

An Improved Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing

Eko Fajar Cahyadi^{1,2}, Yung-Chen Chou¹, Cheng-Ying Yang³, and Min-Shiang Hwang^{1,4,*}

¹Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan 41354 (*Email: mshwang@asia.edu.tw)

²Department of Telecommunication Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia

³Department of Computer Science, University of Taipei, Taipei, Taiwan (Email: cyang@utapei.edu.tw)

⁴Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan 40402

Abstract. In the traditional smart card-based password authentication schemes, the authentication is only applied to verify both of server and user, but not applied to verify the platform. Recently, Yang, Ma, and Jiang proposed a mutual authentication scheme with smart cards and password under trusted computing. Their scheme was designed to authenticate the platform. They claimed that their scheme could withstand most of the possible attacks, such as secure session key agreement, user identity anonymity, password free changing, and platform certification updating. However, we will show that their scheme is vulnerable to on-line guessing password attack with smart card, and man-in-the-middle attack. In this article, we also propose an improved Yang-Ma-Jiang's mutual authentication scheme to withstand the vulnerability in their scheme.

1. Introduction

In the traditional user authentication schemes, the authentication technologies are based on the password which is easy remember by the user [1-4]. However, the main weakness of the password-based user authentication is vulnerable to the guessing password attack [5-7]. To solve the weakness, there are many smart card-based password authentication schemes had been proposed [8-18]. To enhance the security of authenticating the user, many biometric-based user authentication schemes also had been proposed [19-27]. Other schemes with mutual authentication and based on various technique have also been proposed [28-34].

Recently, Yang, Ma, and Jiang proposed a mutual authentication scheme with smart cards and password under trusted computing [35]. Their scheme was designed to authenticate the platform. They claimed that their scheme could withstand most of the possible attacks, such as secure session key agreement, user identity anonymity, password free changing, and platform certification updating. However, we will show that their scheme is vulnerable to on-line guessing password attack with smart card, and man-in-the-middle attack. In this article, we also propose an improved Yang-Ma-Jiang's mutual authentication scheme to withstand the vulnerability in their scheme.

The rest of this article is organized as follows. In Section 2, we review Yang-Ma-Jiang's mutual authentication scheme briefly. In Section 3, we show that Yang-Ma-Jiang's scheme suffers from the



online guessing password and the man-in-the-middle attacks. In Section 4, we propose an improvement of Yang-Ma-Jiang's mutual authentication scheme. Finally, some discussions and conclusions are summarized in Section 5.

2. Review of Yang-Ma-Jiang's Scheme

In this section, we briefly review Yang, Ma, and Jiang's mutual authentication scheme [35]. In their scheme, there are two participants, the user U_i and the server S . There are three phases in their scheme: The registration phase, login and authentication phases, and update phase. Some notations used in the scheme are described in Table 1. We briefly describe Yang-Ma-Jiang's mutual authentication scheme as follows.

Table 1. The notations of Yang-Ma-Jiang's mutual authentication scheme.

Notation	Meaning
U_i	The i th user
S	The server
ID_i	The identity of U_i
PW_i	The password of U_i
$H()$	A one-way hash function
$E_k()$	An encryption function with the secret key k
T	A timestamp
AIK_{priv}	A private AIK of the server
AIK_{pub}	A public AIK of the server
$Cert_{AIK}$	The AIK certification of the server
$Sig\{X\}_{AIK}$	The signature of the message X with AIK secret key
\oplus	An XOR operation

2.1. Registration Phase

A new user U_i has to register to a server S to be a legal user. The user U_i registers to the server S by the following steps:

- Step 1.** The U_i arbitrarily chooses his/her unique identity ID_i and password PW_i . Next, U_i computes $h(PW_i)$ and submits the ID_i and $h(PW_i)$ to the server S over a secure channel.
- Step 2.** After receiving the registration **request** message from the U_i , the server S computes and stores $\{PID_i, B, I, N_0, p, g\}$ in a smart card for the user U_i . Here, N_0 is a random number; p is a large prime number. PID_i , I , and B are computed as follows:

$$\begin{aligned} PID_i &= h(x, ID_i), \\ I &= h(Cert_{AIK}), \\ B &= PID_i \oplus h(PW_i) \oplus I. \end{aligned}$$

Here, x is the server's secret parameter.

