Cryptanalysis of Security Analysis and Enhancements of a Remote User Authentication Scheme

Min-Shiang Hwang[1,2], Hung-Wei Yang[1] and Cheng-Ying Yang[3,*]

[1]Department of Computer Science and Information Engineering, Asia University Taichung, Taiwan 41354 (Email: mshwang@asia.edu.tw)
[2]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan 40402
[3]Department of Computer Science, University of Taipei, Taipei, Taiwan
(*Email: cyang@utaipei.edu.tw)

Abstract. The main purpose of user authentication schemes is to verify the authorized user using a server via an insecure channel. With the authentication, a server and a user could have a mutual authentication. In 2019, Cao proposed an improvement of a user authentication scheme. The scheme was postulated in that it could protect from the several possible attacks and have the following advantages: Identity preservation, not only to resist the slow wrong password detection, to resist the user masquerading, the password guessing, and the sever masquerading attacks, but also to have a mutual authentication between servers and users. However, we will show his scheme is not with the capacity to against the denial of service and on-line password guessing attacks in this article. In order to improve that authentication scheme, this work proposes an enhanced remote authentication scheme with the capacity to resist those vulnerabilities as shown in Cao-Sun-Cao's scheme.

1. Introduction

As cloud-computing technologies matures, more and more data owners are beginning to make heavy use of cloud system services to reduce the cost of building systems and devices [1-3]. However, how to ensure the security of cloud services is also an important issue [4-5]. A remote authentication scheme provides to verify an authorized user in a cloud-computing server via an insecure channel. Both of server and user could have a mutual authentication with a remote user authentication scheme [6-8]. Many remote user authentication schemes had been proposed [9-22]. A secure and simple authentication could be applied to practical [23-24].

Based on using a smart card, Chang and Lee proposed an easy to implement and practical remote user authentication scheme in 2013 [25]. Without withstanding the denial of service attack and the on-line guessing identity attack, Chiou et al. showed the drawbacks in Chang-Lee's scheme. In order to overcome the disadvantage in their scheme, Chang and Lee proposed an improved scheme to withstand these vulnerabilities [26].

Based on Hash function, Hsieh and Leu presented a simple and practical remote user authentication [27]. However, Cao, Sun, and Cao showed that Hsieh-Leu's scheme have not user anonymity in 2019 [28]. Besides, the scheme is vulnerable to the following attacks: the slow wrong password detection, the password guessing, and the masquerading attacks. To resist those possible attacks, Cao, Sun, and Cao proposed another authentication scheme for the remote users [28]. Cap et al. claimed the proposed

scheme could against several possible types of attacks and have the following advantages including Identity preservation, to resist slow wrong password detection, to resist user masquerading attack, to resist sever masquerading attack, to resist password guessing attack, and to provide mutual authentications. Even though that proposed scheme is with the advantages above, with user's smart card, that scheme could not withstand the attacks including denial of service and on-line password guessing attacks. In this work, an improved remote user authentication scheme is proposed to withstand these vulnerabilities as those in Cao-Sun-Cao's scheme.

2. Review of Cao-Sun-Cao's Remote User Authentication Scheme [28]

According to Cao-Sun-Cao's scheme, there are two entities, server S and user U_i [28]. There are four phases in their authentication scheme: Registration phase, login phase, authentication phase, and password change phase. The following gives the description individually.

2.1. Registration Phase

Two phases, Initial registration and Re-registration, are included in the registration. For a new user U_i, registration is the initial phase to use the system and the server authorizes user U_i to be legal. After this initial registration phase, the server S issues a valid smart card to user U_i. These messages, $\{f_u, R, h(\cdot), b, n\}$, are embedded in the issued smart card, where

$R = P \oplus h(b \oplus PW_i)$,
$P = h(EID_i \oplus x)$, and
$EID_i = h(h(ID_i)||n)$

Here, $h(\cdot)$ denotes a hash function; b denotes a random number according to user decision. ID_i and PW_i are the user's identity and password, respectively. Secret key x is for the server, and n is an entry of U_i in the server's database. There are three attributes in the server's database. They are n, EID_i, and $V = h(h(PW_i) \oplus h(x))$.

