ON THE IMPROVEMENT OF REMOTE AUTHENTICATION SCHEME WITH SMART CARDS

Lih-Yang Wang and Chao-Chih Chen
Department of Electronic Engineering, Southern Taiwan University of Technology
Yung-Kang City, Tainan, Taiwan Roc

Keywords: Remote authentication, Privileged Insider attack, smart card.

Abstract: In 2005, Sun et al's proposed a user-friendly remote authentication scheme. In order to improve the efficiency of the authentication process, their method is based on one-way hash function. Unlike previous methods, Sun's method allows the user to choose and change the password locally without connecting to the server. It can resist replay attack, impersonation attack, guessing password attack, denial of service attack. However, in this paper we will point out that their scheme is vulnerable to privileged insider attack, and an enhanced scheme is proposed to eliminate the weakness.

1 INTRODUCTION

In 2000, Sun proposed a remote user authentication scheme using smart card base on one-way hash function (sun, 2000). His method does not need to store user's password and can resist a replay attack of an attacker. However, the user has no power to choose his password. This inconvenience was removed by Wu and Chieu's improved method few years later (Wu and Chieu, 2003), with an additional merit that the selection of password can be accomplished locally without the help of the server. Nevertheless, it is found that their method have some weakness (Yang and Wang, 2004; Wu and Chieu, 2004; Wang et al, 2005; Hsu, 2005; Hwang and Liao, 2005; Hwang et al, 2005; Lee and Chiu, 2005). If the attacker can intercept and forge messages between the user and the remote server, he can login to the server without having the correct password. To cope with this problem, a lot of enhanced schemes are proposed later, including Wu himself (Wu and Chieu, 2004; Wang et al, 2005; Hsu, 2005; Lee and Chiu, 2005). Unfortunately, it is found that Wu's own improved version is still risky under stolen smart card attack, forgery attack, privileged insider's attack and off-line password guessing attack (Yoon and Yoo, 2007 and Ku et al, 2005).

While most of the above methods, some operation of are used the logarithm functions and modulus exponentiation, Sun et al's improvement method (Sun et al, 2005) adopts only simple but effective hash functions. Their method can resist replay attack, impersonation attack, guessing password attack, denial of service attack, and only need to use the smart card to finish the demand of changing the password. But, it is still vulnerable to some attack.

In this paper, we will analyze Sun et al's method, and show that it is not secure under Privileged Insider's Attack (PIA). We then propose a new enhanced scheme to overcome this problem.

This paper is organized as follows: In Section 2, we review Sun et al's user-friendly remote authentication scheme. In Section 3, we prove that it is vulnerable under PIA. An improved scheme to eliminate the weakness is proposed in Section 4. The security analysis of the proposed method is given in Section 5. Finally, a brief conclusion is given in Section 6.

2 REVIEW OF SUN ET AL'S SCHEME

In this section, we briefly review Sun et al's scheme. Table 1 lists the definitions for all required symbols, there are needed for the successive description:

Wang L. and Chen C. (2007).
ON THE IMPROVEMENT OF REMOTE AUTHENTICATION SCHEME WITH SMART CARDS.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 93-97
DOI: 10.5220/0002124900930097

Table 1: Meaning of representatives of symbols.

symbols	meaning
U_i	the remote user
ID_i	U_i's identifier
PW_i	the password chosen by U_i
PW_i^*	the password inputted by U_i
PW_i'	the new password chosen by U_i
S	the server
x	secret key of the server
R	a randomly selected value by the user
R^*	a randomly inputted value by the user
R'	a randomly selected new value by the user
T	the current timestamp of the U_i input message.
T'	the current timestamp of the S receive message.
$T^{\#}$	the current timestamp of the attacker vary message.
$h(.)$	a cryptographic hash function
$\oplus$	a bitwise XOR operation
$\|$	a string concatenation operation

2.1 Registration Phase

In this phase, the legal user applies for his authorization of login.

Step 1: Transfer personal identity and password $\{ID_i , PW_i\}$ from U_i to S via a secure channel.

Step 2: S calculates A_i and B_i , where

$$A_i = h(ID_i , x) \quad (1)$$

$$B_i = A_i \oplus PW_i \quad (2)$$

Step 3: Store the smart card with U_i 's information $\{ ID_i , B_i , h(\cdot)\}$. Deliver the smart card to U_i via a secure channel.

2.2 Login Phase

In this phase, U_i will login to the server.

Step 1: U_i puts the smart card into the card reader, and inputs ID_i^* and PW_i^*

Step 2: The smart card computes A_i^* and C_1, where

$$A_i^* = B_i \oplus PW_i^* \quad (3)$$

$$C_1^* = h(T , A_i^*) \quad (4)$$

Step 3: The login message: $m=\{ ID_i^* , C_1^* , T\}$ are forward to S through a public channel.

2.3 Authentication Phase

In this phase, S verifies U_i 's login demand.

Step 1: S checks the U_i 's ID. If it is incorrect or already login, refuse the login request.

Step 2: S confirms the conveyance of login and receives time (T and T'), if unreasonable, refuse login request.

