International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 7 (2017) pp. 1222-1226
© Research India Publications. http://www.ripublication.com

Security Weakness of Efficient and Secure Smart Card Based Password Authentication Scheme

Younsung Choi
Department of Cyber Security, Howon University,
Impi-Myeon, Gunsan-Si, Jeonrabuk-Do 54058, Korea.

Abstract

After Lamport first proposed password base authentication scheme, various authentication schemes were studied and remote user authentication schemes using smart cards have been widely used with the development of Internet network technologies. Li et al. analyze Chen et al.'s authentication scheme and found the security vulnerabilities of Chen et al.'s scheme such as forward secrecy and the wrong password login problem, and proposed an a new user password authentication scheme based on smart card. However, Liu et al. point out that Li et al.'s scheme still had security weakness such as man-in-the-middle attack and an insider attack, and then Liu et al. proposed an efficient and secure smart card based password authentication scheme. This paper reviews Liu et al.'s authentication and point out that it has security weakness such as off-line password guessing attack, smart-card loss attack, no perfect forward secrecy, and no anonymity.

Keywords: Cryptanalysis, Security analysis, Smart card based password authethentication

INTRODUCTION

With the rapid growth of Internet technology, smart card based remote user authentication schemes have been studied. To identify a legitimate user even over an insecure channel[1,2], Firstly password-based remote authentication scheme was proposed. Lamport published his research in 1981[3]. However, various researcher explain that Lamport's scheme has a serious security weakness because he uses stored verifier table on a remote authentication system so the verifier table risks being modified by an attacker. And Lamport's scheme has a high maintenance cost on verifier table, so it needs many time to store all encrypted secret passwords against the threat of disclosure.

Hwang and Li explained the weakness of Lamport's scheme and proposed an ElGamal public-key encryption system based authentication scheme to solve the problem of Lamport's scheme. Hwang and Li proposed the scheme[4], which is no need to maintain a verifier table to achieve remote user authentication. To reduce the capacity of cryptosystems, Sun proposed an authentication scheme to enhance the performance efficiency of Hwang and Li's scheme using one-way hash operations. However, Lamport's scheme and Hwang and Li's scheme cannot provide freely password choice and mutual authentication. Using smart card on authentication scheme can solve the problem of maintaining the server's verifier table because smart card has tamper-resistant properties. smart card contained all kinds of stored secret information and it is issued by the server to legal user. So only the regular user can get a smart card in a smart card based authentication system. Various studies on smart cards have investigated and then most of remote authentication schemes use smart card to enhance the security[5,6]. Xu et al. proposed a novel and secure user authentication scheme In 2009 [7] but Sood et al. [8] indicates that Xu et al.'s scheme has various weaknesses and so they proposed security enhanced authentication schemes. Chen et al. [9] found the vulnerability of Sood et al.'s schemes and Chen et al. proposed a more secure authentication scheme to solve the vulnerability of Sood et al.'s schemes. However Li et al. [10] found the weakness of Chen et al.'s scheme and proposed a password and smart card based user authentication scheme. Liu et al. point out the vulnerability of Li et al.'s authentication scheme such as man-in-the-middle attack and an insider attack. And they explain computational inefficiency of Li et al.'s authentication scheme and propose an efficient and secure smart card based password authentication scheme to solve Li et al.'s security vulnerability. Liu et al.'s scheme[11] has better computational efficiency comparing previous schemes. Moreover Liu et al. claimed that their scheme provide mutual authentication, session key agreement, freely chosen and exchanged password, a man-in-the-middle attack, an insider attack, a replay attack, perfect forward secrecy, and known-key security. But this paper finds out that Liu et al.'s scheme has various vulnerabilities such as off-line password guessing attack, smart-card loss attack, no perfect forward secrecy, no anonymity. This paper is organized as follows. In Section 2, this paper explains the Liu et al.'s An efficient and secure smart card based password authentication scheme. In Section 3, this paper explain how Liu et al.'s authentication scheme be exposed on vulnerabilities. In Section 4, this paper presents our conclusions.

REVIEW OF LIU ET AL.'S AUTHENTICATION SCHEME

To overcome weaknesses of Li et al.'s authentication, Liu et al. propose smart card based password authentication scheme. Liu et al.'s proposed scheme consists of four phases: (1) The registration phase; (2) the login phase; (3) the authentication phase; and (4) the password change phase. Liu et al. proposed scheme can achieve mutual authentication and users can freely choose and change their passwords. Liu et al. prove that this proposed scheme can be secure on various types of attack, such as a man-in-the-middle attack, insider attack, and replay attack. In the following, This section describes Liu et al.'s scheme in detail[11].

