AN EFFICIENT AND SECURE REMOTE AUTHENTICATION SCHEME USING SMART CARDS

Chin-Chen CHANG and Jung-San LEE

Abstract: Security of data communication becomes a crucial challenge due to the rapid development of computer and information technologies. To ensure security of resource transmission, engineers have proposed numerous schemes for protection. Among them, the remote password authentication schemes using smart cards are regarded as very efficient. As a result, smart-card based authentication schemes has become a popular research topic in recent years. In 2000, Hwang and Li proposed a new remote authentication scheme using smart cards based on ElGamal's cryptosystem. Unfortunately, the scheme Hwang and Li propose suffers from some security flaws. In this article, the authors propose a practical and secure version providing mutual authentication, increasing the authentication efficiency, and allowing the user to choose and change his/ her password at will.

Keywords: Communications, Remote Authentication, Smart Cards, Resource Protection.

Introduction

The control of the access to remote resources has become a crucial challenge due to the rapid development of computer and information technologies. Generally, most of the resources provided on Internet are not free for all users. Often, some services on the remote servers are paid. In other words, the providers of the services/ facilities have to put their resources under appropriate protection. The password authentication schemes are usually considered as the most efficient and practical method to achieve the goal of protecting remote resources. In the password authentication schemes, the user sends his/ her identity (ID) and password (PW) to the server in order to get authentication when he/ she wants to access facilities on the remote system. ID and PW are issued to the user by the remote server in the registration phase. If the user is authenticated successfully, the user will be authorized to access the facilities provided by the remote system; otherwise, the access request will be rejected.[1,2,3,4,5,6,7,8,9,10]

In 1981, Lamport proposed a remote authentication scheme for communication through insecure channels.[11] Lamport's scheme can withstand the replay attack and it needs a verification table to verify the legality of the login user. Nevertheless, the verification table makes Lamport's scheme suffer from the stolen-verifier attack if somehow an intruder succeeds to get the stored verifier. Recently, a great deal of password authentication schemes using smart cards has been proposed to improve the traditional authentication schemes. The smart card is used to authenticate the legality of the user such that it is unnecessary for the remote server to store the verification table. Hence, the stolen-verifier attack can be resolved.[12,13,14,15,16,17,18,19] What is more important, a timestamp is often used to resist the replay attack. However, sophisticated hardware is needed to support the concurrent mechanism.

In 1994, Chang and Liao proposed a remote authentication scheme based on ElGamal's signature scheme.[20] Later, Wu proposed an efficient remote authentication scheme based on a simple geometric approach.[21] Wu's scheme makes possible the user to choose his/ her password at will. Unfortunately, Hwang has found and outlined weaknesses in Wu's scheme.[22] In 2000, Hwang and Li proposed a novel remote authentication scheme (Hwang-Li's scheme) using smart cards based on ElGamal's cryptosystem.[23] Shortly afterwards, Chan and Cheng demonstrated that the scheme of Hwang and Lee is insecure as well.[24] Besides, in 2003, Shen, Lin, and Hwang presented another attack on Hwang-Li's scheme.[25] Furthermore, mutual authentication between the remote server and the user is essential to ensure the security of the data transmitted over the insecure networks. But in most of these schemes, only the user is authenticated.[26,27,28] Therefore, in this article the authors propose an efficient and secure authentication scheme. The proposed scheme not only provides mutual authentication between the remote server and the user but also increases the efficiency of authentication. Furthermore, the attacks that Hwang-Li's scheme cannot resist do not affect the proposed scheme.

The rest of the paper is organized as follows. The article first reviews the scheme proposed by Hwang and Li. Some attacks on Hwang-Li's scheme are presented afterwards. A novel scheme is then proposed. Next, the security of the proposed scheme is analyzed, followed with discussions. Finally, the authors give some conclusions and outline directions for future research.

Review of Hwang-Li's Scheme

This section reviews the scheme proposed by Hwang and Li and then presents possible attacks on that scheme.

Review of Hwang-Li's Scheme

In this subsection, the authors briefly review the remote password authentication scheme of Hwang and Li.[29] The security of Hwang-Li's scheme is based on the ElGamal's public key cryptosystem. Hwang-Li's scheme is divided into three phases: registration phase, login phase and authentication phase. The details of the three phases are shown below.

Registration Phase

Let x be a secret key maintained by the system and $H(\cdot)$ be the public one-way hash function. A new user U_i needs to submit his/her identity ID_i to the system first for registration. The remote system chooses a large prime number P and computes U_i's password PW_i as follows:

$$PW_i = (ID_i)^x \bmod P,$$

The registration center then issues a smart card containing $H(\cdot)$ and P and sends PW_i to U_i through a secure channel.