Step 3: S computes A_i , C_1 and check C_1^*. If inconsistent, refuse the login request.

$$A_i = h (ID_i , x)$$

$$C_1 = h (T \oplus A_I) \quad (5)$$

If $C_1 = C_1^*$, an inconsistency occurred, refuse the login request.

2.4 Password Change Phase

In this phase, U_i changes the password.

Step 1: U_i puts the smart card into the card reader, and input ID_i^*, PW_i^* and PW_i'.

Step 2: It computes a new value B_i' for the smart card to replace B_i. The symbol PW_i^* denotes the new password.

$$B_i' = B_i \oplus PW_i \oplus PW_i' \quad (6)$$

3 ANALYSE THE SUN ET AL'S METHOD

In this Section, we will analyze Sun et al's method from two aspects, that is, security and authentication efficiency.

3.1 Privileged Insider's Attack

Though the user conveys identity and password to the server and applies for the smart card through the secure channel. However, if the user's password is not protected, one single privileged insider can get the user's password, imitate user's login to system and gain improper benefit (Ku et al, 2005).

3.2 Efficiency Analysis

According to Sun et al's scheme, whenever a user inputs a wrong password, he has to wait for the server to decline his request. That is, it needs two transmissions between the user end and the server end. This mechanism seems troublesome and inefficient. If the smart card itself has the ability to verify the password, it can considerably simplify the whole authentication process. In addition, if the password is not confirmed, then the smart card will face the risk revised illegally.

4 THE PROPOSED METHOD

In this section, we propose an improved method can prevent the privileged insider's attack, and add the mechanism of password authentication in the smart card. The scheme includes four phases: registration phase, login phase, authentication phase and password change phase.

4.1 Registration Phase

In this phase, the legal U_i applies for the authorization of login. For presentation neat, we follow the same convention as Sun et al's.

Step 1: U_i randomly chooses a value R, and computes the register password G.

$$G = h(PW_i \| R) \quad (7)$$

Step 2: U_i submits $\{ID_i, G\}$ to S via a secure channel.

Step 3: S calculates A_i, B_i and V, where

$$A_i = h(ID_i \oplus x)$$
$$B_i = A_i \oplus G \quad (8)$$
$$V = h(ID_i \oplus G) \quad (9)$$

Step 4: S send U_i 's information $\{ID_i, B_i, h(.), V\}$ to U_i, it is then stored in the smart card.

4.2 Login Phase

In this phase, U_i will login to S.

Step 1: U_i puts the smart card into the card reader, and input ID_i^*, PW_i^* and the number R^*.

Step 2: Smart card computes G^* and V^*, and then compare it with V. If equivalent, go to the next step; otherwise, stop.

$$G^* = h(PW_i^* \| R^*) \quad (10)$$
$$V^* = h(ID_i^* \oplus G^*) \quad (11)$$

Step 3: The smart card computes A_i^* and C_1^*.

$$A_i^* = B_i \oplus G^* \quad (12)$$
$$C_1^* = h(T \oplus A_i^*) \quad (13)$$

Step 4: The login message $m = \{ID_i, C_1^*, T\}$ is forward to S through a public channel.

4.3 Authentication Phase

In this phase, S verifies U_i's login demand.

Step 1: S confirms the U_i's ID_i, if the identity is incorrect or already logged in, refuse login request.

Step 2: S compares the time stamp T in the login message with the time T' that S acknowledges the login request. If unreasonable, refuses the login request.

Step 3: S computes A_i and C_1, where

$$A_i = h(ID_i \oplus x)$$
$$C_1 = h(T \oplus A_i)$$

If $C_1 = C_1^*$, an inconsistency occurred, refuse the login request.

4.4 Password Change Phase

In this phase, U_i changes his PW_i.

Step 1: U_i puts the smart card into the card reader, and input personal account number ID_i^*, current password PW_i^*, the number R^*, a new password PW_i', and another randomly chosen number R'.

Step 2: Smart card computes G^* and V^*, and then compares it with V. If equivalent, goes to the next step; otherwise, stop.

$$G^* = h(PW_i^* \| R^*)$$
$$V^* = h(ID_i^* \oplus G^*)$$

Step 3: Smart card computes a new value G', V' and B_i', where

$$G' = h(PW_i' \| R) \quad (14)$$
$$V' = h(ID_i^* \oplus G') \quad (15)$$
$$B_i' = B_i \oplus G \oplus G' \quad (16)$$

Step 4: The smart card uses V' and B_i' to replace old V and B_i, and store them.

5 SECURITY ANALYSIS OF OUR METHOD

In this section, we analyze the proposed method. Prove that our method can resist more kinds of attacks than that of Sun et al's method.

5.1 Privileged Insider's Attack

Recently, a lot of financial crimes against banks or enterprises are committed by insiders. This has become a serious problem. In the proposed method, as can be seen in Eq. (6), the message G is used to register to the server. It is the result of a hash function, where the input parameters are the personal password PW_i and random number R. Because of the strength of one-way hash function, the proposed algorithm can resist a PIA, as long as the user does not reveal his registration password.

