Lee-Chiu 使用智慧卡之遠端身份認證法的改良

Improvement of Lee-Chiu's Remote Authentication Scheme with Smart Cards

Hwang, Shin-Jia
Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.
e-mail : sjhwang@mail.tku.edu.tw

Chen, Wen-Yi
Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.
e-mail : chenwy319@yahoo.com.tw

摘要

遠端身份認證法在網際網路上，對於協助伺服器認證遠端使用者，扮演相當吃重的角色。學者 Lee 和 Chiu 提出他們的遠端身份認證法，以改良先前的遠端身份認證法。不幸地，本文提出對 Lee 和 Chiu 的遠端身份認證法之攻擊，說明他們的方法會遭受偽造攻擊與拒絕服務攻擊。為了克服上述的安全缺失，提出我們的遠端身份認證改良法。在我們的改良法中，使用者可以安全地且自由地挑選與更換自己的通行碼。

關鍵詞：遠端身份認證，**智慧卡**

Abstract

Remote authentication schemes play an important role to help server authenticate remote users in the Internet. Lee and Chiu proposed their remote authentication scheme to overcome some security problem in previous remote authentication schemes. Unfortunately, in this paper, some attacks are proposed to show that Lee and Chiu's scheme is vulnerable under the forgery attack and the denial of service attack. To conquer these security problems, our improved scheme is also proposed. So our scheme is more secure than Lee and Chiu's scheme. In our scheme, users freely and securely choose and change their passwords.

1. Introduction

Owing to the prosperous development of the internet, the demand of remote access between servers and clients is more necessary. Remote authentication becomes an important subject of security, for remote access systems through insecure channels. The original password authentication scheme uses a pair of identity number ID and secret password PW to authenticate user's identity. Once a valid user submits his/her correct ID and PW, the remote server provides the service of access. However, password authentication schemes suffer replay attacks. By replay attack, an intruder easily impersonates a legal user to log in the remote server by resubmitting previously intercepted ID and PW through the internet.

To conquer the replay attack, Lamport [5] proposed a remote password authentication scheme using password table in 1981. However, Lamport's scheme suffers from the modification attack on password tables and the protecting and maintaining cost of password tables [4].

Thus, many proposed remote password authentication schemes [1-4, 8, 10] use smart cards to avoid the modification attack on password tables. In 2000, Hwang and Li [4] proposed their scheme using smart cards to withstand the replay attack and modification attack. But, in their scheme, users cannot freely choose and update their passwords. To provide the function of choosing and updating password freely by users, Wu and Chieu [9] proposed a user-friendly remote authentication scheme with smart cards. Lee and Chiu [6] pointed out that Wu-Chieu scheme suffers forgery attack if an attacker got a transmitted valid log sent from smart card to server. To remove the forgery attack, Lee and Chiu also proposed their improved scheme. In this paper, some attacks are proposed to show that Lee-Chiu's scheme is vulnerable to the forgery attack and denial of service attack. To overcome these security flaws, our improved scheme is proposed.

In the next section, Lee-Chiu's scheme is reviewed first. Then our attacks on Lee-Chiu's scheme are given in Section 3. Our improved scheme is proposed in Section 4. Section 5 is the security analysis and discussions. The conclusions are given in the last section.

2. Review of Lee-Chiu's Remote Authentication Scheme with Smart Card

Lee-Chiu's remote authentication scheme [6] is briefly reviewed here. In Lee-Chiu's scheme, the server chooses a large public prime p, a public generator g in GF(p) and a public one-way hash function h(.). Then the server randomly determines an integer x as the system secret key. Their scheme consists of four phases: Registration phase, log in phase, authentication phase and password change phase.

Registration Phase

The user U_i with a unique identifier ID_i wants to make an application to the server through secure channels. The user U_i randomly choose his/her password PW_i. Then he/she submits ID_i and PW_i mod p to the server. Upon receiving the registration request, the server performs the following steps:

Step 1: Compute A_i= h(ID_i, x).

Step 2: Compute B_i= $g^{A_i \times h(PW_i)}$mod p.

Step 3: Store the information {ID_i, A_i, B_i, h(.), p, g } into the smart card.

