A secure and efficient scheme for authenticating remote users using smart card

Iuon-Chang Lin[1] Yang-Bin Lin[2] Chung-Ming Wang[2]
Department of Management Information Systems[1]
National Chung Hsing University, Taichung, Taiwan

Department of Computer Science[2]
National Chung Hsing University, Taichung, Taiwan

Abstract

In 2002, Chien, Jan, and Tseng proposed an efficient and practical solution to remote authentication using smart card. However, in 2004, Hsu pointed out Chien, Jan, Tseng's scheme has a secure flaw that is vulnerable to parallel session attack. Therefore, in this paper, we improve Chien, Jan, Tseng's scheme to withstand parallel session attack. In addition, our scheme also keeps the benefits of Chien, Jan, Tseng's scheme.

Keywords: User authentication, parallel session attack

1 Introduction

Recently, there are many remote user authentication schemes [1, 2, 5, 6, 7] have been proposed. In general, before accessing the resources of a remote server, the system must authenticate the legitimacy of remote user. A remote user authentication scheme must satisfy the following requirements: (1) it doe not need any authentication table; (2) users can freely choose their passwords; (3) it can provide mutual authentication.

In 2000, Hwang and Li [6] proposed a remote user authentication scheme using smart cards. The main advantage of this scheme is that the system does not maintain any authentication table. Later, Sun [7] proposed an efficient remote use authentication scheme using smart cards to improve the efficiency of the scheme proposed by Hwang and Li [6]. However, the two schemes have the same disadvantage that the system users can not freely choose their passwords. In addition, Sun's scheme only provides user authentication but it can't provide mutual authentication. Therefore, in 2002, Chien, Jan, and Tseng [2] proposed an efficient and practical solution to solve these problems. But, in 2004, Hsu [4] pointed out that Chien, Jan, Tseng's scheme is vulnerable to parallel session attack [3]. In order to withstand the parallel session attack, we improve the Chien, Jan, and Tseng's scheme in this paper. In addition, our scheme still maintains the benefits of Chien, Jan, and Tseng's scheme. The benefits of their scheme can be described as follows.

1. Users can freely choose the passwords on their own.
2. It can reach the ability of mutual authentication between the user and the system.
3. Authentication table is not required.
4. Only hash function operations are performed by the system and user, so computational cost is

low.

Later, we firstly review of Chien, Jan, and Tseng's scheme and specify its weakness. In Section 3, the proposed scheme is described and the security of the improved scheme is analyzed. Finally, we make a brief conclusion in Section 4.

2 Review of Chien, Jan, and Tseng's scheme

In this section, we will review the remote authentication scheme proposed by Chien, Jan, and Tseng [2]. Their scheme is composed of three phases: the registration phase, the login phase, and the verification phase.

2.1 The registration phase

Suppose that a remote user U_i wants to register to be a legal user, and then he submits his identity ID_i and password PW_i to the system for registration. The system computes $R_i = h(ID_i \bigoplus x) \bigoplus PW_i$, and stores R_i and $h()$ into the memory of smart card, where $h()$ denotes a secure one-way hashing function, x denotes a secret key kept by the system. Finally, the system issues the smart card to the user.

2.2 The login phase

When an authorized user U_i wants to log into the server, he has to perform the following steps.

Step 1 : U_i inserts his smart card into the terminal and input his ID_i and PW_i.

Step 2 : The smart card enforce the following operations.

$$C_1 = R_i \bigoplus PW_i, \quad (1)$$

$$C_2 = h(C_1 \bigoplus T1), \quad (2)$$

where T_1 is the current timestamp.

Step 3 : U_i sends the message (ID_i, T_1, C_2) to the system.

2.3 The verification phase

After receiving the message(ID_i, T_1, C_2), both the system and user U_i perform mutual authentication as following.

Step 1 : The system checks the validity of ID_i. Then, the system checks whether $T_2 - T_1 <= \Delta T$ or not, where $T2$ is the current timestamp, and ΔT is the reasonable and valid time interval for the transmission delay. If one of the above is not true, then system rejects the user's login request.

Step 2 : The system computes $C_1^{'} = h(ID_i \bigoplus x)$ and verifies $C_2 ?= h(C_1^{'} \bigoplus T_1)$. If it holds, the system can confirm that the login user is authorized and the system accepts the user's login request.

Step 3 : The system computes $C_3 = h(C_1^{'} \bigoplus T_3)$, where T_3 is the current timestamp. Then the system sends the message (T_3, C_3) to the user U_i.

