An improved Chang-Lee's smart card-based authentication scheme

Shu-Fen Chiou[1], Eko Fajar Cahyadi[2,3], Cheng-Ying Yang[4], and Min-Shiang Hwang[2,5,*]

[1]Department of Information Management, National Taichung University of Science and Technology, Taiwan
[2]Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan 41354
[3]Department of Telecommunication Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia
[4]Department of Computer Science, University of Taipei, Taipei, Taiwan
[5]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan 40402
(*Email: mshwang@asia.edu.tw)

Abstract. It is useful to verify a legal user from a remote terminal through the Internet with the user authentication schemes based on the smart card. Usually, the remote user has to use his/her identification accompanying the password to access the system. This action is an important scheme to protect the user's privacy and confidentiality. To achieve the robustness and the efficiency, Chang and Lee proposed a scheme that employs a smart card-based user authentication with the characters of implementation practically and easily. Also, Chang and Lee claim that the scheme could resist the replay attacks, the impersonation attacks, the identity disclosure attacks, and the perfect forward secrecy. However, this work shows that the scheme is in the risk with an on-line guessing identity and password attacks and denial of service attack. Hence, in this paper, it proposes an improved user authentication scheme that holds the capacity to withstand the vulnerability as that in Chang-Lee's smart card-based scheme.

1. Introduction

With a fast revolution of information technology, to access the Internet becomes convenient. To access the internet service and to download the files becomes easy. In order to identify the authorized users to access the remote server, there some schemes have been proposed [1-4]. Almost schemes meet the requirements of simple, useful, and practical user authentication [5-10].

Traditionally, for the user authentication, the registration table records the pairs of identity and password for each registered user in the server. By this way, the security concerns might be hold with various attacks, such as insider attacks, hacker intrusion, and guessing attacks, and other attacks [11-14]. For the attack defeating, the user authentication scheme based on the smart card has been proposed [15-17]. Within that scheme, the smart card keeps the parameters for the secure verification and the remote server does need to keep the registration table. Hence, these attacks could not be the outbreak for the system. Sequentially, based on the smart card, some user authentications have been proposed [18-23]. Recently, the robust user authentication scheme is proposed based on the smart card [24]. However, it is weak to resist the on-line guessing ID and password attacks, and DOS attack.

This work proposes an improved Chang-Lee's user authentication scheme to withstand the vulnerability in the scheme.

2. User Authentication by Chang-Lee

Chang-Lee's scheme is described as the follows [29]. In Chang-Lee's scheme, there are two major members. One is the user U_i and the other is the server S. Also, there are four phases in the scheme.

2.1. User registration phase

Initially, a new user U_i has to register the system as a legal user. Then, the system will send a valid smart card to the user U_i. The issued smart card contains a message {R1, R2, R3, SID_i, h( )}, where h( ) represents a one-way hash function; $R1 = h(id_i||x||r_i)$; $R2 = g^{xy} \bmod p$; $R3 = h(id_i||R2) \oplus h(pw_i)$; and $SID_i = (id_i||sn_i)$; r_i is a random number, x & y are two secret keys of the server S, g is a primitive root, p is a large prime, and sn_i is a serial number.

2.2. User login phase

When the user U_i wants to receive the resource from the remote server, the user U_i should input his/her identity id_i accompanying with the password pw_i to the terminal devise with the smart card. Then, a message {DID_i, V_i, n_i} is generated by the smart card and is sent to the server S. n_i is a random number generating with the smart card; $C1 = R3 \oplus h(pw_i)$; $V1 = R1 \oplus C1$; $DID_i = h(R2||n_1) \oplus SID_i$, where R1, R2, R3, and SID_i are retrieved from the storage of smart card.

2.3. Server authentication phase

According the following steps, the user U_i verifies the server S.

