ISSN: 0974-6471, Vol. 11, No. (4) 2018, Pg. 190-194

Oriental Journal of Computer Science and Technology

Journal Website: www.computerscijournal.org

Revisiting the "An Improved Remote user Authentication Scheme with Key Agreement"

YALIN CHEN,[1] JUE-SAM CHOU*[2] and I - CHIUNG LIAO[2]

[1]Institute of information systems and applications, National Tsing Hua University, Hsinchu, Taiwan.
[2]Department of Information Management, Nanhua University, Dalin, Chiayi, Taiwan.

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" has several drawbacks and does not provide any session key agreement. Hence, they proposed an improved remote user authentication scheme with key agreement based on Chang *et al*. protocol. They claimed that the improved method is secure. However, we found that their improvement still has both anonymity breach and smart card loss password guessing attack which cannot be violated in the ten basic requirements advocated for a secure identity authentication using smart card by Liao *et al*. Thus, we modify their protocol to encompass these security functionalities which are needed in a user authentication system using smart card.

Article History

Received: 6-Decmeber-2018
Accepted: 26-Decmeber-2018

Keywords

User Authentication,
Key Agreement,
Cryptanalysis,
Smart Card,
Password Change,
Untraceable,
Dynamic Identity,
Anonymity,
Remote user Authentication.

Introduction

There have been many cryptographic scientists working within the field of remote user authentication using smart card system design.[1-22] A user authentication system using smart card contains two roles: the user and the server; and three protocols: registration, login and authentication, and password change. In the design principle, the user's identity cannot be revealed to a third party to ensure the login privacy. In 2014, Kumari *et al.*[14] found that Chang *et al.* scheme[15] has some shortcoming, including (1) offline password guessing attack, (2) impersonation attacks, (3) insider attack, (4) anonymity violation when the smart card is obtained by a legal user, (5) suffering the denial of service attack, and (6) doesn't provide session key agreement. Hence, they overcome the security weaknesses by proposing a new one. It possesses user anonymity property and mutual authentication, and offers a secure password change, without demanding any database kept on the server. They claimed that the proposed scheme resists various attacks, including those existed

CONTACT Jue-Sam Choul jschou@ nhu.edu.tw Department of Information Management, Nanhua University, Dalin, Chiayi, Taiwan.

Doi: http://dx.doi.org/10.13005/ojcst11.04.03

in Chang *et al.*s', and outperforms the other six related schemes in the aspect of security demands. Yet, upon a closer examination, we discovered that it suffers from the security weaknesses of (1) anonymity violation, and (2) the password guessing attack when the smart card is lost, still. To enhance, we modified their scheme to include these features. We will demonstrate the enhancement in this article. Besides, In 2018, Gupta *et al.*[22] propose a lightweight anonymous user authentication and key establishment scheme for wearable devices, which is a good design; however, we found the scheme needs to store a verifier table on the server's side. This violates one of the ten security requirements for an authentication scheme advocated by Liao *et al.* In addition, the two parameters $MGID_i$, $MSID_i$ keep unchanged forever, which might incur some malicious attempts. Meanwhile, each GWNi can launch an offline X_{ser} (the server's secret) guessing attack, because ei equals to h(MI_u\\X_{ser}) ⊕h (MP_u// X_{GWNi}).

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

Review of Kumari *et al.*'s scheme

Kumari et al.'s improved protocol is based on Chang *et al.*'s protocol.[15] It also consists of two roles: the user and remote server; and three phases: registration, login, authentication, and password change phase. They claimed that their scheme not only eliminates all security vulnerabilities in 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 their weaknesses. As for the definitions of use notations, please refer to the original article.

Registration Phase

When user Ui registers at server Si, both sides perform the followings.

1. The user Ui picks his identity IDi, password PWi, and selects a random nonce b. He then calculates RPWi= h(b‖PWi) and transmits the registration message {IDi, RPWi} over a secure channel to Si.
2. After acquirig the registration message sent by Ui, Si randomly chooses a number yi, which is different from the other users'.
3. Si counts the value $N_i = h(ID_i \| x) \oplus RPW_i$, $Y_i = y_i \oplus h(ID_i \| x)$, $Di = h(ID_i \| y_i \| RP_{wi})$ and $E_i = y_i \oplus h(y \| x)$
4. Si deposits the values $\{Y_i, D_i, E_i, h(.)\}$ into U_i's smart card SC_i and delivers $\{SC_i$ and $N_i\}$ to U_i through a safe passage.
5. After obtaining the message from SC_i, U_i calculates $A_i = (ID_i \| P_{wi}) \oplus b$, $M_i = N_i \oplus b$, and stores A_i, M_i into SC_i which now contains the parameters $\{Y_i, D_i, E_i, h(.), A_i$ and $M_i\}$ in its storage. After that, U_i needs not bear in mind the random number b anymore.