2.2. Login and Authentication Phase

The user U_i wants to have the service of the server S . The user U_i needs to execute and sends a login request message to S as follows:

- Step 1.** The U_i inserts his/her smart card in the terminal device and then inputs his/her identity ID_i and password PW_i . The smart card checks whether ID_i and PW_i are valid. If they are valid, the smart card computes C , K_u , and H_u as follows:

$$\begin{aligned} C &= h(B \oplus h(PW_i) \oplus N_0 \oplus T_1), \\ K_u &= g^a \bmod p, \\ H_u &= h(PID_i, C, K_u, T_1). \end{aligned}$$

Here, a is a random number; T_1 is current time of the smart card.

- Step 2.** The smart card sends $\{PID_i, C, K_u, T_1, H_u\}$ to the server.

- Step 3.** Upon receiving the login request message $\{PID_i, C, K_u, T_1, H_u\}$ from the user U_i , the server S computes H_u' and C' as follows:

$$H_u = h(PID_i, C, K_u, T1).$$

$$C' = h(PID_i \oplus N_0 \oplus I \oplus T1),$$

The server checks whether the time stamp $T1$ in the legal time interval, H_u is equal to H_u , and C' is equal to C . If they are all valid, the server computes $D1$, $D2$, K_s , K_{us} , PCR , Q , L , and H_s as follows:

$$D1 = h(PID_i \oplus N_0 \oplus I \oplus T2) \oplus N1; D2 = h(D1 \oplus T2);$$

$$K_s = g^b \text{ mod } p; K_{us} = (K_u)^b = g^{ab} \text{ mod } p;$$

$$PCR = \text{SHA1}(PCR_0 \parallel PCR_1 \parallel \dots \parallel PCR_N);$$

$$Q = \text{Sig}[PCR, h(K_s, N1)]_{AIK}; L = \text{Log}(SML);$$

$$H_s = h(D1, D2, K_s, Q, L, \text{Cert}_{AIK}, N1, T2).$$

Here, b and $N1$ are random numbers; $T2$ is the current time of the server.

Step 4. The server sends $\{D1, D2, K_s, Q, L, \text{Cert}_{AIK}, N1, T2, H_s\}$ to the smart card.

Step 5. Upon receiving the mutual authentication request message $\{D1, D2, K_s, Q, L, \text{Cert}_{AIK}, N1, T2, H_s\}$ from the server, the smart card computes H'_s , D'_2 , Γ , and PCR'_s as follows:

$$H'_s = h(D1, D2, K_s, Q, L, \text{Cert}_{AIK}, N1, T2).$$

$$D'_2 = h(D1 \oplus T2),$$

$$\Gamma = h(\text{Cert}_{AIK}),$$

$$PCR'_s = \text{SHA1}(PCR_0 \parallel PCR_1 \parallel \dots \parallel PCR_N).$$

The smart card checks whether H'_s , D'_2 , Γ , and PCR'_s are equal to H_s , $D2$, I , and PCR , respectively. If they are all valid, the smart card computes $N1$ and K_{us} as follows:

$$N1 = D1 \oplus h(PID_i \oplus N_0 \oplus I \oplus T2),$$

$$K_{us} = (K_s)^a = g^{ab} \text{ mod } p.$$

Step 6. The session key between U_i and the server is $K_{us} = g^{ab} \text{ mod } p$.

3. Cryptanalysis of Yang-Ma-Jiang's Mutual Authentication Scheme

In this section, we will show that Yang-Ma-Jiang's mutual authentication scheme is vulnerable to on-line guessing password attack with smart card, and man-in-the-middle attack.

- On-line Guessing Password Attack:

We assume that an adversary is able to operate a legal user's terminal with his/her smart card in some reasons.

Step A1. The adversary guesses the user U_i 's password PW_i . The smart card checks whether ID_i and PW_i are valid. If they are valid, the smart card computes C , K_u , and H_u . Next, the smart card sends $\{PID_i, C, K_u, T1, H_u\}$ to the server.

Step A2. The adversary monitors the traffic between the smart card and the server. If there is no any traffic in this session, the guessed password is incorrect. The adversary repeatedly guesses passwords and executes **Step A1**. However, if there are some messages $\{PID_i, C, K_u, T1, H_u\}$ in this session, the password of the user U_i is guessed by the adversary.