User could invalid his smart card if the issued smart card is lost. If the user wants to have a valid smart card, he should begin with the registration phase.

2.2. Login Phase

Once if user U_i wants to access the resource, with the smart card, user U_i has to give the identity ID_i, the password PW_i to the terminal device to connect the remote system with the following steps.

1) The smart card S calculates $fu` = h(ID_i \oplus h((PW_i))$ and, then, it compares the difference between $f_u`$ and f_u stored in the issued card. If $f_u`$ is not equal to f_u, the processor terminates the connection to service.
2) The end of user sends a login request with the message $\{EID_i, M_2, M_3, T_1\}$ to the server, where $M_2 = M_1 \oplus R_c$, $M_1 = R \oplus h(b \oplus PW_i)$, $M_3 = h(M_1||R_c||T_1)$, and $EID_i = h(h(ID_i)||n)$. Also, R, b, and n are the stored number in the smart card, R_c is a random number, and T_1 is a time stamp in the terminal device.

2.3. Authentication Phase

User U_i and server S authenticates each other with the following steps.

1) Initially, the time stamp T_1 is checked if it is valid or not by server S. If T_s-$T_1 > \varepsilon$, the server stops the connection to the user, where, T_s is the time stamp in the server. Time difference ε could be the threshold for the communication delay or the tolerance for synchronization between the client device and the server.
2) Server S queries EID_i from the server's database. If EID_i is not a valid, the server stops the connection.
3) Server S computes $M_3`$ and checks if $M_3`$ is equal or not to M_3, where $M3` = h(h(EIDi \oplus x)||M2 \oplus h(EIDi \oplus x)||T_1)$ If it is not, the server stops the connection.
4) The server sends $\{EIDi, M_4, M_5, T_2\}$ to the user, where $M_4 = h(EID_i \oplus x) \oplus Rs$, $M_5 = h(h(EID_i \oplus x)||Rs||T_2)$, R_s is a random number generated in the server, and T_2 is the time stamp of the server.

5) The user computes M_5` and checks weather $M_5$` is equal to M_5 or not, where $M_5` = h(M_1||M_4 \oplus M_1)||T_2)$. If it is not, the user stops the connection.
6) The user computes the session key s_k and M_6 according to $s_k = h(M_1||R_c||M_4 \oplus M_1||T_2||T_3)$, $M_6 = h(M_1||R_c||M_4 \oplus M_1||T_3)$, where, T_3 is the valid time stamp of the user. Then, the user sends message $\{M_6, T_3\}$ to the server.
7) The server computes M_6` and checks weather $M_6$` is equal to M_6 or not, where $M_6` = h(h(EID_i \oplus x)||M_2 \oplus h(EID_i \oplus x)||R_s||T_3)$. If it is not, the user stops the connection.
8) S calculates and obtains the session key s_k and M_7 according to $s_k = h(h(EID_i \oplus x)||M_2 \oplus h(EID_i \oplus x)||R_s||T_2||T_3)$ and $M_7 = h(h(EID_i \oplus x)||M_2 \oplus h(EID_i \oplus x)||R_s||T_4)$, where, T_4 is a valid server's timestamp. Then, S sends $\{M_7, T_4\}$ to the user.
9) The user computes M_7` and checks weather $M_7$` is equal to M_7 or not. If it is, the user checks the legal server, and confirms the sharing session key s_k.

3. Weakness in Cao-Sun-Cao's Remote User Authentication

This section shows the weakness in Cao-Sun-Cao's user authentication scheme [28]. The authentication could not resist the attacks from the denial of service attacks and the on-line password guessing with user's smart card attacks.