Login Phase

When the user U_i decides to access data from the remote site, he/she has to insert his/her smart card into the input device and type his/her identity ID_i and password PW_i first. The smart card then executes the following procedure:

- *Step 1*: Generates a random number r .
- *Step 2*: Computes $C_1 = (ID_i)^r \bmod P$.
- *Step 3*: Computes $t = H(PW_i \oplus T) \bmod (P-1)$, where T is the current time-stamp of the input device and $\oplus$ denotes an exclusive "or" operation.
- *Step 4*: Computes $K = (ID_i)^t \bmod P$.
- *Step 5*: Computes $C_2 = K(PW_i)^r \bmod P$.
- *Step 6*: Sends the message $M = \{C_1, C_2, ID_i, T\}$ to the remote server.

Authentication Phase

Upon receiving M from U_i , the system authenticates U_i by performing the following procedure:

- *Step 1*: Checks the validity of ID_i. If the format of ID_i is not correct, rejects the access request; otherwise, the procedure goes to the next step.
- *Step 2*: Checks the validity of the time interval between T and T'. If $(T - T') \geq \Delta T$, rejects the access request; otherwise, performs the next step. Here T' is the current timestamp of the system and ΔT is the acceptable time interval of the transmission delay.
- *Step 3*: Checks if $C_2 (C_1^x)^{-1} \bmod P = (ID_i)^{H(PW_i \oplus T)}$. If it holds, the access request is accepted; otherwise, terminates the connection.

Review of Chan-Cheng's Attack

In 2000, Chan and Cheng[30] pointed out that Hwang-Li's scheme cannot resist the masquerade attack. This attack could be described as follows. Suppose that a user U_c wants to counterfeit other legal users to access facilities on the remote system. U_c submits his/her ID_c to the remote system for registration. The server then issues a smart card and the corresponding password PW_c to him/her after the identity is verified. Now, U_c can generate a legal user identity ID_f and the corresponding password PW_f by computing

$$ID_f = (ID_c \cdot ID_c) \bmod P, \text{ and}$$

$$PW_f = (ID_f)^x = (PW_c \cdot PW_c) \bmod P.$$

Therefore, U_c can successfully login to the remote system to access facilities with the counterfeit (ID_f , PW_f).

Review of Shen-Lin-Hwang's Attack

In 2003, Shen, Lin, and Hwang presented another attack on Hwang-Li's scheme.[31] Their attack could be described as follows. Suppose that a user U_c wants to impersonate a legal user U_h to access the facilities on the remote system. Because ID_h is public, U_c can choose his/her $ID_c = (ID_h)^z \bmod P,$ where z is a random integer chosen by U_c and $\gcd(z, \phi(P)) = 1.$ The user U_c then submits his/her ID_c to the remote system for registration. Upon receiving the registration request from U_c, the remote server will verify the identity attached to the registration request and compute $PW_c = (ID_c)^x \bmod P.$ The registration center then sends PW_c and issues a smart card containing $H(\cdot)$ and P to U_c. As a result, U_c can derive U_h's password PW_h as follows:

$$\begin{aligned}(PW_c)^{-z} \bmod P &= ((ID_c)^x)^{-z} \bmod P \\ &= (((ID_h)^z)^x)^{-z} \bmod P \\ &= (ID_h)^x \bmod P \\ &= PW_h \bmod P.\end{aligned}$$

Then, U_c successfully obtains U_h's password to access the remote system as U_h.

The Proposed Scheme

Due to the fact that the computational ability of the smart card is usually low, it is quite important to reduce the computation load of the smart card to increase the efficiency of authentication. In addition, mutual authentication between the remote system and the user is also an essential requirement in remote password authentication schemes as mentioned above. Therefore, the authors propose an efficient password authentication scheme that not only ensures mutual authentication between the remote system and the user to enhance security, but also increases the efficiency of authentication. Besides, the proposed scheme also overcomes the security weaknesses present in Hwang-Li's scheme. In the proposed scheme, in order to make the password authentication scheme more user-friendly, the user is permitted to choose his/her password at will.

The scheme proposed in this article also consists of three phases: registration phase, login phase and authentication phase. Figure 1 presents the flowchart of the login and authentication phases of the scheme. The three phases could be described as follows.

