometric verification for whatever reason, he/she still cannot masquerade as the legitimate user to login the remote server. This is because the adversary doesn't have the user's correct password, he/she can only randomly guess the password. Therefore, the improved scheme can withstand the stolen smart card attack.

4.1.5 The Security of Session Key *SK*

In Li-Hwang's scheme, the session key establishment is not provided. Without achieving the session key establishment, it may cause some problems. After mutual authenticating is achieved, the legitimate user communicates with the remote server without using encryption operations. These messages are not encrypted and sent between the legitimate user and the remote server in an unsecure domain. Therefore, our improved scheme provides the session key establishment, to address this security hole. In the later communications, the legitimate user and the remote server can use the established session key *SK* to encrypt all the messages sent between them.

Suppose the adversary tries to obtain the one-time session key *SK* from the intercepted message $\{ID_i, M_2, M_3, M_7, M_8, M_{11}\}$ when these messages are sent between the legitimate user and the remote server. However, the one-time session key $SK = h(R_C \| R_S \| ID_i \| S_i)$, can not be properly generated without the random numbers R_C and R_S from the intercepted messages. To get R_C and R_S, it is of no use for the adversary to intercept the messages $\{ID_i, M_2, M_3, M_7, M_8, M_{11}\}$, because R_C and R_S are secretly embedded in M_2 and M_7, respectively. R_C and R_S are not directly sent in the public channel. The adversary therefore has no way to obtain R_C and R_S to compute *SK*. Therefore, our improved scheme is quite difficult for the adversary to obtain the one-time session key *SK*.

4.2 Performance and Functionality Analysis

Li-Hwang's scheme was compared with other schemes in these literatures [1, 6, 11, 12, 15], in terms of security analysis, performance comparisons, and functionality comparisons. They demonstrated that their scheme is more security, reliability, and efficiency than the previously proposed schemes. Therefore, in this section, we focus on the discussion of some performance issues of our improved scheme and only compare that with Li-Hwang's scheme, in terms of computation cost. We define the notation H as a one-way hashing function. Exclusion-OR operations should be neglect, because the computation costs of exclusion-OR operations are very low. Then we mainly focus on the time complexity of calculating one-way hashing operations. Table 2 shows the comparison of our improved scheme and Li-Hwang's scheme. In Li-Hwang's scheme, the computation costs of login and verification phases are 2H and 5H respectively. In our scheme, the computation costs of login and verification phases are 3H and 9H respectively. Our scheme requires five extra hashing operations. However, Li-Hwang's scheme is vulnerable to denial of service attack and cannot provide session key establishment. Our improved scheme is secure against denial of service attack and can achieve session key establishment. It is worth achieving session key establishment and high security with a marginal cost.

Table 2. Comparisons between our scheme and Li-Hwang's scheme

	Ours	Li-Hwang
Communication costs in registration phase	3H	3H
Communication costs in login phase	3H	2H
Communication costs in verification phase	9H	5H
Mutual authentication	O	O
Session key establishment	O	X
The password is chosen by the user freely	O	O
Prevention of a stolen smart card attack	O	O
Prevention of a denial of service attack	O	X
Prevention of an impersonation attack	O	O

5 Conclusions

In this paper, we demonstrate that Li-Hwang's biometrics-based remote user authentication scheme is vulnerable to denial of service attacks and cannot achieve session keys establishment. If the adversary performs the denial of service attacks in Li-Hwang's scheme, the remote server would perform many computationally expensive cryptographic operations. Then the remote server will not be able to respond to the valid requests from legitimate users. Therefore, we propose an improved scheme to resolve these weaknesses. A security analysis and comparisons shows that the proposed scheme is more secure and practical.

Acknowledge

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 100-2221-E-030-015.

References:

[1] Y. F. Chang, C. C. Chang, and Y. W. Su, A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism, *In Proceedings of the IEEE International Conference on Advanced Information Networking and Applications*, vol. 2, April 2006.

[2] Y. Ding and P. Horster, Undetectable on-line password guessing attacks, ACM SIGOPS Operating Systems Review, vol. 29, no. 4, pp. 77-86, 1995.