Finally, the server gives the smart card to the user U_i through secure channels.

Log in phase

The user U_i inserts the smart cad into the smart card reader and keys in the password PW^*_i. Then the smart card performs the following steps.

Step 1: Compute B^*_i= $g^{A_i \times h(PW^*i)}$ mod p

Step 2: Compare B^*_i and B_i. If the equation $B^*_i \neq B_i$ holds, stop the process.

Step 3: compute Z_i= $B^*_i \times A_i$ mod p.

Step 4: Compute C_1 = h(T$\oplus$$B^*_i$), where T is the current time of the input device.

Step 5: Send the message m= {ID_i, Z_i, T, C_1}to the remote server. Here T denotes the time that the smart card sends m to the remote server.

Authentication Phase

After receiving the message m at the time of T', the remote server executes the following steps:

Step 1: Check the validity of ID_i. If the ID_i is invalid, reject U_i's log in request.

Step 2: Check whether or not the ΔT= T'-T is reasonable time difference. If ΔT is not reasonable, reject the log in request.

Step 3: Compute A_i= h(ID_i, x) and C_1*=h(T$\oplus$(Z_i/A_i mod p)).

Step 4: Compare C_1* and C_1. If the equation of C_1* = C_1 holds, the log in request is accepted.

Password change phase

Suppose that the user U_i wants to change his/her password PW_i into PW'_i. The user U_i relogin the server. Then the server will compute a new B'_i = $g^{A_i \times h(PW'i)}$ mod p and write B'_i back into U_i's smart card replace the original B_i. Then the user can use the new password to log in the server.

3. Attacks on Lee-Chiu's scheme

Some security flaws of Lee-Chiu's scheme are described here. In the log in phase of Lee-Chiu's scheme, the user U_i sends the message m= {ID_i, Z_i, C_1, T} to the remote server through the public channel. Suppose that an attacker intercepts m= {ID_i, Z_i, C_1, T} and m'= {ID_i, Z'_i, C'_1, T'} for two different used passwords PW_i and PW'_i, respectively. When the attacker obtains passwords PW_i and PW'_i such that gcd(p-1,(h(PWi)- h(PW'i)))=1, he/she may obtain the secret item A_i by the following steps.

Step 1: Compute $Z_i/Z'_i \equiv B_i/B'_i \equiv g^{A_i \times (h(PW_i)- h(PW'_i))}$ (mod p).

Step 2: Compute $g^{A_i} \equiv (g^{A_i \times (h(PW_i)- h(PW'_i))})^{(h(PW_i)- h(PW'_i))^{-1} \text{ (mod p-1)}}$ (mod p) since gcd(p-1, (h(PWi)- h(PW'i)))=1.

Step 3: Compute B_i= $g^{A_i \times (h(PW_i))}$ mod p.

Step 4: Compute A_i= Z_i/B_i mod p.

Then the attacker can easily forge the message m to log in the server. The attacker first randomly selects B''_i, and computes Z''_i= $B''_i \times A_i$ mod p and C''_i= h($B''_i$$\oplus$T''). Then the message m''= {ID_i, Z''_i, C''_1, T''} can be used to log in to server by impersonating the user U_i because C_1*=h(T''$\oplus$(Z''_i/A_i mod p))= h($B''_i$$\oplus$T'')= C''_i.

Another security flaw is caused by the password change process. Lee-Chiu’s scheme is vulnerable under the denial of services attack [7]. In order to change passwords, the user has to relogin the server. The user submits the new password to the server. Then the server writes the new item B'_i to replace the old one B_i on the smart card. Because the server needs to write B'_i back to the smart card of the user, the user has to authenticate the server. However, Lee-Chiu’s scheme does not provide the mutual authentication, so an attacker easily impersonates the server to write an invalidated B'_i on smart card. Then the user cannot log in the server forever to access the server’s services.

4. Our New Scheme

Our improvement is proposed to withstand the attacks mentioned in previous section. The system parameters are stated first. The server chooses two large primes p and q with q|p-1, and a generator $g \in Z^*_p$ of order q as system parameters. The server also needs a one-way hash function h(•). Then the server determines a random integer $x \in Z^*_q$ as the system secret key. The new scheme is also divided into four phases: Registration phase, log in phase, authentication phase and password change phase.