Registration Phase

Let p and q be the secret keys maintained by the system and $H(\cdot)$ be the one-way hash function, where p and q are large prime numbers. g is a primitive element in $GF(n)$, where $n = p \cdot q$. First, for registration, a new user U_i has to submit his/her identity ID_i and the password PW_i chosen by himself/ herself to the system using a secure channel. After receiving the registration request, the remote system performs the following operations:

- *Step 1*: Computes $H(PW_i)$.
- *Step 2*: Computes $temp$ as follows: $temp = g^{ID_i^{-1}} \bmod n.$

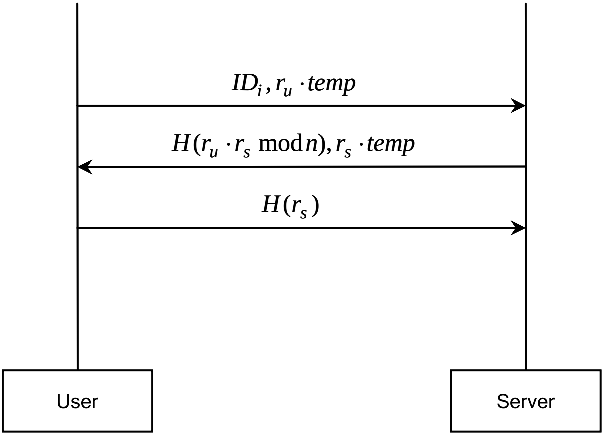

Figure 1: Flowchart of Login and Authentication Phases of the Proposed Scheme.

- *Step 3*: Computes $H(PW_i) \oplus temp$.
- *Step 4*: Issues a smart card containing { $(H(PW_i) \oplus temp)$, n , $H(\cdot)$ } to U_i.

Login Phase

When the user U_i wants to access the facilities offered by the remote system, he/she has to insert the smart card into the input device and enter ID_i and PW_i. The smart card then executes the following procedure:

- *Step 1*: Generates a random number r_u, which is used only once.
- *Step 2*: Computes $H(PW_i)$.
- *Step 3*: Retrieves $temp$.
- *Step 4*: Computes $H(PW_i) \oplus (H(PW_i) \oplus temp)$.
- *Step 5*: Computes $r_u \cdot temp$.
- *Step 6*: Sends the message $M = \{ID_i, r_u \cdot temp\}$ to the remote system.

Authentication Phase

After sending M to the system, the system and the user U_i execute the following procedure to authenticate each other.

- *Step 1*: While receiving M, the remote server generates a random integer r_s, then computes $(((temp)^{-1} \bmod n) \cdot (r_u \cdot temp)) \bmod n$ to retrieve r_u, where r_s is used only once.
- *Step 2*: The system then computes $H(r_u \cdot r_s \bmod n)$ and $r_s \cdot temp$ and sends the message $M' = \{H(r_u \cdot r_s \bmod n),\ r_s \cdot temp\}$ to U_i.
- *Step 3*: Upon receiving M' sent from the remote system, the smart card retrieves r_s and computes $((temp)^{-1} \bmod n) \cdot (r_s \cdot temp) \bmod n$.
- *Step 4*: The smart card then computes $H(r_u \cdot r_s \bmod n)$ and compares it with the received one. If they are not equivalent, the connection is terminated; otherwise, the remote system is authenticated successfully by the user U_i, and the phase continues.
- *Step 5*: The smart card computes $H(r_s)$ and sends the result to the remote system.
- *Step 6*: After receiving the transmitted message sent from U_i, the remote server computes $H(r_s)$ and compares it with the received one. If they are not equal, the authentication fails; otherwise, U_i is authenticated successfully by the remote server.

Security Analysis

This section will demonstrate that the proposed remote password authentication scheme is secure with the following attack scenarios.

The Replay Attack

The replay attacks cannot work on the proposed scheme. That is, retransmitting neither the login message $M = \{ID_i, r_u \cdot temp\}$ in the login phase nor the response message $M' = \{H(r_u \cdot r_s \bmod n), r_s \cdot temp\}$ in the authentication phase will succeed since the validity of M and M' can be checked with the random numbers r_u and r_s, respectively. Even if an intruder eavesdrops M successfully in the login phase and replays M to fool the remote server, he/she will fail in Step 3 of the authentication phase. The reason is that only the legal user can retrieve r_s chosen by the remote system, and r_s is used only once. On the other hand, if an intruder eavesdrops M' in the authentication phase and retransmits it to fool the login user, he/she will fail in Step 4 of the authentication phase. The value of $H(r_u \cdot r_s \bmod n)$ is not equal to the replayed one since the random number r_u is used only once and it is absolutely different from the replayed one.

Deriving the Secret Key of the Remote Server

When an intruder attempts to derive the secret key of the remote system, p and q, from n, he/she will fail. The reason is that he/she will encounter the difficulties of solving the factoring problems.