Login Phase

This phase is to enable Ui access the needed resources from a server. Firstly, Ui plugs in his SCi into a card reader and infiltrates his username IDi and password PWi. SCi then verifies its real owner with the secret data it stored by using the following steps.

1. First, computes $b = A_i \oplus (ID_i \| Pw_i)$, $RP_{wi} = h(b \| P_{wi})$, $h(ID_i \| x) = M_i \oplus RP_{wi} \oplus b$, and $y_i = Y_i \oplus h(ID_i \| x)$, then calculates $D_i^* = h(ID_i \| y_i \| RP_{wi})$.
2. Examines whether the equation $D_i^* = D_i$ holds, if it does not hold, SCi drops the session. Ui then needs to enter PUK (Private Unblocking Key) to re-initialize his SC_i
3. If $D_i^* = D_i$ holds, SCi reckons $B_i = N_i \oplus RP_{wi} = h(ID_i \| x)$, $h(y \| x) = y_i \oplus E_i$, $N_i = M_i \oplus b$, $CID_i = ID_i \oplus h(N_i \| y_i \| T_i)$, $N_i' = N_i \oplus h(y_i \| T_i)$, $C_i = h(N_i \| y_i \| B_i \| T_i)$, and $F_i = y_i \oplus (h(y \| x) \| T_i)$, where Ti is the system's current timestamp Ti.
4. SCi transfers the login postulate $\{CID_i, N_i', C_i, F_i, T_i\}$ to S_i.

Authentication Phase

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

1. Si verifies to see whether $(T_s - T_i) < \triangle T$ holds, where T_s is the current timestamp of S_i. If it does, S_i accesses $y_i = F_i \oplus (h(y \| x) \| T_i)$, $N_i = N_i' \oplus h(y_i \| T_i)$, and $ID_i = CID_i \oplus h(N_i \| y_i \| T_i)$. It then counts $B_i^* = h(ID_i \| x)$, $C_i^* = h(N_i \| y_i \| B_i^* \| T_i)$ and contrasts C_i^* with C_i.
2. If $C_i^* = C_i$ holds, S_i confirms the legality of Ui. It

then calculates $a = h(B_i^* || y_i || T_{ss})$ and issues {a, T_{ss}} to SC_i, where Tss is the server's current timestamp.

3. On acquiring {a, T_{ss}}, SC_i examines T_{ss} to see if it is fresh. If T_{ss} is latest, SC_i counts $a^* = h(B_i || y_i || T_{ss})$ and checks to see whether $a^* = a$ holds. If it holds, SCi confirms the legality of the server.
4. After completing mutual authentication, Ui and Si both calculate the common session key as $Sessku = h(B_i || y_i || T_i || T_{ss} || h(y||x))$ and $Sessks = h(B_i^* || y_i || T_i || T_{ss} || h(y||x))$, respectively.

Weakness of the Scheme

Due to the parameters {Y_i, D_i, E_i, h(.), A_i and M_i} are stored in the smart card and Ui himself may compute $RPwi = h(b||P_{wi})$, $b = A_i \oplus (ID_i || P_{wi})$, $h(ID_i || x) = M_i \oplus RP_{wi} \oplus b$, 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 has two weaknesses: (1) Anonymity gap, and (2) The password guessing attack when the smart card is lost. We describe them below.

The Insider Attacks on the Protocol's Anonymity Property

If a user Bob's login requisition {CID_i, N_i', C_i, F_i, T_i} sent to S_i is intercepted by an insider attacker Alice, Alice can know Bob's yi by calculating $y_i = F_i \oplus (h(y||x) || T_i)$ and then computing $ID_i = CID_i \oplus h(N_i || y_i || T_i)$. That is, Alice can get the user's identity IDi which now is Bob. Therefore, the anonymity property is violated.