Registration Phase

Before starting Liu et al.'s authentication scheme, the server S selects the master secret key x and a one-way hash function $h(\cdot)$. The registration phase is depicted in Figure 1.

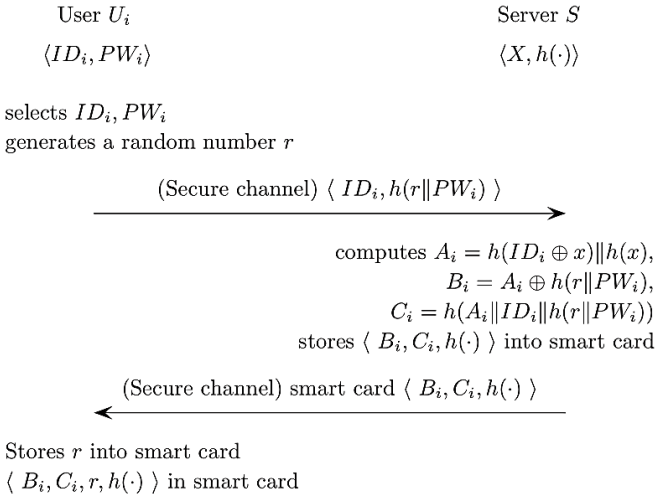

Figure 1. Liu et al.'s Registration Phase

(1) First, The user U_i selects his/her identity ID_i , password PW_i , and a random number r, and then computes h($r \| PW_i$). U_i submits { ID_i , h ($r \| PW_i$) } to the server S for registration over a secure channel.

(2) Then the server S computes the following parameters as follows;

$$A_i = h\ (ID_i \oplus x\ ) \| h(x),$$

$$B_i = A_i \oplus h(\ r \| PW_i\ ),$$

$$C_i = h\ (A_i \| ID_i \| h(\ r\ \| PW_i\ )).$$

(3) The server S stores the data { B_i , C_i , h(·) } on a new smart card and issues the smart card to the user U_i over a secure channel.

(4) The user U_i stores the random number r into the smart card.

Login Phase

This phase is invoked whenever the user U_i wants to login to the server S. The login and authentication phases are shown in Figure 2. The steps of this phase are shown as follows; The steps of this phase are conducted as follows;

(1) The user U_i inserts his/her smart card into a card reader and inputs his/her identity ID_i and password PW_i .

(2) The smart card first computes two parameters as follows;

$$A_i = B_i \oplus \text{h}\ (\ r\ |\ |\ PW_i\ ),$$

$$C_i = \text{h}\ (A_i \| ID_i \| \text{h}(\ r \| PW_i\ )).$$

Then, the smart card examines whether C_i is equal to C_i . If the equation holds, the smart card continues to perform on next step; otherwise, the smart card terminates this session.

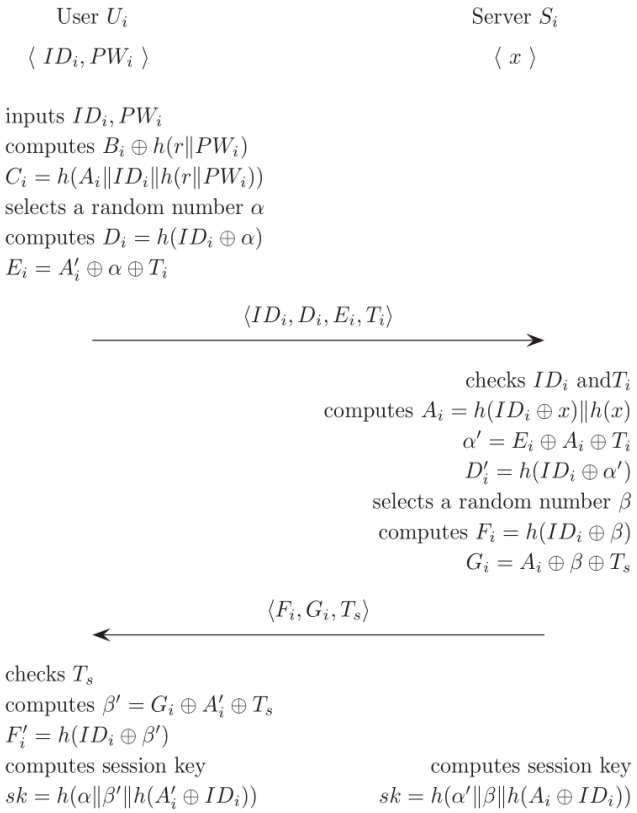

Figure 2. Liu et al.'s Login and Authentication Phase

(3) The smart card randomly selects a number a and computes the following parameters;

$$D_i = \text{h}\ (\ ID_i \oplus \alpha\ )\ ;$$

$$E_i = A'_i \oplus \alpha \oplus T_i\ .$$

(4) The smart card sends the login request message { ID_i , D_i , E_i , T_i } to the server S.