- Man-in-the-Middle Attack:

In this attack, an adversary hides between the legal user and server. If the user U_i wants to have the service of the server S , U_i needs to execute and sends a login request message to S as follows:

Step A1. The U_i inserts his/her smart card in the terminal device and then inputs his/her identity ID_i and password PW_i . The smart card checks whether ID_i and PW_i are valid. The smart card computes C , K_u , and H_u . The smart card sends $\{PID_i, C, K_u, T1, H_u\}$ to the server.

Step A2. The adversary intercepts the $\{PID_i, C, K_u, T1, H_u\}$ from the smart card. The adversary thus chooses a random number z and computes K_u^* and H_u^* as follows:

$$K_u^* = g^z \text{ mod } p,$$

$$H_u^* = h(PID_i, C, K_u^*, T1).$$

The adversary sends $\{PID_i, C, K_u^*, T1, H_u^*\}$ to the server.

Step A3. Upon receiving the login request message $\{PID_i, C, K_u^*, T1, H_u^*\}$, the server S computes H_u^* and C^* as follows:

$$H_u^* = h(PID_i, C, K_u^*, T1).$$

$$C^* = h(PID_i \oplus N0 \oplus I \oplus T1),$$

The server checks whether $T1$, H_u^* , and C^* valid. In this case, the server will check these $T1$, H_u^* , and C are all valid. The server computes and sends $\{D1, D2, K_s, Q, L, Cert_{AIK}, N1, T2, H_s\}$ to the smart card. Here, $K_s = g^b \bmod p$. The server makes a session key with the impersonated user (adversary):

$$K_{zs} = (K_z)^b = g^{zb} \bmod p.$$

Step A4. The adversary intercepts the $\{D1, D2, K_s, Q, L, Cert_{AIK}, N1, T2, H_s\}$ from the server. The adversary thus derives the session key K_{zs} as follows:

$$K_{zs} = (K_s)^z = g^{zb} \bmod p,$$

The adversary forwards the mutual authentication message $\{D1, D2, K_s, Q, L, Cert_{AIK}, N1, T2, H_s\}$ to the smart card.

Step A5. By now, the adversary could impersonate the user $U1$ and have secret communications to the server with the session key, $K_{zs} = g^{zb} \bmod p$.

4. The Improved Yang-Ma-Jiang's Scheme

In order to improve the weaknesses of Yang-Ma-Jiang's mutual authentication scheme, we propose an improvement of Yang-Ma-Jiang's scheme in this section. The registration phase and the update phase are the same as that in Yang-Ma-Jiang's scheme. We only modify the login and authentication phase as follows.

Step 1. The U_i inserts his/her smart card in the terminal device and then inputs his/her identity ID_i and password PW_i^* . The smart card computes $h(PW_i^*)$ and $B \oplus PID_i \oplus I$ as follow:

$$B \oplus PID_i \oplus I,$$

$$= (PID_i \oplus h(PW_i) \oplus I) \oplus PID_i \oplus I,$$

$$= h(PW_i).$$

Here, B , PID_i , and I are retrieved from the smart card. The smart card checks whether $h(PW_i^*)$ and $B \oplus PID_i \oplus I$ are valid. If they are not valid, the user re-inputs ID_i/PW_i^* for three times. Otherwise, the smart card computes C , K_u , and H_u as follows:

$$C = h(PID_i \oplus I \oplus N0 \oplus T1),$$

$$K_u = g^a \bmod p,$$

$$H_u = h(PID_i, C, K_u, T1).$$

Here, a is a random number; $T1$ is current time of the smart card.

Step 2. The smart card sends $\{ID_i, C, K_u, T1, H_u\}$ to the server.

Step 3. Upon receiving the login request message $\{ID_i, C, K_u, T1, H_u\}$ from the user U_i , the server S computes H_u^* and C^* as follows:

$$PID_i = h(x, ID_i),$$

$$H_u^* = h(PID_i, C, K_u, T1).$$

$$C^* = h(PID_i \oplus N0 \oplus I \oplus T1),$$

The server checks whether the time stamp $T1$ in the legal time interval, H_u^* is equal to H_u , and C^* is equal to C . If they are all valid, the server computes $D1, D2, K_s, PCR, Q, L$, and H_s as **Step 3** of the login and authentication phase in the Yang-Ma-Jiang's scheme.

