Cryptanalysis of Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card

Hsieh-Tsen Pan
and Chiu-Shu Pan
Department of Computer Science
and Information Engineering,
Asia University, Taiwan

Shyh-Chang Tsaur
Department of Electronic Engineering,
National Chin-Yi University
of Technology, Taiwan

Min-Shiang Hwang
Department of Computer Science
and Information Engineering,
Asia University, Taiwan

***Abstract*—Recently, Amin proposed an efficient dynamic ID-based remote user password authentication scheme for multi-server environment. They claimed that his scheme resisted different possible attacks include off-line identity guessing attack, off-line password guessing attack, and smart card stolen attack. However, we find some weaknesses of his scheme in this article. We show that his scheme is vulnerable to off-line identity guessing with smart card stolen attack and off-line password guessing with smart card stolen attack.**

I. Introduction

Remote user authentication is the mechanism that widely uses to identify the legitimate user in Internet [8], [12], [20], [26], [27]. Conventional remote user authentication schemes are suited to identify the remote users for single server environment of client/server architecture [2], [7], [16], [19], [23], [25]. However, the use of Internet has grown spectacularly. More and more users need services in different servers. In other word, the users in the network architecture are become in multi-server environment [4], [6], [10], [15]. In conventional user authentication schemes, users not only need to login to various servers with repetitive registration, but also need to remember the various user ID (identities) and passwords [3], [5], [9], [11].

In 2012, Ramasamy et al. proposed a user authentication scheme for smart cards [18]. However, Thandra et al. showed that their scheme is insecure [21]. In 2016, Thandra et al. also proposed a secure and efficient user authentication scheme [21]. However, Pan et al. shown that their scheme is vulnerable to denial of service, online and offline password guessing, and user impersonation attacks [17]. In 2016, Wei et al. proposed a user authentication scheme [24]. However, Tsai et al. shown that their scheme is vulnerable to denial of service, password guessing, and privileged insider attacks [22]. Recently, Liu et al. proposed an efficient user authentication scheme with a smart card [14]. However, Liu et al. shown that their scheme was vulnerable to the replaying attack [13].

Recently, Amin proposed an efficient dynamic ID-based remote user password authentication scheme for multi-server environment [1]. They claimed that his scheme could resist off-line identity guessing attack, off-line password guessing attack, privileged insider attack, user impersonation attack, many logged-in users' attack, smart card stolen attack, and session key recovery attack. However, in this article we show that his scheme is vulnerable to off-line identity guessing with smart card stolen attack and off-line password guessing with smart card stolen attack.

TABLE I
The notations used in this paper.

Notations	Meaning
U_i	The user i
ID_i	The identity of the user i
PW_i	The password of the user i
S_j	The identity of the providing service server j
x	A secret key of the control server
SK	A shared secret session key
$\oplus$	A bitwise XOR operation
$H(\cdot)$	A one-way hash function
$\|\|$	A message concatenation operation

The rest of this paper is organized as follows. In Section 2, we briefly review Amin's remote user authentication scheme. In Section 3, we analyze and show that some security flaws exist in Amin's user authentication scheme. Finally, we present our conclusions in Section 4.

II. Review of Amin's Scheme

In this section, we briefly review Amin's remote user authentication scheme for multi-server environment with smart cards [1]. There are three participants in Amin's remote user authentication scheme: users ($U_i, i = 1, 2, \cdots, m$ for short), A control server (CS for short) and Servers ($S_j, j = 1, 2, \cdots, n$ for short). The scheme consists of four phases, namely the registration, the login, the authentication, and the password update phases. The notations used in this article are listed in Table I.

A. The Registration Phase

There are registration phases: server registration phase and user registration phase.

In the server registration phase, the control server CS makes a secret parameter P_j for the server S_j as follows:

$$P_j = H(SID_j||x),$$

where x is a CS's secret key, and SID_j is an identity of the server S_j.