[3] T. Hwang, Y. Chen, and C. S. Laih, Non-interactive password authentications without password tables, IEEE Region 10 Conference on Computer and Communication Systems, pp. 429–431, 1990.

[4] M. S. Hwang and L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[5] T. Hwang and W. C. Ku, Reparable key distribution protocols for Internet environments, IEEE Transaction on Consumer Electronics, vol. 43, no. 5, pp. 1947–1949, 1995.

[6] M. K. Khan and J. Zhang, Improving the security of a flexible biometrics remote user authentication scheme, Computer Standards & Interfaces, vol. 29, no. 1, pp. 82-85, 2007.

[7] W. C. Ku and S. M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics, vol. 50, no. 1, pp. 204-207, 2004.

[8] C. T. Li and M. S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1-5, January 2010.

[9] L. Lamport, Password authentication with insecure communication, Communication of ACM, vol. 24, pp. 770-772, 1981.

[10] J. K. Lee, S. R. Ryu, and K. Y. Yoo, Fingerprint-based remote user authentication scheme using smart cards, Electronic Letters, vol. 38, no. 12, pp. 554-555, 2002.

[11] C. H. Lin and Y. Y. Lai, A flexible biometrics remote user authentication scheme, Computer Standards & Interfaces, vol. 27, no. 1, pp. 19-23, 2004.
[12] N. Y. Lee and Y. C. Chiu, Improved remote authentication scheme with smart card, Computer Standards & Interfaces, vol. 27, no. 2, pp. 177-180, 2005.
[13] H. M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics, vol. 46, no. 4, pp. 958-961, 2000.
[14] J. J. Shen, C. W. Lin, and M. S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transaction on Consumer Electronics, vol. 49, no. 2, pp. 414-416, 2003.
[15] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, An improvement of Hwang–Lee–Tang's simple remote user authentication scheme, Computers & Security, vol. 24, no. 1, pp. 50-56, 2005.
[16] R. Zhang and K. Chen, Improvements on the WTLS protocol to avoid denial of service attacks, Computers & Security, vol. 24, no. 5, pp. 76-82, 2005.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he was an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. From 2010, he is now an assistant professor of Library and Information Science, Fu Jen Catholic University. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 60+ articles on the above research fields in international journals.

Rui-Xiang Chang received the B.S. in Photonics and Communication Engineering, Asia University, Taichung, Taiwan, Republic of China, in 2008. He is currently pursuing his master degree in the same University. His current research interests include information security, cryptography, and mobile communications.

Lung Albert Chen is loaded with almost 20 years of solid software industrial experience in the Silicon Valley. As Vice President of Global Operation, Consulting Services & Product Management at BroadVision, he was responsible for delivering more than 50% of the Company Annual Revenue, for the last four years. He was also responsible for driving a new product line of eMerchandising Solution, and delivering every major product releases of the Enterprise Portal & Commerce Solutions. He also managed the CIO Organization, the owner of Corporate Information, Forecast tools, and Global IT Operation as well. He received Corporate Significant Contribution Award in 2008. Prior to that, Dr. Chen was Regional Vice President, Global Professional Services, Asia Pacific & Japan, also at BroadVision. He founded a Consulting Services Organization from scratch and built a new line of business with 150+ consultants, and complete portfolio of Services throughout the region. He received three times President Club Awards. Before joining BroadVision, Dr. Chen worked at Tandem Computer, as a key contributor of the Non-stop SQL Optimization team, conducted Performance Tuning for TPCC, TPCD Benchmark and designed customer benchmarks for major Retail Customers. Prior to that, he worked at IBM Santa Teresa Lab., where he designed and implemented Access Path Algorithms for DB2 parallelism solution. Dr. Chen graduated from National Taiwan University, Electrical Engineering Department. He has a Ph.D. Degree in Computer Science, from University of California, Berkeley. His thesis title is 'Knowledge-based retrieval of information as a process of evidential reasoning', with Dr. Lotfi Zaheh as his advisor.