Registration Phase

The user U_i makes an application to the server by secure channels. The user U_i randomly chooses his/her password PW_i and computes $R_i = g^{h(PW_i)}$ mod p. Then he/she submits his/her unique identifier ID_i and R_i to the server. After receiving ID_i and R_i , the server performs the following steps.

Step 1: Compute $A_i = h(ID_i, x)$.

Step 2: Compute $E_i \equiv g^{A_i^{-1}}$(mod p) and $B_i \equiv (R_i)^{A_i^{-1}} \equiv g^{A_i^{-1} \times h(PW_i)}$ (mod p).

Step 3: Store the information {p, q, g, h(.), B_i, E_i, R_i} into the smart card of the user U_i.

On Step 2, the server needs to compute A_i^{-1} mod q when A_i^{-1} and q are relatively prime. Since q is a large prime number, the probability that A_i and q are not relatively prime is negligible.

Log in phase

The user U_i inserts the smart card into the smart card reader and gives the password PW_i*. Then the smart card performs the following steps.

Step 1: Compute $R_i^* = g^{h(PW_i^*)}$ mod p

Step 2: Compare whether or not the equation $R_i^* = R_i$ hold. If the equation holds, execute the next step.

Step 3: Select a random integer $r \in Z^*_q$.

Step 4: Compute $C_2 = B_i^r$ mod p= $g^{rA_i^{-1} h(PW_i)}$ mod p and $C_1 = h(R_i^r \bmod p, T)$. Here T denotes the time that the smart card sends m= {ID_i, T, C_1, C_2} to the remote server.

Step 5: Send the remote server the message m= {ID_i, T, C_1, C_2}.

To speed up the log in process, the pre-computation is adopted. Before the remote server gives the response, the smart card selects another random integer $r' \in Z^*_q$, computes and stores $C'_2 = B_i^{r'}$ mod p= $g^{r'A_i^{-1} h(PW_i)}$ mod p and $R_i^{r'}$ mod p on the smart card for the next log in process. Then the log in process can be speeded up by pre-computing the items C'_2 and $R_i^{r'}$ mod p.

Authentication Phase

After receiving the message m at the time of T', the remote server executes the following steps:

Step 1: Check the validity of ID_i. If the ID_i is invalidated, U_i’s log in request is rejected.

Step 2: Check whether or not the $\Delta T = T' - T$ is reasonable time difference. If ΔT is not reasonable, reject the log in request.

Step 3: Compute $A_i = h(ID_i, x)$ and $C_1^* = h(C_2^{A_i} \bmod p, T)$.

Step 4: Compares C_1* and C_1. If the equation $C_1^* = C_1$ holds, accept the log in request.

Password change phase

Suppose that the user U_i wants to change his/her password PW_i into PW'_i. First, the user gives his/her current password PW_i* and the new one PW'_i, the smart card of user U_i executes the following steps:

Step 1: Compute $R_i^* = g^{h(PW_i^*)}$ mod p

Step 2: Compare whether or not the equation $R_i^* = R_i$ holds. If the equation holds, go next step.

Step 3: Compute $R'_i = g^{h(PW'_i)}$ mod p.

Step 4: Compute $B'_i = E_i^{h(PW'_i)}$ mod p=$g^{A_i^{-1} \times h(PW'_i)}$ mod p .

Step 5: Store the R'_i and B'_i to replace the original R_i and B_i.

5. Security Analysis and Discussions

The security of our proposed scheme is based on the discrete logarithm hard problem and a one-way hash function. In our scheme, smart cards are tamper resistant to protect the secret data on smart cards. The m = {ID_i, T, C_1, C_2} is the only message may be easily obtained by attackers through the public channel.

The security analysis of our proposed scheme is given below.

(1) It is hard for the attacker to derive the A_i from the message m = {ID_i, T, C_1, C_2}. A_i is protected by the discrete logarithm problem for C_2= g $^{rAi^{-1}h(PWi)}$ mod p. The password PW_i is protected the discrete logarithm problem and one-way hash functions.