In the user registration phase, the control server CS makes a smart card for a new user (U_i). The registration phase is executed as follows:

1) The new user U_i firstly chooses his/her identity ID_i, password PW_i, and a random number b.
2) The new user U_i computes $PWR_i = H(PW_i \oplus b)$.
3) The new user U_i sends (ID_i, PWR_i) to the control server CS through a secure channel.
4) The control server CS generates a random nonce y_i for the user U_i and computes CID_i, REG_i, and T_i as follows:

$$\begin{aligned} CID_i &= H(ID_i|| \oplus y_i \oplus x); \\ REG_i &= H(ID_i||PWR_i||CID_i); \\ T_i &= H(CID_i||x) \oplus PWR_i. \end{aligned} \quad (1)$$

5) The control server CS delivers the smart card to U_i securely. The smart card contains six parameters, $\{CID_i, REG_i, T_i, y_i, b, H(\cdot)\}$.

B. The Login Phase

In this phase, the user (U_i) wants to login to the server S_j for obtaining some services, the user (U_i) firstly attaches his/her smart card to a device reader and inputs his/her identity ID_i', password PW_i', and the server identity SID_j. The login phase is executed in the following:

1) The smart card computes PWR_i' and REG_i' as follows:

$$\begin{aligned} PWR_i' &= H(PW_i' \oplus b) \\ REG_i' &= H(ID_i'||PWR_i'||CID_i). \end{aligned}$$

2) The smart card checks whether REG_i' equals REG_i of smart card holds or not. If it's holds, it implies both of ID_i' and PW_i' are correct.
3) The smart card $\{CID_i, SID_j, T_i, L3, L2, N_3\}$ to the control server CS, where L_3, L_2, N_3 are computed by the smart card:

$$\begin{aligned} L_1 &= T_i \oplus PWR_i; \\ N_3 &= N_1 \oplus N_2; \\ L_2 &= N_2 \oplus PWR_i; \\ L_3 &= H(L_1||SID_j||N_1||L_2||N_3). \end{aligned} \quad (2)$$

Here N_1 and N_2 are two random number selected by the smart card.

C. The Authentication Phase

Upon receiving the authentication request message $\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$ from U_i, the control server CS executes this authentication phase in the following:

1) The control server CS checks CID_i and SID_j formats and computes A_1 and N_1' as follows:

$$\begin{aligned} A_1 &= H(CID_i||x); \\ PWR_i' &= T_i \oplus A_1; \\ N_2' &= L_2 \oplus PWR_i'; \\ N_1' &= N_3 \oplus N_2'; \\ L_3' &= H(A_1||SID_j||N_1'||L_2||N_3). \end{aligned}$$

2) The control server CS verifies whether L_3' equals with L_3. If it's holds, CS believes that the user U_i is legal and SID_j is the registered identity of the provider server S_j.
3) CS sends $\{CID_i, A_4, A_3, N_5\}$ to the provider server S_j. Here A_4, A_3, and N_5 are computed by CS as follows:

$$\begin{aligned} A_2 &= H(SID_j||x); \\ A_3 &= A_2 \oplus N_4; \\ N_5 &= N_1' \oplus N_4; \\ A_4 &= H(A_2||N_4||N_1||CID_i). \end{aligned}$$

Here, N_4 is a random number.
4) The provider server S_j computes A_4' as follows:

$$\begin{aligned} N_4' &= P_j \oplus A_3; \\ N_1' &= N_4' \oplus N_5; \\ A_4' &= H(P_j||N_4'||N_1'||CID_i). \end{aligned}$$

5) The provider server S_j verifies whether A_4' equals with A_4. If it's holds, S_j believes that the user U_i and the control server CS are legal.
6) S_j sends $\{SID_j, A_5, N_7\}$ to U_i. Here A_5 and N_7 are computed by S_j as follows:

$$\begin{aligned} N_7 &= N_1' \oplus N_6; \\ SK_s &= H(SID_j||CID_i||N_6||N_1'); \\ A_5 &= H(SK_s||N_6). \end{aligned}$$

Here, N_6 is a random number.
7) The user U_i computes A_5' as follows:

$$\begin{aligned} N_6' &= N_7 \oplus N_1; \\ SK_u &= H(SID_j||CID_i||N_6'||N_1); \\ A_5' &= H(SK_u||N_6'). \end{aligned}$$

8) The user U_i verifies whether A_5' equals with A_5. If it's holds, U_i believes that the provider server S_j is legal.