Losing the Smart Card

An intruder will also fail in the case when he/she steals the smart card of the legal user U_i and wants to use it to access the facilities provided by the remote server. The reason is that the intruder can not retrieve $temp$ without knowing PW_i.

The Server Spoofing Attack

When a masqueraded server intends to cheat an innocent user, it cannot fake a response message $M'' = \{H(r_u \cdot r_s \bmod n), r_s \cdot temp\}$. First, it is due to the fact that the intruder cannot retrieve $temp$ as stated before. Second, without knowing $temp$, r_u, used only once, also cannot be obtained successfully.

The Stolen-Verifier Attack

In the scheme proposed in this article, no verification table is needed. That is, it is impossible for an attacker to mount the stolen-verifier attack on it.

Discussion

The security flaws of the remote password authentication scheme proposed by Hwang and Li do not affect the scheme proposed here. On the other hand, when a legal user U_i wants to change his/her password, he/she only needs to submit his/her smart card to the remote system together with a new password PW_i' through a secure channel. The remote system then re-computes $H(PW_i')$ and $(H(PW_i') \oplus temp)$. Then, the server uses $(H(PW_i') \oplus temp)$ to replace the original one stored in U_i's smart card. After the replacement, the user U_i can use the new password PW_i to login to the remote server. Therefore, it is easy for the user to change the password and to remember it. In other words, the proposed scheme enables the users to choose and change their passwords at will.

Table 1 provides comparison between the characteristics of the proposed scheme and the scheme of Hwang and Li. Among the considered characteristics, mutual authenti-

Table 1: Comparison between the Proposed Scheme and Hwang-Li's Scheme.

	Proposed Scheme	*Hwang-Li's Scheme*
Security Flaw	No	Yes
Choose and Change Password at Will	Yes	No
Verification Table	No	No
Concurrent Mechanism	No	Yes
Mutual Authentication	Yes	No

cation is only present in the proposed scheme to enhance security as elaborated in a previous section. In addition, the proposed scheme can withstand the replay attack without employing the timestamp as shown above. In other words, the scheme presented in this article does not require an additional sophisticated concurrent mechanism to resist the replay attack.

What is more important, in what follows the authors present efficiency comparisons between the proposed scheme and Hwang-Li's scheme in order to demonstrate that the scheme proposed here is not only more secure but also more efficient. Nowadays, most of the servers have high computational power, while the smart cards are still with low computation ability. The key point in improving the efficiency of the authentication processes is reducing the computation load of the smart card. Therefore, the authors have made the computation load of the smart card as light as possible in the scheme they propose.

First, the authors define the symbols used in Table 2. e denotes the exponential computation operation. h denotes the computation operation of the one-way hash func-

Table 2. Comparison of the Efficiency between the Proposed Scheme and Hwang-Li's Scheme.

	Proposed Scheme		*Hwang-Li's Scheme*	
	Smart Card	*System*	*Smart Card*	*System*
Computation of RP	0	$1e, 1h, 1\oplus$	0	$1e$
Computation of LP	$1h, 1\oplus$	0	$3e, 1h, 1\oplus$	0
Computation of AP	$2h$	$1e, 1h$	0	$3e, 1h, 1\oplus$

tion. $\oplus$ denotes XOR. RP means Registration Phase. LP means Login Phase. AP means Authentication Phase. Considering the several computation operations, the exponential operation is of main concern for the whole computation load since the computation load of the exponential operation is far heavier than that of the other operations. According to Table 2, it is evident that the proposed scheme is more efficient than Hwang-Li scheme. It is because only one exponential operation is needed for mutual authentication.

Conclusions

In this article, the authors propose a novel remote password authentication scheme that overcomes the security weaknesses of Hwang-Li's scheme. The proposed scheme provides mutual authentication between the remote system and the user such that the server spoofing attack cannot have an effect. Besides, the scheme allows the user to choose and change passwords at will and can resist the replay attack without sophisticated concurrent mechanisms.

As mentioned above, the proposed scheme is more efficient, secure and user-friendly than Hwang-Li's scheme. Since the computation load of both the smart card and the whole system is quite low, the proposed scheme is efficient, secure, user-friendly to be applied in practice; moreover it could be employed on imbalanced networks as well.

Notes:

[1] Jau-Ji Shen, Chih-Wei Lin, and Min-Shiang Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards," IEEE *Transactions on Consumer Electronics* 49, no. 2 (May 2003): 414-416.

[2] Min-Shiang Hwang and Li-Hua Li, "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics* 46, no. 1 (February 2000): 28-30.

