Comments on A Remote User Authentication Scheme Using Smart Cards with Forward Secrecy

Yi-Hwa Chen[1], Jinn-Ke Jan[2]
[1]*Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan 402*
[2]*Institute of Computer Science, National Chung Hsing University,Taichung, Taiwan 402*
Corresponding E-mail: jkjan@cs.nchu.edu.tw

Abstract- *Hwang and Li proposed a new remote user authentication scheme, based on ElGamal's cryptosystem, using smart card in 2000. However, Chan and Chang and Shen, Lin and Hwang first and last pointed out different type of masquerade attacks on this scheme. In 2003, Awasthi and Lal (Shortly, A-L) presented a new scheme to overcome these attacks. In addition, they claimed that the scheme with the property of forward secrecy. Lee et al. showed that the A-L scheme is incorrect. However, their analysis was not complete. Kumar proposed an attack to A-L scheme via the previously registered ID or by creating a new ID. Unfortunately, his attack is meaningless since the A-L scheme cannot work. In this paper, we will discuss the later both. In addition, we will show that the A-L scheme is vulnerable to the online password guessing attack even if it can work.*
By increasing a verification mechanism to the login phase, a cardholder needn't worry about the problem of masquerading usage by this attack if he loses his smart card by accident.

Keywords: Forward Secrecy, Authentication, Smart Card, Password.

1. Introduction

For obtaining various services of a remote server, a legal user must send his/her password to the server for authenticating his/her identification. To prevent from sending a clear password to the server, message digest function (e.g. hash function) may be used. Therefore, the server must maintain a hashed password table in order to verify the legitimacy of a user. However, if an intruder can break into the server then he has an opportunity to modify or steal the contents of the table. Thus, the modification or stolen-verifier attack succeeds. The problem has been solved by several schemes proposed by some researchers [5-8]. In their schemes, the password table is no longer required in the server.

Recently, by using the characteristics of smart card with the capabilities of computing and storing, many researchers [1][9-13] have proposed several remote user authentications without the password tables. Therefore, smart card now has been widely used in remote password authentication schemes. Hwang and Li [1] proposed a remote user authentication scheme based on Elgamal's cryptosystem in 2000. However, their scheme is insecure. Without through the registration phase, Chan and Chang [2] proposed a successful masquerade attack. The attack points out that a legal user can easily create a valid pair of (ID, PW) by itself to pass the authentication phase in the server. In 2003, Shen, Lin and Hwang [3] proposed another masquerade attack. Through the registration phase, a legitimate user can compute some other user's password. In addition, Shen, Lin and Hwang proposed a modified scheme to overcome the weakness. Lately, Awasthi and Lal [4] pointed out that Shen, Lin and Hwang's modified scheme without forward secrecy. Therefore, they presented a new scheme to provide the property of forward secrecy. However, Lee et al. [14] showed that the A-L scheme is incorrect. They analyzed that the server cannot compute the user's password such that the server cannot perform the verification procedure in the authentication phase. Unfortunately, their analysis was not complete enough. Kumar [15] proposed an attack to A-L scheme via the previously registered ID or by creating a new ID. In this paper, we will discuss the security of the A-L scheme completely and show that Kumar's attack is meaningless since the A-L scheme cannot work. In addition, we will show that the A-L scheme is vulnerable to the online password guessing attack even if it can work. By increasing a verification mechanism to the login phase, a cardholder needn't worry about the problem of masquerading usage by this attack if he loses his smart card by accident.

In next section, a brief review of the A-L scheme is provided. Section 3 discusses the security of A-L scheme. Finally, a conclusion is given.

2. Review of The A-L Scheme

There are three entities: user, server and time stamping authority (TSA) in A-L scheme. User is who wants to access the server and obtains its services. Server is responsible for the authentication of the legitimacy of a user. TSA is a trusted authority that can provide a current time stamp whenever required. Their scheme is composed of four phases: the initial phase, the registration phase, the login phase and the authentication phase. A new user must register to the server first. After the server identifies the user, it will issue a password and a smart card with some relative information to the user over a secure channel. Whenever the user wants to login the server, he inserts his smart card to the terminal and keys in his password. The server will give the user services after he has passed the authentication. A detailed description presents as follows:

Initial Phase:

The server generates the following parameters:

p : a large prime number

$h(.)$: a one-way function

x_s : a secret key of the server

Registration Phase:

A user U_i wants to access the server, he submits his ID_i to it. The server computes

$$m = h(ID_i \oplus T), \qquad (1)$$

where T denotes the time stamp given by TSA, and

$$PW_i = m^{x_s} \bmod p. \qquad (2)$$

The server stores the parameters $(h(.), p, T)$ to a smart card then issues it with a password PW_i to the user.

Login Phase:

User U_i inserts his smart card to the terminal and keys in his ID_i and PW_i for login to the server. The smart card performs the following steps:

1.Choose a random number r.

2.Compute $m = h(ID_i \oplus T)$, and $C_1 = m^r \bmod p$.

3.Compute $t = h(T_c \oplus PW_i) \bmod p - 1$, here T_c is the current time.

4.Compute $M = ID_i^{\,t} \bmod p$.

5.Compute $C_2 = M(PW_i)^r \bmod p$.

6.Sends the message $C = (ID_i, C_1, C_2, T_c)$ to the server.

Authentication Phase:

Upon receiving the message C at time T_s, the server works as follows.

1.Check the validity of the format of ID_i.

2.Test whether it is a reasonable time interval between T_c and T_s.

3.Verify whether the following equation holds:

$$C_2(C_1^{\,x_s})^{-1} = (ID_i)^{h(T_c \oplus PW_i)} \bmod p. \qquad (3)$$

3. Security Analyses

Forward Secrecy: If long-term private keys of one or more entities are comprised, the session keys (password) used in the past should not be recovered.