III. Cryptanalysis of Amin's Scheme

In this section, we will analyze Amin's remote user authentication scheme [1]. Amin claimed that his scheme is resisted different possible attacks include off-line identity guessing attack, off-line password guessing attack, and smart card stolen attack. In this section, we show that Amin's remote user authentication scheme is vulnerable to off-line identity guessing with smart card stolen attack and off-line password guessing with smart card stolen attack.

A. Off-line Password Guessing with Smart Card Stolen Attack

Amin claimed that an attacker is hard to derive user's password PW_i if the attacker gets the user's smart card and extracts the parameters $\{CID_i, REG_i, T_i, y_i, b, H(\cdot)\}$ in the smart card and a login message $\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$. In this section, we will show that Amin's scheme is vulnerable to off-line password guessing with smart card stolen attack.

Suppose an attacker has stolen the user's smart card and extracted the parameters $\{CID_i, REG_i, T_i, y_i, b, H(\cdot)\}$ from the smart card. The attacker also intercepts and obtains a login message $\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$. The attacker may guess the user's password PW_i as follows.

1) The attacker guesses the user's password PW' and computes L'_3 as follows:

$$\begin{aligned} PWR'_i &= H(PW'_i \oplus b); \\ L'_1 &= T_i \oplus PWR'_i; \\ N'_1 &= L_2 \oplus PWR'_i \oplus N_3; \\ L'_3 &= H(L'_1||SID_j||N'_1||L_2||N_3). \end{aligned}$$

   Here, b and T_i are extracted from the user's smart card. L_2, N_3, and SID_j are obtained from a login message $\{CID_i, SID_j, T_i, L_3, L_2, N_3\}$.

2) From Equation (2):

$$L_3 = H(L_1||SID_j||N_1||L_2||N_3).$$

   The attacker compares L'_3 whether is equal to the login message L_3 or not. If it is false, the guessing password PW'_i is incorrect. The attacker could repeat the above step to re-guess the other password. If it is true, this implies which the guessing password PW'_i is correct. Therefore, Amin's remote user authentication scheme is vulnerable to the off-line password guessing with smart card stolen attack.

B. Off-line Identity Guessing with Smart Card Stolen Attack

Next, we show that Amin's scheme is also vulnerable to the off-line identity guessing with smart card stolen attack.

We also suppose an attacker has stolen the user's smart card and extracted the parameters $\{CID_i, REG_i, T_i, y_i, b, H(\cdot)\}$ from the smart card. The attacker may guess the user's identity ID_i as follows.

1) The attacker guesses the user's identity ID'_i and password PW' and computes REG'_i as follows:

$$\begin{aligned} PWR'_i &= H(PW'_i \oplus b); \\ REG'_i &= H(ID'_i||PWR'_i||CID_i). \end{aligned}$$

   Here, b and CID_i are extracted from the user's smart card.

2) From Equation (1):

$$REG_i = H(ID_i||PWR_i||CID_i).$$

   The attacker compares REG'_i whether is equal to the stored smart card REG_i or not. If it is false, the guessing identity ID'_i and password PW'_i are incorrect. The attacker could repeat the above step to re-guess the other identity and password. If it is true, this implies which the guessing identity ID'_i and password PW'_i are correct. Therefore, Amin's remote user authentication scheme is vulnerable to the off-line identity and password guessing with smart card stolen attack.

IV. Conclusion

In this article, we have reviewed Amin's remote user authentication scheme [1] and cryptanalyzed its security. Because the user identity and password are chosen by easy to remember, we showed that Amin's remote user authentication scheme cannot withstand the off-line identity guessing with smart card stolen attack and off-line password guessing with smart card stolen attack.

Acknowledgment

This study was supported by the National Science Council of Taiwan under grant MOST 104-2221-E-468-004.

References

[1] R. Amin, "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", *International Journal of Network Security*, Vol. 18, No. 1, pp. 172-181, 2016.

[2] N. Anwar, I. Riadi, A. Luthfi, " Forensic SIM Card Cloning Using Authentication Algorithm", *International Journal of Electronics and Information Engineering*, Vol. 4, No. 2, pp. 71-81, 2016.

[3] C. C. Chang, W. Y. Hsueh, T. F. Cheng, "An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards", *International Journal of Network Security*, Vol. 18, No. 6, pp. 1010-1021, 2016.

