Improved on an improved remote user authentication scheme with key agreement

Yalin Chen[1] and Jue-Sam Chou*[2] and I - Chiung Liao[3]

[1] Institute of information systems and applications, National Tsing Hua University

Yalin78900@gmail.com

[2] Department of Information Management, Nanhua University, Taiwan
*: corresponding author: jschou@mail.nhu.edu.tw
Tel: 886+ (0)5+272-1001 ext.56536

[3] Department of Information Management, Nanhua University, Taiwan
davidliao126@gmail.com

Abstract

Recently, Kumari et al. pointed out that Chang et al.'s scheme "Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update" not only has several drawbacks, but also does not provide any session key agreement. Hence, they proposed an improved remote user authentication Scheme with key agreement on Chang et al.'s Scheme. After cryptanalysis, they confirm the security properties of the improved scheme. However, we determine that the scheme suffers from both anonymity breach and he smart card loss password guessing attack, which are in the ten basic requirements in a secure identity authentication using smart card, assisted by Liao et al. Therefore, we modify the method to include the desired security functionality, which is significantly important in a user authentication system using smart card.

Keywords: user authentication, key agreement, cryptanalysis, smart card, password change, untraceable, dynamic identity, anonymity, remote user authentication

1. Introduction

There have been many cryptographic scientists working within the field of remote user authentication using smart card system design [1-21]. A user authentication using smart card system typically contains two roles: the user and the server; and three protocols: registration, login and authentication, and password change. In the protocol design principle, to ensure the login privacy, it cannot reveal the user's identity. In

2014, Kumari et al. [14] pointed out that Chang et al.'s scheme [15] has some shortcomings: (1). offline password guessing attack, (2). impersonation attacks, (3). insider attack, (4). anonymity breach when the smart card is obtained by a legal user, (5). It sufferers from the denial of service attack, and (6). It doesn't provide session key agreement. Hence, they overcome the security weaknesses by proposing a new one with key agreement. It provides user anonymity, establishes proper mutual authentication, and offers a secure password change phase, without maintaining any database record at the server side. They claimed that the proposed scheme resists various attacks, including those existing in Chang et al.s', and outperforms six other related schemes in the aspect of security characteristics. However, upon a closer examination, we discovered that it suffers from the security weaknesses of (1) anonymity breach, and (2) the smart card loss password guessing attack. To enhance its security, we modified their scheme to include these features. We will demonstrate the enhancement in this article.

The rest of this article is organized as follows. In Section 2, we briefly introduce Kumari et al.'s Scheme. In Section 3, we analyze the weaknesses of the scheme. The modifications and the security issues are demonstrated and discussed in Section 4 and 5, respectively. Finally, a conclusion is given in Section 6.

2. Review of Kumari et al.'s scheme

Kumari et al.'s improved remote user authentication Scheme with key agreement is based on Chang et al.'s Scheme [15]. It also consists of two roles: user and the remote server; and the phases: registration, login, authentication, and password change phase. They claimed that their scheme not only tackles and eliminates all security shortcomings and vulnerabilities of Chang et al.'s Scheme, but also introduces the session key agreement. In this article, we only review the registration phase, and login and authentication phase to illustrate its weaknesses. As for the definitions of the used notations, please refer to the original article.

2.1 Registration Phase

When a user Ui registers to the service provider server Si, this phase is performed as follows:

(1) The user U_i chooses its identity ID_i, password PW_i, and selects a random nonce b. He then computes $RPW_i = h(b \,||\, PW_i)$ and sends $\{ID_i, RPW_i\}$ to Si over a secure channel.

(2) After receiving the registration message from U_i, Si chooses a random number yi, which is different for each user.

(3) Si computes the value $N_i = h(ID_i \,||\, x) \oplus RPW_i$, $Y_i = y_i \oplus h(ID_i || x)$, $D_i =$

$h(ID_i||y_i||RPw_i)$ and $E_i = y_i \oplus h(y||x)$

(4) Si stores the values $\{Y_i, D_i, E_i, h(.)\}$ into U_i's smart card SC_i for and delivers $\{SC_i$ and $N_i\}$to U_i via a secure channel.

(5)After receiving the message from SC_i, U_i computes $A_i =(ID_i||Pw_i)\oplus b$ and $M_i = N_i \oplus b$, inserts A_i and M_i into SC_i which now contains the parameters $\{Y_i, D_i, E_i, h(.), A_i$ and $M_i\}$. U_i needs not remember the random number b anymore.

2.2 Login phase

This phase is to enable a user to access the needed resources from a server. U_i inserts his SC_i into a card reader and inputs its username ID_i and password PW_i. The SCi then verifies the owner of the SC_i with the secret data stored in it.