(2) The server's secret key x is secure. To get the server's secret key x, the attacker must know the value of A_i at first. As the above cryptanalysis, it is very hard to derive A_i. Even though the attacker got A_i = h(ID_i, x), the system secret key x is still protected by the one-way hash function.

(3) The transmitted message m cannot be forged in our scheme. Without knowing the user's password PW_i and A_i = h(ID_i, x), no one can forge a valid pair {C_1, C_2} in the message m= {ID_i, T, C_1, C_2} because C_2= $g^{rAi^{-1}h(PWi)}$ mod p and C_1= h($g^{h(PWi)r}$ mod p, T)= h(C_2^{Ai} mod p, T).

(4) Our scheme is secure against the replay attack. By performing replay attacks, the attacker uses an old valid message m = {ID_i, T, C_1, C_2} to log in the remote servers. The attack has to replace T with the new time T' in order to get a reasonable ΔT. Fortunately, the attacker is still found out in the authentication phase because he/she cannot forge C_1' and C_2' for the new time T'.

(5) Our scheme is secure against the denial of service attack. In our scheme, without the valid password, no one can log in the remote the items C_1 and C_2 in m to achieve the goal of authentication. The server uses the secret key x and C_2 to count C_1*, then compares it to the C_1. without any user authentication message stored in the server, the intruder can't modify it on the server.

(6) Without knowing the user's password PW_i, no one can log in the server, although the smart card is stolen. In the log in phase, anyone has to give the password PW_i^* passing the verification equation R_i^*= $g^{h(PW^*i)}$ mod p. Without knowing the user's password PW_i, the attacker has to guess the correct password PW_i. Without the guess of the correct passwords, the attacker must forge m to log in the server. Due to the above analysis, this is also impossible to forge m. So the attack cannot log in the server.

(7) Our scheme is secure against password guessing attacks. Consider the on-line password guessing attack. Although C_2= $g^{rAi^{-1}h(PWi)}$ mod p contains the h(PW_i), C_2 is randomize by the random number r, so the attack has to guess PW_i and r at the same time. Since r is a random number, the attack cannot distinguish the correct and incorrect guessing on passwords by the log in results. By the same reason, C_2 cannot be used for the off-line password guessing attack. Because our smart cards are tamper-resistant, so the smart cards cannot be used in off-line password guessing attack. Therefore our scheme is secure against password guessing attack.

6. Conclusions

In this paper, some attacks are proposed to show that Lee-Chiu's scheme is vulnerable under the forgery attack and the denial of service attack. To conquer these flaws of Lee-Chiu's scheme, our improved remote authentication scheme is proposed. Except preserving the properties of a friendly authentication scheme, our scheme is more secure than Lee-Chiu's scheme. Moreover, in our scheme, users freely choose and change their passwords without causing security flaws.

References

[1] C. C. Chang and W.Y. Liao, "A remote password authentication scheme based on ELGamal's signature scheme," Computer and Security, 13 (2), 1994, pp. 137-144.

[2] C. C. Chang and T.C. Wu, "Remote password authentication with smart cards," *IEE Proceedings. Part E*, 138, 1991, pp. 165-168.

[3] M.S. Hwang, "A remote password authentication scheme based on the digital signature method," *International Journal of Computer Mathematics*, 70, 1999, pp. 657-666.

[4] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, 46 (1), 2000, pp. 28-30.

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

[6] N.Y. Lee and Y.C. Chiu, “Improved remote authentication scheme with smart card,” *Computer Standards and Interfaces*, 27, 2005, pp. 177-180.

[7] C.L. Lin, H.M. Sun and T. Hwang, “Attacks and solutions on strong-password authentication,” *IECIE Transactions on Communications*, E84-B (9), 2001, pp. 2622-2627.

[8] T.C. Wu, “Remote log in authentication scheme based on a geometric approach,” *Computer Communications*, 18(12), 1995, pp. 959-963.

[9] S.T. Wu and B.C. Chieu, “A user friendly remote authentication scheme with smart cards,” *Computer and Security*, 22 (6), 2003, pp. 547-550.

[10] W.H. Yang and S.P. Shieh, “Password authentication schemes with smart cards,” *Computers and Security*, 18 (8), 1999, pp. 727-733.