An Enhanced Remote Login Authentication with Smart Card

Junqing Liu
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China
liujqsjtu@yahoo.com

Jun Sun
Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China
sunjun@cdtv.org.cn

Tianhao Li
Department of Electrical and Computer Engineering
IUPUI
Indianapolis, USA
tianhaolee@yahoo.com

Abstract—**Based on one-way hash function, Sun proposed an efficient remote login authentication protocol with smart card in 2000. However, in 2002, Chien at al. pointed out a deficiency of sun's scheme which only realized unilateral authentication and put forward an efficient and practical solution for remote mutual authentication scheme. But recently, Hsu discussed that this scheme was not secure enough since it was vulnerable to the parallel session attack again. In this paper, we will give an enhanced remote login authentication with smart card, which inherits all the merits of the previous schemes as well as realizes secure mutual authentication without significantly increasing the computational cost[1]**

I. Introduction

With the rapid development of the technology of in the field of information, corporation with the remote sever through network is becoming indispensability. Although network can provide convenience for people, its resource is vulnerable to be illegal access or changed by intruders or illegitimate users due to the insecure transferring network. So, when a user logins a remote sever by network, identity authentication is an important way to guarantee the security of the communication.

In traditional scheme, one user has an identity ID and a password PW . The server stores a verified table like table I in memory in which all the ID and PW of the users are arranged correspondingly. When a user wants to login to the remote server, he must input his ID and PW to the system. Then the system compares the data with the stored data in verified table to decide accepting or denying the login of the user. In this scheme, once the verified table is leaked or attacked, all the PW will be disclosed. Moreover, this scheme can't resist replay attack even if the stored PW is encrypted.

Lamport[1] provided a scheme to resist the replay attack, but it still suffers a risk of a modified verified table. In 2000, Hwang et al.[2] proposed a new remote user authentication scheme using smart card based on ElGamal's cryptosystem, however, Chen et al.[3] gave a cryptanalysis of this scheme an pointed out that a legal user can easily create a valid pair of ID and PW even without knowing the secret key x_s of the system. Moreover, Shen et al.[4] pointed that this scheme can't resist masquerade attack. Recently, Sun[5] proposed an efficient smart card base remote login authentication to improve Hwang's scheme. Awasthi[6] et.al also put forward a remote user authentication scheme with forward secrecy. However, like Chien at al.[7] pointed, these schemes only considered unilateral authentication while ignore the mutual authentication to improve the security of the system further. A mutual authentication scheme is also proposed by Chien at al., but Hsu ointed out that this scheme is vulnerable to the parallel session attack that an intruder without knowing the user's PW

[1] This work was supported by Electronic Development Fund of Ministry of Information Industry of P.R.China.

can masquerade as the legal user by eavesdropping the communication and tampering the message[8].

TABLE Ⅰ

Verified Table for Authentication

User	Identity	Password
U_1	ID_1	PW_1
U_2	ID_2	PW_2
$\vdots$	$\vdots$	$\vdots$
U_n	ID_n	PW_n

In this paper, we will propose an enhanced remote login authentication scheme based on the scheme of Chien at al. In our scheme, users can freely choose or change their PWs. Compared with Chien's scheme, it will not increase the computation significantly. Finally, it provides secure mutual authentication which can withstand the parallel session attack. As for the rest of the paper, in section 2, we will give a brief review of Chien at al's scheme and the parallel session attack on it. The proposed remote login authentication scheme with smart card will be discussed in section 3. Security and the performance of the proposed scheme will be discussed in section 4. Finally, we conclude our scheme in section 5.

II. REVIEW OF CHIEN ET AL'S SCHEME AND PARALLEL SESSION ATTACK

Like most remote authentication scheme, there are registration phase, login phase and authentication phase in Chien et al's scheme. The registration phase deals with the remote user's registration, i.e., processing the user's identity ID and password PW by a special algorithm and storing the user's information briefly which can be used to help the system identify the user and finally issuing smart card to user. User can use the information and function stored in his smart card and the PW to constitute a login request which is sent to the remote server for authenticating. Finally, in verification phase, the remote server can identify the login user and return message to the user to verify its own identity. We will give a brief review of these phases.

A. Registration Phase

Let h be a secure one-way hash function and $''\oplus''$ is the bitwise-or exclusion operation. When a new user puts forward his application containing his identity ID_i and password PW_i for registration to the system, the system computes

$$R_i = h(ID_i \oplus x_s) \oplus PW_i \tag{1}$$

in which the secret key x_s for the user is chosen randomly. Then, the system issues a smart card which stores $h(\ )$ and R_i to the user.

B. Login Phase

When the user wants to login to the system, he inserts his smart card to the terminal and input his ID_i and PW_i Smart card then computes

$$\begin{cases} C_i = R_i \oplus PW_i \\ C_2 = h(C_i \oplus T) \end{cases} \tag{2}$$

and sends the login request (ID_i, T, C_2) to the system, where T is the current time.

C. Verification Phase

Suppose that the system receives the login request (ID_i, T, C_2) at time T', it takes the following steps to verify the login request.

1. The system checks the valid of the ID_i, if it is valid, then receiving the login request, otherwise denying this request.