[3] Shyi-Tsong Wu and Bin-Chang Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards," *Computers & Security* 22, no. 6 (2003): 547-550.

[4] Hung-Min Sun, “An Efficient Remote User Authentication Scheme Using Smart Cards,” *IEEE Transactions on Consumer Electronics* 46, no. 4 (November 2000): 958-961.

[5] Suguru Yamaguchi, Kiyohiko Okayama, and Hideo Miyahara, “Design and Implementation of an Authentication System in WIDE Internet Environment,” in *Proceedings of the 10th IEEE Regional Conference on Computers and Communication Systems* (Hong Kong, 24-27 September 1990), 653-657.

[6] Chin-Chen Chang and Tzong-Chen Wu, “Remote Password Authentication with Smart Cards,” *IEE Proceedings-E* 138, no. 3 (1991): 165-168.

[7] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang, “A Remote User Authentication Scheme Using Smart Cards,” *ACM Operating Systems Review* 36, no. 4 (2002): 23-29.

[8] Yuan-Liang Tang, Cheng-Chi Lee, and Min-Shiang Hwang, “A Simple Remote User Authentication Scheme,” *Mathematical and Computer Modelling* 36 (2002): 103-107.

[9] Tzong-Chen Wu and Hung-Sung Sung, “Authenticating Passwords over an Insecure Channel,” *Computers & Security* 15, no. 5(1996): 431-439.

[10] Kaijun Tan and Hongwen Zhu, “Remote Password Authentication Scheme Based on Cross-Product,” *Computer Communications* 22, no. 4 (March 1999): 390-393.

[11] Leslie Lamport, “Password Authentication with Insecure Communication,” *Communications of the ACM* 24, no. 11 (November 1981): 770-772.

[12] Shen, Lin, and Hwang, “A Modified Remote User Authentication Scheme Using Smart Cards.”

[13] Chin-Chen Chang and Wen-Yuan Liao, “A Remote Password Authentication Scheme Based upon ElGamal’s Signature Scheme,” *Computers & Security* 13, no. 2 (April 1994): 137-144.

[14] Min-Shiang Hwang, “Cryptanalysis of a Remote Login Authentication Scheme,” *Computer Communications* 22 (1999): 742-744; Hwang and Li, “A New User Authentication Scheme Using Smart Cards.”

[15] Chin-Chen Chang and C. S. Liah, “Comment on Remote Password Authentication with Smart Cards,” *IEE Proceedings-E* 139, no. 4 (1992): 372-372.

[16] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, “An Efficient and Practical Solution to Remote Authentication: Smart Card,” *Computers & Security* 21, no. 4 (2002): 372-375.

[17] Debbie McElroy and Efraim Turban, “Using Smart Cards in Electronic Commerce,” *International Journal of Information Management* 18, no. 1 (1998): 61-72.

[18] Chin-Chen Chang and Shin-Jia Hwang, “Using Smart Cards to Authenticate Remote Passwords,” *Computers and Mathematics with Applications* 26, no. 7 (1993): 19-27.

[19] Shiuh-Jeng Wang and Jin-Fu Chang, “Smart Card Based Secure Password Authentication Scheme,” *Computers & Security* 15, no. 3 (1996): 231-237.

[20] Tan and Zhu, “Remote Password Authentication Scheme Based on Cross-Product.”

[21] Tzong-Chen Wu, “Remote Login Authentication Scheme Based on a Geometric Approach,” *Computer Communications* 18, no. 12 (1995): 959-963.

[22] Min-Shiang Hwang, “Cryptanalysis of a Remote Login Authentication Scheme,” *Computer Communications* 22, no. 8 (1999): 742-744.

[23] Hwang and Li, “A New User Authentication Scheme Using Smart Cards.”

[24] Chi-Kwong Chan and L.M. Cheng, “Cryptanalysis of a Remote User Authentication Scheme Using Smart Cards,” *IEEE Transactions on Consumer Electronics* 46, no. 4 (November 2000): 992-993.

[25] Shen, Lin, and Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards."

[26] Wu and Chieu, "A User Friendly Remote Authentication Scheme with Smart Cards."

[27] Sun, "An Efficient Remote User Authentication Scheme Using Smart Cards."

[28] Chien, Jan, and Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card."

[29] Hwang and Li, "A New User Authentication Scheme Using Smart Cards."

[30] Chan and Cheng, "Cryptanalysis of a Remote User Authentication Scheme Using Smart Cards."

[31] Shen, Lin, and Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards."

JUNG-SAN LEE see page 84

CHIN-CHEN CHANG see page 84