Authentication Phase

After completing this phase, the user U_i and the server S can mutually authenticate each other and establish a shared session key for the subsequent secret communication.

(1) The server S verifies whether ID_i is valid and checks the freshness of timestamps.

$$T'_i - T_i \leq \Delta T,$$

where T'_i is the time of receiving the login request message and ΔT is a valid time threshold. If both conditions are true, the server S continues to execute next step; otherwise, the server S rejects the login request.

(2) The server S computes the following parameters;

$$A_i = \mathrm{h}(ID_i \oplus x) \,||\, \mathrm{h}(x),$$
$$\alpha' = E_i \oplus A_i \oplus T_i,$$
$$D'_i = \mathrm{h}(ID_i \oplus \alpha').$$

Then, the server S compares whether D'_i equals D_i. If they are equal, the server S confirms that the user U_i is valid and the login request is accepted; otherwise, the login request is rejected.

(3) The server S randomly selects a number r and computes the following parameters as follows;

$$F_i = \mathrm{h}(ID_i \oplus \beta),$$
$$G_i = A_i \oplus \beta \oplus T_s.$$

(4) The server S sends the mutual authentication message $\{F_i, G_i, T_s\}$ to the user U_i.

(5) Upon receiving the message $\{F_i, G_i, T_s\}$, the user U_i checks the validity of T_s. If $T'_s - T_s \leq \Delta T$, where T's is the time of receiving the mutual authentication message, the user U_i continues to perform next step; otherwise, the user U_i terminates this connection.

(6) The user U_i computes the following parameters;

$$\beta' = G_i \oplus A'_i \oplus T_s,$$
$$F'_i = \mathrm{h}(ID_i \oplus \beta').$$

and then checks whether F'_i equals F_i. If they are equal, the validity of the server S is authenticated; otherwise, the session is terminated.

(7) The user U_i and the server S construct a shared session key as follows to ensure the secret communication;

$$sk = \mathrm{h}(\alpha \,||\, \beta' \,||\, \mathrm{h}(A'_i \oplus ID_i)) = \mathrm{h}(\alpha' \,||\, \beta \,||\, \mathrm{h}(A_i \oplus ID_i))$$

Password Change Phase

Liu et al.'s protocol allows users to freely update their passwords. The password Change Phase works as follows ;

(1) The user U_i inserts his/her smart card into a card reader, enters his/her old identity ID_i and password PW_i, and requests to change the password.

(2) The smart card computes the following parameters ;

$$A^*_i = B_i \oplus \mathrm{h}(r \,||\, PW_i),$$
$$C^*_i = \mathrm{h}(A^*_i \,||\, ID_i \,||\, \mathrm{h}(r \,||\, PW_i)).$$

and then checks whether C^*_i equals C_i that is stored in the smart card. If the equation holds, the user U_i submits the new password PW_i^{new} ; otherwise, the smart card rejects the password change request.

(3) The smart card computes the following parameters ;

$$B_{new} = A_i^* \oplus \mathrm{h}(r \,||\, PW_i^{new}),$$
$$C_i^{new} = \mathrm{h}(A_i^* \,||\, ID_i \,||\, \mathrm{h}(r \,||\, PW_i^{new})).$$

SECURITY WEAKNESS OF LIU ET AL.'S AUTHENTICATION SCHEME

This paper analyze Liu et al.'s authentication scheme and determine various security vulnerabilities including off-line password guessing attack, smart-card loss attack, no perfect forward secrecy, and no anonymity.

Off-line Password Guessing Attack

Kocher et al. and Messerges[12] et al. explain that various information stored in smart cards could be extracted by physically monitoring its power consumption. So it is possible to say that if a user loses his or her smart card, all information in the smart card may be revealed to the attacker. In Liu et al.'s authentication scheme, the smart card stores important information for user login and authentication phase. Figure 3 describes the off-line password guessing attack of Liu et al.'s authentication.