2. The system computes $\varDelta = T' - T$ and checks whether $\varDelta > \varDelta T$ or not. If $\varDelta > \varDelta T$, it denies this request. Here, $\varDelta T$ is a constant time parameter decided by the system based on the network's condition.
3. The system computes $h(h(IDi \oplus xs) \oplus T)$ and checks if it is equal to C_2. If it is the same, the user's identification is passed, otherwise failed.
4. The system computes C_3 as $h(h(ID_i \oplus x_s) \oplus T'')$ and sends returned message (C_3, T'') back to the user to verify the identity of the system. Here, T'' is the current time of the system. Once the user receives the returned message, it checks whether $h(C_1 \oplus T'') = C_3$ or not. If so, the identity of the system is passed; otherwise, user disconnects the connection.

Hsu[8] pointed out that Chien et al's scheme is vulnerable to parallel session attack in which an adversary U_a without knowing user's password can masquerade as a legal user U_i by eavesdropping and tampering the message between the system and U_i. It attacks on Chien at al's scheme as the following steps. By eavesdropping the communication, the adversary U_a can get the message (ID_i, T, C_2) and (C_3, T''). Then U_a masquerades as U_i to start a new session and sending (ID_i, T, C_3) back to the system, it will pass the authentication by the system due to

$$C_3 = h(h(ID_i \oplus x_s) \oplus T'') \qquad (3)$$

U_a just needs to ignore the returned message.

III. An Enhanced Remote Login Authentication Scheme with Smart Card

In this section, we will propose en enhanced remote login authentication scheme. This scheme has merits of secure mutual authentication, resistance of replay attack, freely password for user, no verified table and low computation and communication cost. Without loss generality, our scheme has registration, login and verification phase.

A. Registration phase

In registration phase, assume that a user U_i submits his ID_i and PW_i to the system for registration, the system computes

$$R_i = h(ID_i \oplus x_s) \oplus h(PW_i) \qquad (4)$$

and stores R_i, ID_s and the one-way function $h(\ )$ and a random constant e chosen by system in the smart card. Here ID_s is the server' s identity.

B. Login phase

When U_i wants to login in the system in login phase, he input his ID_i and PW_i to the terminal. The smart card computes

$$\begin{cases} C_i = R_i \oplus h(PW_i) \\ C_2 = h(C_i \oplus T) \\ M = h(e \oplus T) \end{cases} \qquad (5)$$

here T is the current time. The login request (ID_i, T, C_2, M) is sent to the system for verification.

C. Verification Phase

In the verification phase, after checking the validity of the request by checking the user's ID and the time stamp, the system computes and checks the following equation

$$C_2 = h(h(ID_i \oplus x_s) \oplus T) \tag{6}$$

if so, accept the request. And then, the system computes return message.

$$M_s = h(ID_s \oplus M) \tag{7}$$

and sends it back to the user. Upon receiving the M_s, user checks this equation

$$M = h(M_s \oplus ID_s) \tag{8}$$

if so, it means that mutual authentication succeeds.

IV. Security and perfomance analysis

In our scheme, the communication message contains (ID_i, T, C_2, M) and Ms. Since Ms has no relation with C_2, so the adversary can't take parallel session attack on it. Moreover, M is changed with the login time, which can resist replay attack by someone masquerading as a server. Besides, due to the time stamp, the scheme can resist the replay attack. Furthermore, if a user wants to change his password from PW_{iold} to PW_{inew}, he only needs to calculate

$$R_{inew} = R_i \oplus h(PW_{iold}) \oplus h(PW_{inew}) \tag{9}$$

and stores it replacing R_i in smart card. Comparing with Chien at al's scheme, our scheme didn't increase the communication cost. It only increases two more parameter stored in the smart card, i.e., ID_s and e, and several computations on hash function and exclusive-or operation which will not increase the computational cost significantly.

V. Conclusion

In this paper, we firstly discussed the Chien at al's scheme for remote login authentication and the parallel session attack on it. Then we put forward an enhanced remote login authentication with smart card, which is a secure mutual authentication with resistance to parallel session attack. Moreover, it can resist replay attack and freely change password by user. Comparing with Chien at al's scheme, our scheme didn't increase communication and computation cost significantly.

References

[1] Lamport L. Password authentication with insecure communication. *Comm ACM*, 24(11), pp 770-773, 1981.

[2] M.S.Hwang, L.H.Li, A new remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics* Vol.46, pp28-30, 2000.

[3] C.K.Chan and L.M.Cheng, Cryptoanalysis of a remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol.46. pp. 992-993, 2000.

[4] J.J.Shen, C.W.Lin and M.S.Hwang, A modified remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, Vol. 49, No.2, pp. 414-416, 2003.

[5] H.M.Sun, An efficient remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, Vol.46, pp.958-961,2000.

[6] A.K.Awasthi and S.Lal, A remote user authentication scheme using smart cards with forward secrecy, *IEEE Trans. Consumer Electronics*, Vol. 49, pp.1246-1248, 2003.

[7] H.Y.Chien, J.K.Jan and Y.M.Tseng, An efficient and practical solution to remote authentication: smart card, *Computers&Security*, Vol. 21 (4), pp.372-375, 2002.

[8] C.L.Hsu, Security of two remote user authentication schemes using smart cards, *IEEE Trans. Consumer Electronics*, Vol. 49, pp.1196-1198, 2003