(1) First, the SC_i computes $b = A_i \oplus (ID_i||Pw_i)$, $RPw_i = h(b||Pw_i)$, $h(ID_i||x)= M_i \oplus RPw_i \oplus b$, and $y_i = Y_i \oplus h(ID_i||x)$. He then computes $D_i^*= h(ID_i||y_i||RPw_i)$

(2) SC_i verifies whether the equation $D_i^*= D_i$ holds, if it does not hold, SC_i drops the session. And U_i is required to enter PUK (Private Unblocking Key) to re-activate his SC_i

(3) Only if $D_i^*= D_i$ holds, SCi proceeds further. it computes $h(y||x)= y_i \oplus E_i$, $N_i = M_i \oplus b$, $CID_i = ID_i \oplus h(N_i||y_i||T_i)$, $N_i' = N_i \oplus h(y_i||T_i)$, $B_i = N_i \oplus RPw_i =h(ID_i||x)$, $C_i = h(N_i||y_i||B_i||T_i)$ and $F_i = y_i \oplus (h(y||x)||T_i)$, where T_i is the system's current timestamp T_i.

(4) SC_i transfers the login request = $\{CID_i, N_i', C_i, F_i, T_i\}$ to S_i.

2.3. Authentication phase

After receiving the login request, S_i and U_i together perform the following steps to authenticate each other:

(1) S_i verifies to see whether $(T_s - T_i) < \triangle T$ holds, where Ts is the current timestamp. If it does, S_i retrieves $y_i = F_i \oplus (h(y||x)||T_i)$, $N_i = N_i' \oplus h(y_i||T_i)$ and $ID_i = CID_i \oplus h(N_i||y_i||T_i)$. It then computes $B_i^*= h(ID_i||x)$, $C_i^*= h(N_i||y_i||B_i^*||T_i)$ and compares C_i^* with C_i.

(2) If $C_i^*=C_i$ holds, S_i confirms the legality of U_i. It then computes $a = h(B_i^*||y_i||Tss)$ and transmits $\{a, T_{ss}\}$ to SC_i, where T_{ss} is the server's current timestamp.

(3) On receiving $\{a, T_{ss}\}$, SC_i checks T_{ss} for freshness. If T_{ss} is fresh, SC_i computes $a^*= h(B_i||y_i||T_{ss})$ and verifies to see whether $a^*= a$ holds. If it holds, SC_i confirms the legality of the server.

(4) After successful mutual authentication, U_i and S_i both compute the common session key as $Sessk = h(B_i||y_i||T_i||T_{ss}||h(y||x))$ and $(Sessk)= h(B_i^*||y_i||T_i||T_{ss}||h(y||x))$ respectively.

3. Weakness of the scheme

Due to the parameters $\{Y_i, D_i, E_i, h(.), A_i$ and $M_i\}$ stored in the smart card and the user himself can compute the $b = A_i \oplus (ID_i||Pw_i)$, $RPw_i = h(b||Pw_i)$, $h(ID_i||x) = M_i \oplus RPw_i \oplus b$, and $y_i = Y_i \oplus h(ID_i||x)$, an insider can compute his own $h(y||x) = y_i \oplus E_i$. That is, each user can know the value $h(y||x)$. Under this situation, we can see that their scheme suffers from: (1) Anonymity breach, (2) The smart card loss password guessing attack. We describe them below.

(1) The insider attacks on the protocol's anonymity property

If a user Bob's login request $\{CID_i, N_i', C_i, F_i, T_i\}$, transferred to S_i, is intercepted by an insider attacker Alice, Alice can know Bob's y_i by calculating $y_i = F_i \oplus (h(y||x)||T_i)$. He then computes $ID_i = CID_i \oplus h(N_i||y_i||T_i)$. That is, Alice obtains the user's ID_i, which now is Bob. Therefore, the attack succeeds.

(2) The smart card loss password guessing attack

From the collected login request messages $\{CID_i, N_i', C_i, F_i, T_i\}$ and from the equations $y_i = F_i \oplus (h(y||x)||T_i)$ and $h(y||x) = y_i \oplus E_i$, the insider Alice can calculate the corresponding E_is of each login request by computing $E_i = y_i \oplus h(y||x)$. Therefore, once Bob, who has ever loggined to the server, loses his smart card and obtained by Alice, then from comparing the value E_i stored in the lost card with the calculated corresponding E_is. Alice can identify which intercepted login request is Bob's own. After obtaining the knowledge of Bob's ID_i, and the stored values A_i, D_i, Alice can successfully launch a smart card loss password guessing attack as follows.

The insider first guesses the lost card owner's password as pw_i'. He then computes $b' = A_i \oplus (ID_i||pw_i')$, $RPw_i' = h(b'||pw_i')$, and $D_i' = h(ID_i||y_i||RPw_i')$. Obviously, we can see that if $D_i' = D_i$, then pw_i' is Bob 's password. Therefore, the attack succeeds.