In [14], Lee et al. only take the parameter T into their consideration to show that the A-L scheme cannot work. However, a parameter m is with the same situation in analyzing the security of the A-L scheme. We discuss the security including both of the parameters T and m in section 3.1. Section 3.2 presents Kumar's attack and demonstrates it to be unworkable. Section 3 shows that the A-L scheme is vulnerable to the online password guessing attack even if it can work.

3.1 The A-L scheme cannot work

The server can obtain a time stamp T from TSA to compute m and PW_i from equation (1) and (2) respectively when user U_i registers to the server. However, the server doesn't store T or m in its database. Therefore, in authentication phase, the server without T or m cannot compute a correct password PW_i of the user to verify whether the equation (3) holds or not.

Furthermore, we discuss and analyze two conditions to mend the previous leak in the A-L scheme. For providing T or m to compute the user's password PW_i, the server may store T or m in its database. However, that falls into the same situation as storing a password file in server's database and is vulnerable for modification or stolen-verifier attack. Another condition is that the user sends a message C including T or m to the server in login phase. However, adversary can collect the user's message C by eavesdropping in advance then compute the user's password PW_i when server's secret key x_s is revealed.

Generally, it is a better method by using ephemeral keys to obtain the forward secrecy. The normal method for getting one ephemeral key is to provide a random number as the parameter of session key (password) generating algorithm. Unfortunately, in A-L scheme, the necessary parameters, timestamp T and user's identity ID_i, for computing some user's password PW_i are all fixed values.

3.2 Kumar's attack

According to the property of forward secrecy, Kumar assumed that three conditions were taken into conditions: (1) an attacker obtains the secret key x_s of the server, (2) the server doesn't store the user's ID and PW, and (3) the messages for authentication are passing over an insecure channel. Under the three assumptions, Kumar claimed that the attacker could forge every user's password via the previously registered ID or by creating a new ID. The attacker randomly chooses a timestamp T_B to forge the password. The forged password is as follows:

$$PW = h(ID \oplus T_B)^{x_s} \bmod p \, .$$

By the assumption (2), the server must compute the user's password PW to perform the verification procedures in authentication phase. However, the server cannot compute the user's password without obtaining the time stamp T_B. Therefore, his attack cannot work. Any modification to make the attack be useful will fall into the same situation as the discussion in section 3.1.

3.3 Online password guessing attack

Assumed that the A-L scheme is able to work after being modified. However, it is still vulnerable to the online password guessing attack. Even if this kind attack is easily to be found and prevented by the smart server, a small modification for the scheme may avoid this threat efficiently. We describe the details as follows.

If any cardholder loses his smart card by accident, he must worry about the impersonation attack by online password guessing since there is not any verifying mechanism in login phase. Therefore, an adversary who obtains the smart card can try any password to login with the AS. If the login request succeeds on the trial of some time, then the password keyed in that time is the correct password.

To prevent from this attack, in the login phase, it is necessary to provide an authentication equation to verify the password keyed in. If the password keyed in by some user is incorrect then the smart card stops and registers the error at the same time. If the error times collected have been over a threshold value, the smart card will destroy itself. The improvement will solve the problem of the online password guessing attack by using other's smart card without his agreement.

4. Conclusion

Throughout the discussions and analyses in section 3, we conclude that the A-L scheme cannot work since their scheme cannot perform the authentication equation without the time stamp T or message m. Even though their scheme makes some modifications to obtain T or m, their scheme still provides without forward secrecy. The reason is that if the server's secret key is compromised, the adversary can easily obtain the information stored in the server or passed from the channel to compute the previous passwords. In addition, adding a verification mechanism to check the password keyed in by the user will improve the security of the smart card.

References

[1] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, No. 1, pp. 28 -30, February, 2000.

[2] C.K. Chan and L.M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, Vol. 46, pp. 992-993, 2000.

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

[4] A.K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Transaction on Consumer Electronics*, Vol. 49, No. 4, pp. 1246-1248, November, 2003.

[5] T. Hwang, Y. Chen and C. S. Laih, "Non-interactive password authentications without password tables," *IEEE Region 10 Conference on Computer and Communications, IEEE Computer Society*, pp. 429-431, 1990.

[6] H. Y. Chien, J. K. Jan and Y. M. Tseng, "A modified remote login authentication scheme based on geometric approach," *The Journal of System and Software*, Vol. 55, pp. 287-290, 2001.

[7] G. Horng, "Password authentication without using password table," *Information Processing Letters*, Vol. 55, 247-250, 1995.

[8] J. K. Jan and Y. Y. Chen, "Paramita wisdom' password authentication scheme without verification tables," *The Journal of Systems and Software*, Vol. 42, pp. 45-57, 1998.

[9] T. C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communications*, Vol. 18, No. 12, pp. 959-963, 1995.

[10]C. C. Chang and W. Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," *Computers and Security*, Vol. 13, No. 2, pp.137-144, April 1994.

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

[12]W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computer & Security*, Vol. 18, No. 8, pp. 727-733, 1999.

[13]S. T. Wu and B. C. Chieu, "A user friendly remote authentication scheme with smart cards," *Computer & Security*, Vol. 22, No. 6, pp. 547-550, 2003

[14]S.U. Lee, H.S. Kim and K.Y. Yoo, "comment on 'A remote user authentication scheme using

smart cards with forward secrecy,'" *IEEE Transaction on Consumer Electronics*, Vol. 50, No. 2, pp. 576-577, May, 2004.

[15]M. Kumar, "Some remarks on a remote user authentication scheme using smart cards with forward secrecy," *IEEE Transaction on Consumer Electronics*, Vol. 50, No. 2, pp. 615-618, May, 2004.