3.1. On-Line Password Guessing with User'S Smart Card Attacks

The adversary might use password guessing attack if he/she has a chance to hold the user's smart card. The following event might be hold at the login steps in Cao-Sun-Cao's authentication.

1) With guessing user's password, the adversary inputs ID_i and PW_i` with the user's smart card.
2) Smart card S calculates $f_u` = h(ID_i \oplus h((PW_i`))$ and compares the difference between f_u` and $f_u$ stored in smart card. If $f_u$` is not equal to f_u, the smart card terminates the service. Otherwise, the smart card begins to send the login request messages: $\{EID_i, M_2, M_3, T_1\}$ to the server.
3) The adversary monitors the login request message. If there are messages send to the server, this implies the password was guessed. Otherwise, the adversary repeatly guesses a password and performs Steps 1-3.

3.2. Denial of Service Attack

The login request message $\{EID_i, M_2, M_3, T_1\}$ might be interrupted by the adversary in Step 2 of the login phase. Then, the adversary uses a fake message $\{EID_i, M_2, M_3, T_1`\}$ to send to the server, where $T_1$` is updated time stamp. The server will process the following steps in the authentication phase.

1) 1) The server checks whether the time stamp T_1 is valid or not. If the difference $(T_s\text{-}T_1)$ is larger than the time difference ε, the server stops the connection to the user, where T_s is the time stamp of the server. ε is a threshold for the communication delay or the tolerance for synchronization between the client device and the server. In this step, the server will pass the verification because the T_1`is a new current time stamp.
2) Server S queries EID_i from the database. If EID_i not exists, the server stops the connection. In this step, the server will pass the verification because the EID_i is a legal ID_i.
3) The server S computes M_3` and checks weather $M_3$` is equal to M_3 or not, where $M3` = h(h(EID_i \oplus x)||M_2 \oplus h(EID_i \oplus x)||T_1)$. If it is not, the server stops the connection. In this step, the server has an ability to check the illegal login request and will stop the connection to the user. However, the server needs to compute 2 X-ORs, 2 hash functions, and one comparison computations.

In summary, for an illegal login request message, the server needs to compute 2 X-ORs, 2 hash functions, 2 comparisons computations, and a query to a database. These computations will slow down the server's performance and unable to provide normal services.

4. The Proposed Authentication Scheme

To improve those weaknesses in Cao-Sun-Cao's scheme, this work proposes an authentication scheme. Compared with those phases in Cao-Sun-Cao's scheme, this proposed scheme modifies the registration in login phase and the password change phases in authentication phase.

4.1. Login Phase

For the remote access, user U_i inputs his/her identity ID_i and password PW_i to the end device with the smart card according to the following steps.

1) Smart card S calculates $f_u` = h(ID_i \oplus h((PW_i))$ and compares the difference between $f_u`$ and f_u stored in the smart card. If $f_u`$ is not equal to f_u, smart card S cumulates the number of wrong login requests and terminates the service to the user. If the number of the wrong login requests is larger than 3, the smart card automatically idles for a period (i.e. one day).
2) If $f_u`$ is equal to f_u, smart card S resets the number of the wrong login requests.
3) The user begins to send the login request message $\{EID_i, M_2, M_3, N_1\}$ to the server, where $M_2 = M_1 \oplus R_c$, $M_1 = R \oplus h(b \oplus PW_i)$, $M_3 = h(M_1||R_c||T_1)$, $EID_i = h(h(ID_i)||n)$, $N_1 = T_1 \oplus n$. Also, R, b, and n are retrieved from the smart card, R_c is a random number and T_1 is a current time stamp of the terminal device.

4.2. Authentication Phase

For authentication in the proposed scheme, Step 2 to Step 9 are kept the same as those authentication phase in Cao-Sun-Cao's remote user scheme. The modified Step 1 in the proposed scheme is the following.

1) Server S queries EID_i from the database. If EID_i does not exist, the server disconnects to the user. Otherwise, the server retrieves n from the database. Next the server obtains the time stamp T_1 by $T_1=N_1 \oplus n$.