5.2 Replay Attack

If the attacker sends the interceptive information $\{ID_i^*, C_1^*, T\}$ to the server, his login request will be

refused, because of the timestamp mechanism. Refer to Eq. (13), since C_1^* consists of A_i^* and T, the attacker must face the complexity of one-way hash function. That is to say, assume that the attacker replaces the conveyance time T with a false one, said $T^{\#}$, in the interceptive information, and pass it to the server. His conspiracy will be discovered, because he can not produce the value $C_1^{\#}$ corresponding to $T^{\#}$. Therefore, the proposed method also can resist the replay attack.

5.3 Impersonation Attack

The attacker has two major approaches to conduct the Impersonation attack. Firstly, he can steal the legal user's smart card, and input the password of guessing. According to Eq. (12), because we increase the mechanism of password authentication, whenever the attacker inputs wrong ID_i^*, PW_i^* and R^* values, he can't obtain the service of the smart card. Secondly, the attacker makes use of old messages to perform an intercept attack. Again, according to Eq. (1) and Eq. (13), he will have to resolve the difficult problem of one-way hash function. Moreover, he has to steal the secret information(x and G^*) from the user and the server. So, their attack will not succeed.

5.4 Guessing Password Attack

Similar to the above analysis, if the attacker wants to utilize some interceptive information { ID_i^*, C_1^*, T} to attack, then he must face the challenge of breaking a double-hash function. In addition, based on Eq. (10) and Eq. (12), if the attacker wants to obtain the secret of G^*, then he must face the problem of solving a one-way hash function. Even if the attacker gets the smart card, it is difficult to guess the correct values of PW_i and R by using the dictionary attack, because value R is chosen at random. So, the proposed method can resist the guessing password attack.

5.5 Denial of Service Attack

We divide the denial of service attack into three phases, and discuss them one by one. Consider the login phase. Refer to Eq. (11), users can confirm the legitimacy of the input information (ID_i^*, PW_i^* and R^*) and transfer the message of login by himself. Then, consider the authentication phase. The server can distinguish the legitimacy of login information alone. Finally, consider the process of password changes phase. Refer to Eq. (11), users also utilize the smart card to verify the correctness of the input information (ID_i^*, PW_i^* and the number R^*), and offer change service of register password. As can be seen, all these phases require only local operations, no message exchanges between the smart card and the server are required, and thus it can resist the denial of service attack.

6 CONCLUSION

In this paper, a remote user authentication scheme using smart card base on one-way hash function was proposed. This method provides an enhancement protocol to Sun et al's scheme, which has been shown insecure. In their method, a privileged insider can impersonate the lawful user to login remote server. We not only resolve this security problem, but also increase the verification efficiency of the password.

ACKNOWLEDGEMENTS

This research was partially supported by the National Science Council, Taiwan, R.O.C., under grant NSC95-2220-E-218-002.

REFERENCES

Eun-Jun Yoon, Kee-Young Yoo, 2007. Comments on Modified User Friendly Remote Authentication Scheme with Smart Cards. *IEICE TRANS. COMMUN.*

Da-Zhi Su , Ji-Dong Zhong, Yu Sun, 2005. Weakness and improvement on Wang–Li–Tie's user-friendly remote authentication scheme. *Applied Mathematics and Computation* 170.

Narn-Yih Lee, Yu-Chung Chiu, 2005. Improved remote authentication scheme with smart card. *Computer Standards & Interfaces*.

Wei-Chi KU, Hsiu-Mei CHUANG, Maw-Jinn TSAUR, 2005. Vulnerabilities of Wu-Chieu's Improved Password Authentication Scheme Using Smart Cards. *IEICE TRANS. FUNDAMENTALS.*

Min-Shiang Hwang, Jung-Wen Lo, Chi-Yu Liu, Shu-Chen Lin, 2005. Cryptanalysis of a User Friendly Remote Authentication Scheme with Smart Card, *Journal of Applied Sciences.*

Kuo-Feng Hwang, I-En Liao, 2005. Two attacks on a user friendly remote authentication scheme with smart cards, *ACM SIGOPS Operating Systems Review*.

Chien-Lung Hsu, 2005. A user friendly remote authentication scheme with smart cards against

impersonation attacks, *Applied Mathematics and Computation*.

Yingjie Wang, J.H. Li, L. Tie, 2005. Security analysis and improvement of a user-friendly remote authentication protocol, *Applied Mathematics and Computation*.

Shyi-Tsong Wu, Bin-Chang Chieu, 2004. A note on a user friendly remote authentication scheme with smart cards. *IEICE Trans. Fundamentals*.

Chou-Chen Yang, Ren-Chiun Wang, 2004. Cryptanalysis of a user friendly remote authentication scheme with smart, *Computers & Security*.

Shyi-Tsong Wu, Bin-Chang Chieu, 2003. A User Friendly Remote Authentication Scheme with Smart Cards. *Computer and Security*.

Hung-Min Sun. 2000. An efficient remote use authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics.*