1) The server S retrieves the identity id_i and the serial number ni from SID_i:

$$SID_i = DID_i \oplus h(g^{xy} \bmod p)||n_i)$$
$$= (id_i \,||\, sn_i)$$

2) The server S checks the formats for id_i and sn_i. If the formats are correct, the server computes R1*, V2, and V3 and sends {id_s, V2, V3} to the user U_i, here id_s is the identity of the server. $R1^* = V1 \oplus h(id_i \,||\, g^{xy} \bmod p))$; $V2 = h(R1^* \,||\, id_s \,||\, n_i)$; $V3 = h(h(id_i||g^{xy} \bmod p))||n_i) \oplus n_2$. Here n_2 is the random number generating with the server S.
3) Upon receiving {id_s, V2, V3} from the server, the user U_i computes V2* and check V2, $V2^* = h(R1 \,||\, id_s \,||\, n_i)$. If V2 = V2*, the server is authenticated; otherwise, the user stops the procedure.
4) U_i send V4 to the server, $n_2 = V3 \oplus h(C1 \,||\, n_2)$, $SK = h(n_1 \,||\, SID_i \,||\, R2 \,||\, n_2)$, and $V4 = h(SK \,||\, (n_2 + 1))$.

2.4. User authentication phase

According to the following steps, the server S verifies the user U_i.

1) V4* is calculated by S: $SK = h(n_1 \,||\, SID_i \,||\, (g^{xy} \bmod p) \,||\, n_2)$ and $V4^* = h(SK \,||\, (n_2+1))$.
2) S checks V4* whether the result is equal to V4. If it is, the user U_i and the session key SK shared with U_i are authenticated; otherwise, the server terminates the connection to the user, and also stops the service to the user.

2.5. User password changing phase

After id_i and pw_i are input by the user, the smart card executes the procedures to change the current password pw_i to a new one pw'_i.

1) The smart card calculates $Q1 = h(id_i \,||\, R2)$ and $Q1^* = R3 \oplus h(pw_i)$.
2) The smart card checks Q1 and Q1*. If $Q1 \neq Q1^*$, it is not allowed to change the password.
3) The new R`3 is calculated by the smart card and, then, the original R3 is replaced.

$$R`3 = R3 \oplus h(pwi) \oplus h(pw`_i)$$
$$= h(id_i \,||R2) \oplus h(pw_i) \oplus h(pw_i) \oplus h(pw`_i)$$
$$= h(id_i||R2) \oplus h(pw`_i)$$

3. Weakness in Chang-Lee Scheme

Within Chang-Lee's scheme, for the on-line password guessing attack with user's smart card and the denial of service attack, it could not effectively withstand these attacks [29].

3.1. Password guessing attack

The adversary might have a chance to use password guessing attack when he steals the user Ui's smart card or he gets the lost smart card. In the user login phase,

1).The adversary intercepted the message {DIDi, V1, n_1} belonging to the user U_i and the server in this phase. The adversary computes V1 as follows,

$$V1 = R1 \oplus C1$$
$$= R1 \oplus R3 \oplus h(pw_i)$$
$$= R1 \oplus (h(id_i||R2) \oplus h(pw_i)) \oplus h(pw_i)$$
$$= R1 \oplus (h(id_i||R2)$$

2) The user U_i's smart card is replaced and, then, the adversary uses an arbitrary identity and guesses a password PW`$_i$.

3). The message {DID`$_i$, V`$_i$, n`$_i$} is sent to the server S. Here n_i is the random number generating by the smart card. The fake message DID_i and V_i are computed as follows,

$$C`1 = R3 \oplus h(pw`i)$$
$$V`1 = R1 \oplus C`1$$
$$DID`i = h(R2||n`1) \oplus SIDi.$$

4). The adversary could check V`1 and V1,

$$V`1 = R1 \oplus C`1$$
$$= R1 \oplus R3 \oplus h(pw`_i)$$
$$= R1 \oplus (h(id_i||R2) \oplus h(pw_i)) \oplus h(pw`_i)$$

If the guessing password pw`$_i$ is equal to the original password $pw_i$, $h(pw_i) = h\{pw`_i\}$, this implies V`1 = V1. Otherwise, the guessing password is not correct. The adversary repeats Steps 2 – 4 till the guessing password is correct.