4. Modification

From the weaknesses found in Section 3, we note that the key point is the insider can obtain the value $h(y||x)$. To disguise it, we modify the messages in the registration phase and the login and authentication phases as follows.

4.1 Registration phase

When a user Ui registers to the service provider server Si, they perform the following steps:

(1) The user U_i chooses its identity ID_i, password PW_i, and selects a random nonce b. He then computes $RPW_i = h(b \,||\, PW_i)$ and sends $\{ID_i, RPW_i\}$ to S_i over a secure channel.

(2) After receiving the registration message from U_i, S_i chooses two random number r_i,

y_i, which are different for each user.

(3) S_i computes the values $G_i=r_i \oplus h(x)$, $H_i = y_i \oplus h(y|| r_i)$, $E_i = y_i \oplus h(y||x||y_i)$, $W_i = y_i \oplus RPW_i$, $N_i = h(ID_i || x) \oplus RPW_i$, $Y_i = y_i \oplus h(ID_i||x)$, and $D_i = h(ID_i||y_i||RPw_i)$

(4) Si stores the values { G_i, H_i, W_i, Y_i, D_i, E_i, h(.)} into U_i's smart card SC_i for and delivers {SC_i and N_i}to U_i via a secure channel.

(5)After receiving the message from SC_i, U_i computes $A_i =(ID_i||Pw_i) \oplus b$ and $M_i = N_i \oplus b$, inserts Ai and Mi into SC_i which now contains the parameters { G_i, H_i, W_i, Y_i, D_i, E_i, h(.), A_i and M_i}. U_i needs not remember the random number b anymore.

From the above-mentioned, we know that we add three values G_i, H_i, W_i and replace E_i with $y_i \oplus h(y||x|| y_i)$. The others are the same to the original scheme.

4.2 Login and authentication phase

This phase is to enable a user to access the needed resources from a server. U_i inserts his SC_i into a card reader and inputs its username ID_i and password PW_i. The SCi then verifies the owner of the SC_i with the secret data stored in it.

(1) First, the SC_i computes $b = A_i \oplus (ID_i||Pw_i)$, $RPw_i = h(b||Pw_i)$, $h(ID_i||x)= M_i \oplus RPw_i \oplus b$, and $y_i = Y_i \oplus h(ID_i||x)$. He then computes $D_i^*= h(ID_i||y_i||RPw_i)$

(2) SC_i verifies whether the equation $D_i^*= D_i$ holds, if it does not hold, SC_i drops the session. In addition, U_i is required to enter PUK (Private Unblocking Key) to re-activate his SC_i

(3) Only if $D_i^*= D_i$ holds, SC_i proceeds further. it computes $y_i = W_i \oplus RPW_i$, $h(y||x||y_i)= y_i \oplus E_i$, $N_i = M_i \oplus b$, $CID_i = ID_i \oplus h(N_i||y_i||T_i)$, $N_i' = N_i \oplus h(y_i||T_i)$, $B_i = N_i \oplus RPw_i =h(ID_i||x)$, $C_i = h(N_i||y_i||B_i||T_i)$ and $F_i = y_i \oplus (h(y||x||y_i)||T_i)$, where T_i is the system's current timestamp T_i.

(4) SC_i transfers the login request = { G_i, H_i, CID_i, N_i', C_i, F_i, T_i} to S_i.

4.3. Authentication phase

After receiving the login request, S_i and U_i together perform the following steps to authenticate each other:

(1) S_i verifies to see whether $(T_s - T_i) < \triangle T$ holds, where Ts is the current timestamp. If it does, S_i computes $r_i = G_i \oplus h(x)$, $y_i = H_i \oplus h(y|| r_i)$. Then, calculates $h(y||x||y_i)$ to retrieve $y_i = F_i \oplus (h(y||x||y_i)||T_i)$, $N_i = N_i' \oplus h(y_i||T_i)$ and $ID_i = CID_i \oplus h(N_i||y_i||T_i)$. It then computes $B_i^*= h(ID_i||x)$, $C_i^*= h(N_i||y_i||B_i^*||T_i)$ and compares C_i^* with C_i.

(2) If $C_i^*=C_i$ holds, S_i confirms the legality of U_i. It then computes $a = h(B_i^*||y_i||Tss)$ and transmits {a, T_{ss}} to SC_i, where T_{ss} is the server's current timestamp.

(3) On receiving {a, T_{ss}}, SC_i checks T_{ss} for freshness. If T_{ss} is fresh, SC_i computes

$a^* = h(B_i||y_i||T_{ss})$ and verifies to see whether $a^* = a$ holds. If it holds, SC_i confirms the legality of the server.