The Smart Card Loss Password Guessing Attack

From the collected login postulating 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 $h(y||x) = y_i \oplus E_i$, an insider Alice can calculate the corresponding Eis of each login request by computing $E_i = y_i \oplus h(y||x)$. Therefore, once Bob, who has ever logged into the server, loses his smart card and obtained by Alice, then by comparing the value Ei stored in the lost card with the calculated corresponding Eis. Alice can identify which login request intercepted is Bob's. After obtaining the knowledge of Bob's IDi, and the stored values Ai, Di, Alice can successfully launch a smart card loss password guessing attack as follows.

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

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.

Registration Phase

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

1. The user Ui picks his identifier ID_i, passphrase PW_i, and randomly selects a nonce b. He then calculates $RPW_i = h(b || PW_i)$ and sends {ID_i, RPW_i} to Si over a safe route.
2. After obtaing the registration message from U_i, S_i picks two random numbers r_i, y_i, which are different from the other users'.
3. S_i counts the values $H_i = y_i\ h(y|| r_i)$, $G_i = r_i \oplus h(x)$, $E_i = y_i \oplus h(y||x||y_i)$, $W_i = y_i \oplus RPW_i$, $N_i = h(ID_i \oplus x) \oplus RPW_i$, $Y_i = y_i \oplus h(ID_i || x)$, and $D_i = h(ID_i || y_i || RPw_i)$
4. Si deposits the values {G_i, H_i, W_i, Y_i, D_i, E_i, h(.)} to U_i's smart card SC_i and delivers {SC_i and N_i}to U_i through a secure path.
5. After getting the message from SC_i, U_i calculates $A_i = (ID_i || Pw_i) \oplus b$, $M_i = N_i \oplus b$, and saves Ai, Mi into the storage of SCi, which now contains the parameters { G_i, H_i, W_i, Y_i, D_i, E_i, h(.), A_i and M_i}. After that, Ui needs not keep in mind 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 as the original scheme.

Login and Authentication Phase

This phase is to enable a user U_i access the needed resources from a server. U_i plugs in his SC_i into a card reader and infiltrates his username ID_i and password PW_i. SC_i then verifies its real owner with the secret data stored by using the following steps.

1. First, 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 $y_i = Y_i \oplus h(ID_i||x)$. It then reckons $D_i^* = h(ID_i||y_i||RPw_i)$
2. SCi checks whether the equation $D_i^* = D_i$ holds, if it does not hold, drops the session. After that, Ui needs to enter PUK (Private Unblocking Key) to re-activate his SC_i
3. In the case of $D_i^* = D_i$ holds, SC_i 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 Ti is the system's current timestamp T_i.
4. SCi transfers the login requisition { G_i, H_i, CID_i, N_i', C_i, F_i, T_i} to the server S_i.

Authentication Phase

After obtaining the login demand, S_i and U_i together exercise 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 server's 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 calculates $B_i^* = h(ID_i||x)$, $C_i^* = h(N_i||y_i||B_i^*||T_i)$ and contrasts C_i^* with C_i.
2. If $C_i^* = C_i$ holds, Si confirms the legality of U_i. It then counts $a = h(B_i^*||y_i||T_{ss})$ and transfers {a, T_{ss}} to SC_i, where T_{ss} is the server's current timestamp.
3. After getting {a, T_{ss}}, SC_i dertermines Tss's freshness. If Tss is latest, SCi computes $a^* = h(B_i||y_i||T_{ss})$ and examines to see whether $a^* = a$ holds. If it holds, SC_i confirms the legality of the server.
4. After completing mutual authentication, Ui and Si both calculate the common session key $Sessku = h(B_i||y_i||T_i||T_{ss}||h(y||x))$ and $Sessks = h(B_i^*||y_i||T_i||T_{ss}||h(y||x))$, respectively.

Security Analysis

After the above modification, we can see that without the knowledge of server's secrets x and y, an insider cannot calculate 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.

Conclusion

In this article, we showed that Kumari et al.'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.

Acknowledgements

The author(s) received no specific funding for this work.

Conflict of Interest

The author(s) declares no conflict of interests.

Funding Source

There is no funding source.

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) l 24 -l 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," E*xpert 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.
22. Gupta, A., Tripathi, M., Shaikh, T. J., & Sharma, A., "A Lightweight Anonymous User Authentication and Key Establishment Scheme for Wearable Devices", Computer Networks, 2018.