3.2. Identity and password guessing attack

Because of the lost or stolen user Ui's smart card, the adversary might have a chance to guess the identity id`$_i$ and password pw`$_i$ of the smart card. Also, he might intend to change the password in the login phase.

1).For the password changing, Q1 and Q1* are calculated by the smart card,

$$Q1 = h(id`_i \| R2)$$
$$Q1^* = R3 \oplus h(pw`_i).$$

2) The smart card checks if Q1 is not equal to Q1*. If it is, the password changing is not allowed.

3) The original R3 is replaced with the new R`3 generating by the smart card,

$$R`3 = R3 \oplus h(pw`_i) \oplus h(pw``_i)$$
$$= h(id_i \|R2) \oplus h(pw_i) \oplus h(pw`_i) \oplus h(pw``_i)$$
$$= h(id_i||R2) \oplus h(pw``_i)$$

4) In the login phase, the guessed identity id`$_i$ is input and the password pw``$_I$ is changing. The message {DID`$_i$, V`1, n`$_1$} is sent to the server by the smart card. Here V`1 is calculated,

$$V`1 = R1 \oplus C1 = R1 \oplus R`3 \oplus h(pw``_i)$$
$$= R1 \oplus (h(id_i||R2) \oplus h(pw_i) \oplus h(pw`_i) \oplus h(pw``_i)) \oplus h(pw``_i)$$

When the guessed password pw`$_i$ is correct (i.e., $pw`_i = pw_i$), the hash function $h(pw_i)$ is equal to h(pw`$_i$), V`1 is calculated,

$$V`1 = R1 \oplus (h(id_i||R2) \oplus h(pw_i) \oplus h(pw`_i) \oplus h(pw``_i)) \oplus h(pw``_i)$$
$$= R1 \oplus (h(id_i||R2)$$
$$= V1$$

If V`1 is not equal to V_i, the adversary repeats to execute Steps 1-4 with re-guessing the identity and password.

3.3. Denial of service attack

The message $\{DID_i, V_i, n_i\}$ belonging to the legal user U_i and the server S could be interrupt in the login phase.

1). The intercepted message $\{DID_i, V1, n_1\}$ is sent to the server S in this phase.

2) The server executes the server authentication phase of Change-Lee's authentication scheme. The server will cost a large CPU to compute SIDi, R1*, V2, and V3. The server sends $\{id_s, V2, V3\}$ to adversary.

3) The adversary sends back an arbitrary V`4 to the server. The server needs to computes,

$SK = h(n_1 \| SID_i \| (g^{xy} \bmod p) \| n_2)$

$V4^* = h(SK \| (n_2+1))$

and it hecks V`4 and V4. In this step, the server could know the user is an adversary. However, the server had spent a large computation for authenticating the user. Therefore, the server is unable to serve other legal users.

4. The Proposed Authentication Scheme

In the proposed scheme, the registration phase and the revocation phase are kept as those in Chang-Lee's scheme.

4.1. User login phase

While the user U_i keys in his/her identity id_i and password pw_i to access the remote server, the user U_i has to keep the smart card in the terminal device.

1) The smart card computes Q1 and Q1*,

$Q1 = h(id_i \| R2)$

$Q1^* = R3 \oplus h(pw_i)$.

2) If Q1 is not equal to Q1*, the smart card asks the user to repeat his/her identity id_i and password pw_i for three times. If the user does not input the correct identity and password, the smart card stops the connection between the smart card and the terminal device.

3) The login message $\{DID_i, V_i, T_i\}$ to the server S is sent by the smart card. Here T_i is a time stamp of the smart card. DID_i and V_i are computed,

$C1 = R3 \oplus h(pw_i)$

$V_i = R1 \oplus C1$

$DID_i = h(R2 \| T_i) \oplus SID_i$, .

where R1, R2, R3, and SID_i are obtained from the storage of smart card.