(4) After successful mutual authentication, U_i and S_i both compute the common session key as $Sessk = h(B_i||y_i||T_i||T_{ss}||h(y||x))$ and $(Sessk) = h(B_i^*||y_i||T_i||T_{ss}||h(y||x))$ respectively.

5. Security analysis

After the above modification, we can see that without the knowledge of server's secrets x and y, an insider cannot compute the value of $h(y||x||y_i)$ due to the one-way hash and the unknown value of y_i. Hence, the insider attack fails. About the lost card password guessing attack, even if an insider obtains a lost card and knows all the parameters stored, however, without the knowledge of y, y_i, b and ID_i, he cannot launch a password guessing attack. Therefore, both attacks in the original article have been resolved.

6. Conclusion

In this paper, we showed that Kumari et al.'s Scheme's Scheme is flawed, because it suffers from (1). The smart card loss password guessing attack, and (2). Anonymity breach. We, therefore, modify the Scheme to avoid these weaknesses. From the analysis shown in Section 5, we see that we have corrected the security issues.

References

[1] Chun-Ta Li, Min-Shiang Hwang , "An efficient biometrics-based remote user authentication Scheme using smart cards", Journal of Network and Computer Applications, Volume 33, Issue 1, January 2010, Pages 1–5

[2] Wen-Chung Kuo, Hong-Ji Wei, Jiin-Chiou Cheng, "An efficient and secure anonymous mobility network authentication Scheme", journal of information security and applications 19 (2014) 18-24

[3] Jue-Sam Chou, Yalin Chen, "An Efficient Two-Pass Anonymous Identity Authentication Protocol Using a Smart Card", Vol 63, No. 8;Aug 2013

[4] Ding Wang, Ping Wang, "Understanding security failures of two-factor authentication Schemes for real-time applications in hierarchical wireless sensor networks", Ad Hoc Networks 20 (2014) 1–15

[5] "Preserving privacy for free: Efficient and provably secure two-factor authentication Scheme with user anonymity", Ding Wang, Nan Wang b, Ping Wang, Sihan Qing, Information SCiences 321 (2015) 162–178

[6] Muhamed Turkanovic´, Boštjan Brumen, Marko Hölbl, "A novel user

authentication and key agreement Scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion”, Ad Hoc Networks 20 (2014) 96–112

[7] Kaiping Xue, Peilin Hong, Changsha Ma, “A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture”, Journal of Computer and System SCiences 80 (2014) 195–206

[8] Ding Wang, Ping Wang, “On the anonymity of two-factor authentication Schemes for wireless sensor networks: Attacks, principle and solutions” Computer Networks 73 (2014) 41–57

[9] Chun-Ta Li, Cheng-Chi Lee , “A novel user authentication and privacy preserving Scheme with smart cards for wireless communications”, Mathematical and Computer Modelling 55 (2012) 35–44

[10] Ding Wang, Ping Wang,“Understanding security failures of two-factor authentication Schemes for real-time applications in hierarchical wireless sensor networks”, Ad Hoc Networks 20 (2014) 1–15

[11] Mohammad Sabzinejad Farasha, Muhamed Turkanovic, Saru Kumaric,Marko Hölblb,“An efficient user authentication and key agreement Scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment” Ad Hoc Networks 36 (2016) 152–176

[12] Celia Li, Uyen Trang Nguyen, Hoang Lan Nguyen, Nurul Huda, “Efficient authentication for fast handover in wireless mesh networks”, computers & securit y 37(2013) I 24 -I 42

[13] I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, “A password authentication Scheme over insecure networks”, Journal of Computer and System SCiences, Vol. 72, No. 4, pp. 727-740, 2006.

[14] Kumari, Saru, Muhammad Khurram Khan, and Xiong Li. "An improved remote user authentication Scheme with key agreement." Computers & Electrical Engineering 40.6 (2014): 1997-2012.

[15] Chang, Ya-Fen, Wei-Liang Tai, and Hung-Chin Chang. "Untraceable dynamic-identity-based remote user authentication Scheme with verifiable password update." International Journal of Communication Systems 27.11 (2014): 3430-3440.

[16] M.-C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," Expert Systems with Applications, vol. 41, pp. 1411-1418, 2014.

[17] M. Karuppiah and R. Saravanan, "A secure remote user mutual authentication scheme using smart cards," Journal of Information Security and Applications, vol.

19, pp. 282-294, 2014.
[18] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," Expert Systems with Applications, vol. 41, pp. 8129-8143, 2014.
[19] A. K. Das and A. Goswami, "A robust anonymous biometric-based remote user authentication scheme using smart cards," Journal of King Saud University - Computer and Information Sciences, vol. 27, pp. 193-210, 2015.
[20] V. Odelu, A. K. Das, and A. Goswami, "An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card," Journal of Information Security and Applications, vol. 21, pp. 1-19, 2015.
[21] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," Information Sciences, 2015.