Step 4 : After receiving the message (T_3, C_3), the user U_i verifies the message by checking $T_4 - T_3 <= \Delta T$, where T_4 is the current timestamp. Then, the user verifies $C_3 ?= h(C_1^{'} \bigoplus T_3)$. If both of the above are true, the user can confirm that the system is a legal system.

2.4 The security weakness of Chien, Jan, and Tseng's scheme

Hsu [4] in 2004 pointed out that Chien, Jan, and Tseng's scheme is vulnerable to parallel session attack. Suppose that a legal user U_i wants to log into the system, U_i sends the message (ID_i, T_1, C_2) to the system. Then, the system authenticates the login request. Due to U_i is a legal user, the system can accept the the login request. Then, the system responses the message (T_3, C_3) to the user U_i. In the meanwhile, a illegal user Bob wants to act as a legal user U_i without knowing the $U_i^{'}$ password. Bob can intercept the message (T_3, C_3). Next, Bob sends the message (ID_i, T_3, C_3) to the system to start a new session. The message can pass the authentication process at

the Step 1. Thus, Chien, Jan, and Tseng's scheme can not withstand parallel session attack.

3 Proposed scheme

In this section, we will improve Chien, Jan, and Tseng's scheme to withstand the parallel session attack. Our scheme also divides into three phases. The registration phase and the login phase in our scheme are the same as Chien, Jan, and Tseng' scheme [2]. Therefore, we only describe the verification phase as following.

3.1 The modified phase

After receiving the message(ID_i, T_1, C_2), both the system and user U_i will perform mutual authentication as follows.

Step 1 : The system checks the validity of ID_i. Then, the system checks whether $T_2 - T_1 <= \Delta T$ or not, where $T2$ is the current timestamp, and ΔT is the reasonable and valid time interval for the transmission delay. If above verifications hold, then system accepts the login request.

Step 2 : The system computes $C_1^{'} = h(ID_i \bigoplus x)$ and verifies $C_2 ?= h(C_1^{'} \bigoplus T_1)$. If it holds, the system accepts the login request. Otherwise, the system rejects the login request.

Step 3 : The system computes $C_3 = h(C_1^{'} \bigoplus T_3) \bigoplus ID_i$, where T_3 is the current timestamp. Then the system sends the message (T_3, C_3) to U_i.

Step 4 : After receiving the message (T_3, C_3), U_i checks $T_4 - T_3 <= \Delta T$, where T_4 is the current timestamp. Then, U_i verifies $C_3 ?= h(C_1^{'} \bigoplus T_3) \bigoplus ID_i$. If the above verifications hold, U_i confirms that the system is legal.

3.2 Security analysis

The security of the proposed scheme can be analyzed as follows.

1. Our scheme can prevent from reply attack by using the concept of timestamps.

2. Our scheme can prevent from parallel session attack by checking $C_2 = ?\ h(C_1^{'} \bigoplus T_1)$ and $C_3 = ?\ h(C_1^{'} \bigoplus T_3) \bigoplus ID_i$.

3. Due to the property of one-way hash function, given a valid message (ID_i, T_1, C_2), an adversary can not derive another valid message $(ID_i, T_1^{'}, C_2^{'})$.

4. If a camouflaged system wants to cheat a requesting legal user, it must prepare a valid message (T_3, C_3). However, it is infeasible to know the value $h(ID_i \bigoplus x)$. Thus, it can't compute the value C_3.

5. If an adversary wants to act as a legal user, he must prepare a valid message (ID_i, T_1, C_2). But, it is infeasible to know the value C_1.

4 Conclusions

In 2004, Hsu pointed out that Chien, Jan, and Tseng' scheme can not withstand parallel session attack. In this paper, we mainly improve Chien, Jan, and Tseng' scheme to prevent from parallel session attack. Then, our scheme still maintains the benefits of Chien, Jan, and Tseng' scheme. Furthermore, our scheme only requires to perform the operations one-way hash function. Thus, the computation cost is low and the proposed scheme is efficient.

References

[1] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "A modified remote login authentication scheme based on geometric approach," *Journal of Systems and Software Volume*, vol. 55, pp. 287–290, Jan. 2001.

[2] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: Smart card," *Computers and Security*, vol. 21, pp. 372–375, Aug. 2002.

[3] L. Gong, "A security risk of depending on synchronized clocks," *Operating Systems Review*, vol. 26, pp. 49–53, Sep. 1992.

[4] C. L. Hsu, "Security of chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, pp. 167–169, May. 2004.

[5] M. S. Hwang, "Cryptanalysis of a remote login authentication scheme," *Computer Communications*, vol. 22, pp. 742–744, May. 1999.

[6] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 28–30, Feb. 2000.

[7] H. M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 958–961, Nov. 2000.