4.2. Server authentication phase

According to the following steps, the user U_i verifies the server S.

1) The server S checks if the time stamp T_i is valid. If the time stamp is invalid, the server disconnects the link between the user U_i and the server. Also, it stops to provide the serves to the user.

2) The server retrieves the identity id_i and the serial number sn_i from SID_i,

$SID_i = DID_i \oplus h(g^{xy} \bmod p) \| T_i)$

$= (id_i \| sn_i)$

3) The server checks the formats for id_i and sn_i. If the formats are matched, the server computes R1*, V2, and V3 and sends $\{id_s, V2, V3\}$ to the user U_i, here id_s is the identity of the server.

$R1^* = V1 \oplus h(id_i \| g^{xy} \bmod p))$

$V2 = h(R1^* \| id_s \| T_i)$

$V3 = h(h(id_i \| g^{xy} \bmod p)) \| T_i) \oplus T_s$,

where T_s is a time stamp of the server.

4) Upon receiving the message {id_s, V2, V3}, the user U_i checks if the time stamp T_s is valid. If T_s is not valid, the user terminates the connection with the illegal server.
5) The user computes V2* and check V2,

$$V2^* = h(R1 \| id_s \| T_i).$$

If V2 = V2*, the server is authenticated; otherwise, the user stops the procedure.
6) The user Ui send V4 to the server,

$$T_s = V3 \oplus h(C1 \| T_s)$$
$$SK = h(n_1 \| SID_i \| R2 \| T_s)$$
$$V4 = h(SK \| T_s).$$

4.3. User authentication phase

Oppositely, according to the following steps, the server S verifies the user U_i.
1) The server calculates V4* ,

$$SK = h(T_i \| SID_i \| (g^{xy} \bmod p) \| T_s)$$
$$V4^* = h(SK \| T_s).$$

2) The server S compares V4* and V4. If V4* is equal to V4, the user U_i and the session key SK shared are authenticated. Otherwise, the server terminates the connection to the user, and also stops to provide the service to the user.

4.4. User password changing phase

When the user U_i needs to alter the password, after the user inputs his/her id_i and pw_i, the following procedures for password changing are executed.
1) The smart card calculates Q1 and Q1*,

$$Q1 = h(id_i \| R2)$$
$$Q1^* = R3 \oplus h(pw_i).$$

2) The smart card checks if Q1 and Q1* are equal. If it is, the smart card asks the user re-inputs his/her identity id_i and password pw_i for three times. If the identity and the password could not be input correctly, the connection between the smart card and the terminal device is terminated.
3) The smart card computes a new R`3 and replaces the original R3 with the new R`3.

$$R`3 = R3 \oplus h(pw_i) \oplus h(pw`_i)$$
$$= h(id_i \| R2) \oplus h(pw_i) \oplus h(pw_i) \oplus h(pw`_i)$$
$$= h(id_i \| R2) \oplus h(pw`_i)$$

5. Conclusion

In summary, this work has shown the weakness of Chang-Lee's smart card-based authentication scheme. That authentication could not withstand the on-line identity and password guessing attacks with a smart card, and denial of service attack. For these weaknesses in the authentication, in this paper, the scheme authentication scheme has been proposed. With the proposed scheme, it improves authentication without the on-line guessing identity and the password attacks and the denial of service attack.

Acknowledgments

This work was partially supported by the Ministry of Science and Technology, Taiwan, under grant MOST 108-2622-8-468-001-TM1, MOST 107-2221-E-845-002-MY3, and MOST 107-2221-E-845-001-MY3.

References

[1] Hou G, Wang Z. A robust and efficient remote authentication scheme from elliptic curve cryptosystem [J]. International Journal of Network Security, 2017, 19(6): 904-911.
[2] Hwang M S, Li L H. A new remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2000, 46(1): 28-30.