[4] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards Secure and Efficient User Authentication Scheme Using Smart Card for Multi-Server Environments", *The Journal of Supercomputing*, Vol. 66, No. 2, pp. 1008-1032, 2013.

[5] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's Improvement on a Password Authentication Scheme for Multi-server Environments", *International Journal of Network Security*, Vol. 16, No. 4, pp. 318-321, 2014.

[6] D. He, W. Zhao, and S. Wu, "Security Analysis of a Dynamic ID-based Authentication Scheme for Multi-server Environment Using Smart Cards", *International Journal of Network Security*, Vol. 15, No. 5, pp. 350-356, 2013.

[7] M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[8] C. C. Lee, M. S. Hwang, I. E. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity For Wireless Environments", *IEEE Transactions on Industrial Electronics*, Vol. 53, No. 5, pp. 1683-1687, 2006.

[9] L. H. Li, I. C. Lin, M. S. Hwang, "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks", *IEEE Transactions on Neural Networks*, Vol. 12, pp. 1498-1504, 2001.

[10] I. C. Lin, M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme for Multi-Server Architecture", *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13-22, 2003.

[11] C. H. Ling, W. Y. Chao, S. M. Chen, and M. S. Hwang, "Cryptanalysis of Dynamic Identity Based on a Remote User Authentication Scheme for a Multi-server Environment", in *2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015)*, Zhengzhou, April 11-12, 2015, Advances in Engineering Research, vol. 15, pp. 981-986, Atlantis Press, 2015.

[12] J. Ling, G. Zhao, "An Improved Anonymous Password Authentication Scheme Using Nonce and Bilinear Pairings", *International Journal of Network Security*, Vol. 17, No. 6, pp. 787-794, 2015.

[13] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[14] Y. Liu, C. C. Chang, S. C. Chang, "An Efficient and Secure Smart Card Based Password Authentication Scheme", *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, 2017.

[15] Y. Liu, C. C. Chang, C. Y. Sun, "Notes on An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics", *International Journal of Network Security*, Vol. 18, No. 5, pp. 997-1000, 2016.

[16] E. O. Osei, J. B. Hayfron-Acquah, "Cloud Computing Login Authentication Redesign", *International Journal of Electronics and Information Engineering*, Vol. 1, No. 1, pp. 1-8, 2014.

[17] Chiu-Shu Pan, Cheng-Yi Tsai, Shyh-Chang Tsaur, Min-Shiang Hwang, "Cryptanalysis of an Efficient Password Authentication Scheme", *2016 3rd International Conference on Systems and Informatics (ICSAI 2016)*, 2016.

[18] R. Ramasamy and A. P. Muniyandi, "An Efficient Password Authentication Scheme for Smart Card", *International Journal of Network Security*, Vol. 14, No. 3, pp. 180-186, 2012.

[19] J. J. Shen, C. W. Lin, M. S. Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.

[20] M. Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", *International Journal of Network Security*, Vol. 18, No. 4, pp. 798-801, 2016.

[21] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an Efficient Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 2, pp. 362-368, 2016.

[22] C. Y. Tsai, C. S. Pan, and M. S. Hwang, "An Improved Password Authentication Scheme for Smart Card", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[23] Y. Wang and X. Peng, "Cryptanalysis of Two Efficient Password-based Authentication Schemes Using Smart Cards", *International Journal of Network Security*, Vol. 17, No. 6, pp. 728-735, 2015.

[24] J. Wei, W. Liu, X. Hu, "Secure and Efficient Smart Card Based Remote User Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 4, pp. 782-792, 2016.

[25] H. Wijayanto, M. S. Hwang, "Improvement on Timestamp-based User Authentication Scheme with Smart Card Lost Attack Resistance", *International Journal of Network Security*, Vol. 17, No. 2, 2015, pp. 160-164, 2015.

[26] H. Zhu, Y. Zhang, and Y. Zhang, "A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm", *International Journal of Network Security*, Vol. 18, No. 4, pp. 688-698, 2016.

[27] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A Simple Password Authentication Scheme Based on Geometric Hashing Function", *International Journal of Network Security*, Vol. 16, pp. 271-277, 2014.