5. Security Analysis of the Proposed Scheme

This section shows that the proposed scheme could resist the attacks from on-line password guessing with user's smart card and the denial of service in Cao-Sun-Cao's remote user authentication.

5.1. Resist The Attack from On-Line Password Guessing with User's Smart Card

In login phase, the adversary might use the attack from on-line password guessing when he/she hold the user's smart card.

1) The adversary begins to conjectures the password $PW_i`$ and inputs $ID_i$ and $PW_i`$ with the user's smart card.
2) Smart card S calculates $f_u` = h(ID_i \oplus h((PW_i`))$ and compares $f_u`$ and $f_u$ stored in smart card. If $f_u`$ is not equal to f_u, the smart card cumulates the number of wrong login requests and terminates the service to the user. Once if the number of the wrong login requests is larger than 3, the card automatically idles for a period (i.e. one day). Otherwise, the login request message $\{EID_i, M_2, M_3, T_1\}$ is sent to the server by the card.
3) The adversary monitors the login request message. If there are messages send to the server, this implies the password was guessed. Otherwise, the adversary repeatly guesses a password and performs Steps 1-3.

If the number of the wrong login requests is larger than 3, the smart card automatically idles for a period (i.e. one day). With this proposed authentication, it could resist the attack from on-line password guessing with user's smart card.

5.2. Resist Denial of Service Attack

The login request messages, $\{EID_i, M_2, M_3, N_1\}$, could be intercepted by the adversary in Step 3 of login phase in our proposed user authentication scheme. Since the adversary did not know the n, he/she is thus unable to masquerade $N_1`$ with the valid time stamp. The server authenticates these illegal login request messages in Step 1 of the authentication phase in our proposed scheme. In this step, the server has an ability to check the illegal login request and will stop the connection to the user. The server only needs one X-OR, one comparison, and a query to a database. These computations are less than that of Cao-Sun-Cao's scheme.

6. Conclusion

In this article, we have shown the weaknesses in Cao-Sun-Cao's scheme for remote users. Their scheme could not against the denial of service attack and the on-line guessing password attack with user's smart card. For the purpose of improvement, this work proposes a user authentication scheme for remote users. With security analysis, this proposed scheme has an ability to withstand these vulnerabilities as those in Cao-Sun-Cao's scheme.

7. Acknowledgments

We gratefully acknowledge the anonymous reviewers for their valuable comments. This study was supported by the Ministry of Science and Technology (Taiwan), under grant MOST 108-2410-H-468-023.