Steps 4, 5, & 6. The three steps are the same as **Steps 4, 5, and 6** of the login and authentication phase in the Yang-Ma-Jiang's mutual authentication scheme.

5. Discussion and Conclusion

In this paper, we have shown that the vulnerabilities of Yang-Ma-Jiang's mutual authentication scheme. Their scheme could not against the on-line guessing password attack and the main-in-the-middle attack.

The first weakness of Yang-Ma-Jiang's scheme is that the adversary could guess the password of the legal user many times. In the improved scheme, the user has been limited to login his/her identity and password for three times (See **Step 1** of the improved scheme).

The second weakness of Yang-Ma-Jiang's scheme is that the adversary could intercept the login request message $\{PID_i, C, K_u, T1, H_u\}$ from the user and tampers K_u^* and H_u^* . Since H_u^* is calculated from the $h(PID_i, C, K_u, T1)$ which PID_i, C, K_u , and $T1$ are transmitted from the user and an adversary could intercept them. Therefore, the adversary is easy to tamper K_u^* and H_u^* and the server will check them valid. To resist the weakness, we modify that the login request message $\{ID_i, C, K_u, T1, H_u\}$ but not $\{PID_i, C, K_u, T1, H_u\}$. We replace PID_i to ID_i . The adversary did not know the PID_i , thus he/she could not tamper K_u^* and H_u^* such that $H_u^* = h(PID_i, C, K_u^*, T1)$. Therefore, the improved scheme will against the on-line guessing and the man-in-the-middle attacks.

6. Acknowledgments

This work was partially supported by the Ministry of Science and Technology, Taiwan, under grant MOST 106-3114-E-005-001, MOST 107-2221-E-845-002-MY3, and MOST 107-2221-E-845-001-MY3.

7. References

- [1] 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.
- [2] 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.
- [3] Zhuang X, Chang C C, Wang Z H, Zhu Y. A simple password authentication scheme based on geometric hashing function [J]. *International Journal of Network Security*, 2014, 16: 271-277.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] Ling C H, Chao W Y, Chen S M, Hwang M S. Cryptanalysis of dynamic identity based on a remote user authentication scheme for a multi-server environment [C]. In: *Advances in Engineering Research*, 2015, 15: 981-986.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] Huang H F, Chang H W, Yu P K. Enhancement of timestamp-based user authentication scheme with smart card [J]. *International Journal of Network Security*, 2014, 16: 463-467.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] Kumar M. A new secure remote user authentication scheme with smart cards [J]. *International Journal of Network Security*, 2010, 11(2): 88-93.

- [17] Kumar M. An enhanced remote user authentication scheme with smart card [J]. *International Journal of Network Security*, 2010, 10(3): 175-184.
- [18] Amin R. Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment using smart card [J]. *International Journal of Network Security*, 2016, 18(1): 172-181.
- [19] 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.
- [20] 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.
- [21] 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.
- [22] Chang C C, Hsueh W Y, Cheng T F. An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards [J]. *International Journal of Network Security*, 2016, 18(6): 1010-1021.
- [23] Zhu H, Zhang Y, Li H, Lin L. A Novel Biometrics-based One-Time Commitment Authenticated Key Agreement Scheme with Privacy Protection for Mobile Network [J]. *International Journal of Network Security*, 2016, 18(2): 209-216.
- [24] Zhu H, Zhang Y, Wang X. A Novel One-Time Identity-Password Authenticated Scheme Based on Biometrics for E-coupon System [J]. *International Journal of Network Security*, 2016, 18(3): 401-409.
- [25] 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.
- [26] 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.
- [27] Liu Y, Chang C C, Sun C Y. Notes on "An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics [J]. *International Journal of Network Security*, 2016, 18(5): 997-1000.
- [28] 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.
- [29] Chang T Y, Yang W P, Hwang M S. Simple Authenticated Key Agreement and Protected Password Change Protocol [J]. *Computers & Mathematics with Applications*, 2005, 49: 703-714.
- [30] 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.
- [31] 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.
- [32] 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.
- [33] 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.
- [34] Ma Y. NFC Communications-based Mutual Authentication Scheme for the Internet of Things [J]. *International Journal of Network Security*, 2017, 19(4): 631-638.
- [35] Yang L, Ma J F, Jiang Q. Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing [J]. *International Journal of Network Security*, 2012, 14(3): 156-163.