[3] Lee C C, Hwang M S, Yang W P. A flexible remote user authentication scheme using smart cards [J]. ACM Operating Systems Review, 2002, 36(3): 46-52.
[4] Shen J J, Lin C W, Hwang M S. A modified remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2003, 49(2): 414-416.
[5] Tsai C S, Lee C C, Hwang M S. Password authentication schemes: Current status and key issues [J]. International Journal of Network Security, 2006, 3: 101-115.
[6] Hwang M S, Lee C C, Tang Y L. An Improvement of SPLICE/AS in WIDE Against Guessing Attack [J]. International Journal of Informatica, 2001, 12(2): 297-302.
[7] Sood S K, Sarje A K, Singh K. Inverse Cookie-based Virtual Password Authentication Protocol [J]. International Journal of Network Security, 2016, 13(2): 172-181.
[8] Tarek E, Ouda O, Atwan A. Image-based multimodal biometric authentication using double random phase encoding [J]. International Journal of Network Security, 2018, 20(6): 1163-1174.
[9] Han L, Xie Q, Liu W. An improved biometric based authentication scheme with user anonymity using elliptic curve cryptosystem [J]. International Journal of Network Security, 2017, 19(3): 469-478.
[10] Prakash A. A biometric approach for continuous user authentication by fusing hard and soft traits [J]. International Journal of Network Security, 2014, 16(1): 65-70.
[11] Chiou S F, Pan H T, Cahyadi E F, and Hwang M S. Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications [J]. International Journal of Network Security, 2019, 21(1): 100-104.
[12] Lee C C, Liu C H, Hwang M S. Guessing Attacks on Strong-Password Authentication Protocol [J]. International Journal of Network Security, 2013, 15(1): 64-67.
[13] Thandra P K, Rajan J, Murty S A V S. Cryptanalysis of an efficient password authentication scheme [J]. International Journal of Network Security, 2016, 18(2): 362-368.
[14] Yang C C, Chang T Y, Hwang M S. The security of the improvement on the methods for protecting password transmission [J]. Informatica, 2003, 14: 551-558.
[15] Chen T Y, Lee C C, Hwang M S, Jan J K. Towards secure and efficient user authentication scheme using smart card for multi-server environments [J]. The Journal of Supercomputing, 2013, 66(2): 1008-1032.
[16] Moon J, Lee D, Jung J, Won D. Improvement of efficient and secure smart card based password authentication scheme [J]. International Journal of Network Security, 2017, 19: 1053-1061.
[17] Liu Y, Chang C C, Chang S C. An efficient and secure smart card based password authentication scheme [J]. International Journal of Network Security, 2017, 19(1): 1-10.
[18] Annamalai P, Raju K, Ranganayakulu D. Soft biometrics traits for continuous authentication in online exam using ICA based facial recognition [J]. International Journal of Network Security, 2018, 20(3): 423-432.
[19] Prakash A, Dhanalakshmi R. Stride towards proposing multi-modal biometric authentication for online exam [J]. International Journal of Network Security, 2016, 18(4): 678-687.
[20] Wei C H, Hwang M S, Chin A Y H. A mutual authentication protocol for RFID [J]. IEEE IT Professional, 2011, 13(2): 20-24.
[21] Guo C, Chang C C, Chang S C. A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications [J]. International Journal of Network Security, 2018, 20(2): 323-331.
[22] Chiou S Y, Ko W T, Lu E H. A secure ECC-based mobile RFID mutual authentication protocol and its application [J]. International Journal of Network Security, 2018, 20(2): 396-402.
[23] Ma Y. NFC communications-based mutual authentication scheme for the internet of things [J]. International Journal of Network Security, 2017, 19(4): 631-638.
[24] Chang C C, Lee C Y. A smart card-based authentication scheme using user identity cryptography [J]. International Journal of Network Security, 2013, 16: 139-147.