8. References

[1] Yang C, Chen Q, and Liu Y. Fine-grained outsourced data deletion scheme in cloud computing [J]. *International Journal of Electronics and Information Engineering*, 2019, 11(2): 81--98.
[2] Liu L, Cao Z, Mao C. A note on one outsourcing scheme for big data access control in cloud [J]. International Journal of Electronics and Information Engineering, 2018, 9(1): 29-35.
[3] Rezaei S, Doostari M A, and Bayat M. A lightweight and efficient data sharing scheme for cloud computing [J]. International Journal of Electronics and Information Engineering, 2018, 9(2): 115-131.
[4] AbdElminaam D S. Improving the security of cloud computing by building new hybrid cryptography algorithms [J]. *International Journal of Electronics and Information Engineering*, 2018, 8(1): 40-48.
[5] Al-Shaikhly M H R, El-Bakry H M, and Saleh A A. Cloud security using Markov chain and genetic algorithm [J]. *International Journal of Electronics and Information Engineering*, 2018, 8(2): 96-106.
[6] Bayat M, Atashgah M B, Barari M, and Aref M R. Cryptanalysis and improvement of a user authentication scheme for internet of things using elliptic curve cryptography [J]. *International Journal of Network Security*, 2019, 21(6): 897-911.
[7] Hou G and Wang Z. A robust and efficient remote authentication scheme from elliptic curve cryptosystem [J]. *International Journal of Network Security*, 2017, 19(6): 904-911.
[8] Hwang M S and Li L H. A new remote user authentication scheme using smart cards [J]. *IEEE Transactions on Consumer Electronics*, 2000, 46(1): 28-30.
[9] Wan T, Liu X, Liao W, and Jiang N. Cryptanalysis and improvement of a smart card based authentication scheme for multi-server architecture using ECC. *International Journal of Network Security*, 2019, 21(6): 993-1002.
[10] Annamalai P, Raju K, and 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.
[11] Chiou S Y. An efficient RFID authentication protocol using dynamic identity [J]. *International Journal of Network Security*, 2019, 21(5): 728-734.
[12] Cao S Q, Sun Q, and Cao L L. Security analysis and enhancements of a remote user authentication scheme [J]. *International Journal of Network Security*, 2019, 21(4): 661-669.
[13] Chen TY, Lee CC, Hwang MS, and Jan JK. Towards secure and efficient user authentication scheme using smart card for multi-server environments. *The Journal of Supercomputing*, 2013, 66(2): 1008-1032.
[14] Chiou SF, Pan HT, Cahyadi EF, and Hwang MS. Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications. *International Journal of Network Security*, 2019, 21(1): 100-104.
[15] Liu Y, Chang C C, and Chang S C. An efficient and secure smart card based password authentication scheme [J]. *International Journal of Network Security*, 2017, 19(1): 1-10.

[16] Hong S. Authentication techniques in the internet of things environment: A survey [J]. *International Journal of Network Security*, 2019, 21(3): 462-470.
[17] Zhang X, Wang B, and Zhang W. A robust authentication protocol for multi-server architecture using elliptic curve cryptography [J]. *International Journal of Network Security*, 2019, 21(2): 191-198.
[18] Agidi R C. Biometrics: The future of banking and financial service industry in Nigeria [J]. International Journal of Electronics and Information Engineering, 2018, 9(2): 91-105.
[19] Liu Y and Chang C C. A cloud-assisted passenger authentication scheme for Japan rail pass based on image morphing [J]. *International Journal of Network Security*, 2019, 21(2): 211-220.
[20] Tian X, Tian F, Zhang A, and Chen X. Privacy-preserving and dynamic authentication scheme for smart metering [J]. *International Journal of Network Security*, 2019, 21(1): 62-70.
[21] Tarek E, Ouda O, and Atwan A. Image-based multimodal biometric authentication using double random phase encoding [J]. *International Journal of Network Security*, 2018, 20(6): 1163-1174.
[22] Wei CH, Hwang MS, and Chin AYH. A mutual authentication protocol for RFID. *IEEE IT Professional*, 2011, 13(2): 20-24.
[23] Chiou SY, Ko WT, and Lu EH. A secure ECC-based mobile RFID mutual authentication protocol and its application. *International Journal of Network Security*, 2018, 20(2): 396-402.
[24] Guo C, Chang CC, and Chang SC. A secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications. *International Journal of Network Security*, 2018, 20(2): 323-331.
[25] Chang CC and Lee CY. A smart card-based authentication scheme using user identity cryptography. *International Journal of Network Security*, 2013, 16(1): 139-147.
[26] Chiou S F, Cahyadi E F, Yang C Y, and Hwang M S, An improved Chang-Lee's smart card-based authentication scheme [C]. *Journal of Physics: Conference Series*, ICSP 2019, Mar. 29-31, 2019.
[27] Hsieh W B and Leu J S, Exploiting hash functions to intensify the remote user authentication scheme [J]. *Elsevier Advanced Technology Publications*, 2012, 31(6): 791-798.
[28] Cao S Q, Sun Q, and Cao L L. Security analysis and enhancements of a remote user authentication scheme [J]. *International Journal of Network Security*, 2019, 21(4): 661-669.