Attacker gets ID_i in public communication

Attacker steals user U_i's smart card

Attacker obtains all information from smart card using physical monitoring

→ So attacker can gets ID_i, B_i, C_i, r, $h(\cdot)$

$C_i = h(A'_i \,||\, ID_i \,||\, h(r \,||\, PW_i))$

$A_i = B_i \oplus h(r \,||\, PW_i)$

→ $C_i = h(B_i \oplus h(r \,||\, PW_i) \,||\, ID_i \,||\, h(r \,||\, PW_i))$

Attacker know all formula's parameter except for PW_i

→ So attacker can executes off-line password attack and obtain PW_i

Figure 3. Off-line password guessing attack of Liu et al.'s authentication

The smart card for the user U_i stores B_i , Ci , r , h(·). Using smartcard stored information and ID_i, attacker can guess password PW_i. The attacker can easily get ID_i in public communication and then he steals user's smart card to find out user's password. By physical monitoring on smart card, the attacker can obtain all information on smart card. So the attacker can get ID_i , B_i , C_i , r , h(·) then, he compute the following formula ;

$C_i = \mathrm{h}(A'_i \| ID_i \| \mathrm{h}(r \| PW_i))$,

$A_i = B_i \oplus \mathrm{h}(r \| PW_i)$,

$\rightarrow C_i = \mathrm{h}(B_i \oplus \mathrm{h}(r \| PW_i) \| ID_i \| \mathrm{h}(r \| PW_i))$.

In C_i formula, the attacker know all parameter except for PW_i , so he can user's password PW_i by off-line password attack.

Smart-card Loss Attack

When an attacker gets or steals the user's smart card in Liu et al.'s scheme, he can login and authenticate to server S_i , and compute the session key sk between the user U_i and server S_i , so the attacker can impersonate the legitimate user. It is critical problem that the attacker can be authenticated with the server using user's smart card. Figure 4 describes the smart-card attack on Liu et al.'s scheme. As described 3.1, the attacker can illegally extract the secret values in user's smart card and get ID_i in public communication, then guess PW_i using off-line password guessing attack. So the attacker impersonate user U_i as following steps. The attacker inputs known ID_i and PW_i to user's stolen smart card and then smart card computes A_i , C_i , D_i , E_i using ID_i , PW_i , B_i , C_i , r, and generated α_{at} at (attacker's random number). Then, the attacker sends ID_i , D_i , E_i , T_i to server S but S cannot figure out that the message is made by the attacker. So server computes A_i , α' , D'_i , F_i , G_i and generates β, and then, server S send F_i , G_i , T_s to attacker. So the attacker can login and authenticate to server S, and he can compute $sk = \mathrm{h}(\alpha_{at} \| \beta' \| \mathrm{h}(A'_i \oplus ID_i))$, which is same to server S's session key sk.

Attacker gets ID_i in public communication

Attacker steals user U_i's smart card

Attacker obtains all information from smart card using physical monitoring

→ So attacker can gets PW_i using off-line password guessing attack.

Attacker computes A_i , C_i , D_i , E_i using ID_i , PW_i , B_i , C_i , r .

Attacker generated α_{at} and sends ID_i , D_i , E_i , T_i to server S

Server computes A_i , α' , D'_i , F_i , G_i

Server generates β' and sends F_i , G_i , T_s to the attacker

Attacker know all formula's parameter in $sk = \mathrm{h}(\alpha_{at} \| \beta' \| \mathrm{h}(A'_i \oplus ID_i))$

→ So attacker can authenticate with server and compute session key sk

Figure 4 Smart-card Loss Attack of Liu et al.'s authentication

No Perfect Forward Secrecy

When one of the long-term keys is compromised in the future, if session key derived from a set of long-term keys will not be compromised, then it is meant that perfect forward secrecy is provided. But Liu et al.'s scheme does not achieve perfect forward secrecy. In Liu et al.'s scheme, the attacker can compute the all session key between the user U_i and server S if the attacker knows the one of long-term keys in future[13,14] . Figure 5 describes why Liu et al.'s scheme cannot provide perfect forward secrecy. First, the attacker got ID_i , E_{Pi} , G_{Pi} , T_{Pi} and T_{Ps} in previous communication between user U_i and server S. Then, the attacker knows one of long-term secret A_i . So the attacker can compute α and β as follows;

· Attacker got ID_i, E_{Pi} , G_{Pi} , T_{Pi} , and T_{Ps} in previous public communication

· Attacker know one of user's long-term secret : A_i

· Attacker has ID_i, E_{Pi} , G_{Pi} , T_{Pi} , T_{Ps} and A_i

→ $\alpha = E_{Pi} \oplus A_i \oplus T_{Pi}$
→ $\beta = G_{Pi} \oplus A_i \oplus T_{Ps}$
→ $sk_P = h(\alpha \| \beta \| h(A_i \oplus ID_i))$

· Attacker has can compute all of previous session key sk_P

Figure 5. No Perfect Forward Secrecy of Liu et al.'s authentication

$\alpha = E_{Pi} \oplus A_i \oplus T_{Pi}$,

$\beta = G_{Pi} \oplus A_i \oplus T_{Ps}$,

$sk_P = \mathrm{h}(\alpha \| \beta \| \mathrm{h}(A_i \oplus ID_i))$.

The attacker can compute the previous session key sk_P using α and β. Therefore, this scheme does not achieve perfect forward secrecy. In Liu et al.'s scheme, A_i is a secure shared long-term secret between U_i and S. If the attacker knew A_i , he can computes all of previous session key between between U_i and S. To solve this problem, it is necessary that the attacker cannot compromise the session key between U_i and server S by adding another secret information.

No Anonymity

Liu et al.'s authentication scheme does not provide the anonymity. In this scheme, the user sends its own U_i to server S over public communication without any protection. Therefore, an attacker can easily get U_i from public communications. This results in an information exposure problem. By the server's incoming communication, an attacker can obtain information of the approximate number of registered user to sever and attacker can acquire information on which user communicates with server. Therefore, the lack

of anonymity in Liu's authentication scheme raises some problem that need to be addressed by providing user anonymity through a protection technique. To solve this problem, It is necessary for use anonymity identification in the communication instead of sending a normal ID_i [15]

CONCLUSION

Liu et al. proposed an efficient and secure smart card based password authentication scheme but their scheme has security problem. So this paper analyze Liu et al.'s scheme and shows that this scheme has security weakness such as off-line password guessing attack, smart-card loss attack, no perfect forward secrecy, and no anonymity. Henceforth, it is needed to propose security enhanced scheme for solving Liu et al.'s scheme's security weaknesses.

ACKNOWLEDGMENTS

This research was supported by financial support of Howon University in 2017.

REFERENCES

[1] Chang, C. C., Lee, C. Y., & Chiu, Y. C., 2009, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," Computer Communications, 32(4), 611-618.

[2] Tzong-Chen, W., & Hung-Sung, S., 1996, "Authenticating passwords over an insecure channel," Computers & Security, 15(5), 431-439.

[3] Lamport, L., 1981, "Password authentication with insecure communication," Communications of the ACM, 24(11), 770-772.

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

[5] Kim, S. K., & Chung, M. G., 2009, "More secure remote user authentication scheme. Computer Communications," 32(6), 1018-1021.

[6] Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., & Won, D., 2014, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, 14(6), 10081-10106.

[7] Xu, J., Zhu, W. T., & Feng, D. G., 2009, "An improved smart card based password authentication scheme with provable security," Computer Standards & Interfaces, 31(4), 723-728.

[8] Sood, S. K., Sarje, A. K., & Singh, K., 2010, "An improvement of Wang et al.'s authentication scheme using smart cards," In Communications (NCC), 2010 National Conference on (pp. 1-5).

[9] Chen, B. L., Kuo, W. C., & Wuu, L. C., 2014, "Robust smart-card-based remote user password authentication scheme," International Journal of Communication Systems, 27(2), 377-389.

[10] Li, X., Niu, J., Khan, M. K., & Liao, J., 2013, "An enhanced smart card based remote user password authentication scheme," Journal of Network and Computer Applications, 36(5), 1365-1371.

[11] Liu, Y. J., Chang, C. C., & Chang, S. C., 2016, "An efficient and secure smart card based password authentication scheme," International Journal of Network Security.

[12] Messerges, T. S., Dabbish, E. A., & Sloan, R. H., 2002, "Examining smart-card security under the threat of power analysis attacks," IEEE transactions on computers, 51(5), 541-552.

[13] Choi, Y., Nam, J., Lee, D., Kim, J., Jung, J., & Won, D., 2014, "Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics," The Scientific World Journal, 2014.

[14] Choi, Y., Nam, J., Lee, Y., Jung, S., & Won, D., 2015, "Cryptanalysis of advanced biometric-based user authentication scheme for wireless sensor networks," In Computer Science and Its Applications (pp. 1367-1375). Springer Berlin Heidelberg..

[15] Jung, J., Choi, Y., Lee, D., Kim, J., Mun, J., & Won, D., 2015, "Cryptanalysis of Dynamic ID-Based User Authentication Scheme Using Smartcards Without Verifier Tables," In Advances in Computer Science and Ubiquitous Computing (pp. 45-51).