Cryptanalysis of Dynamic Identity Based on a Remote User Authentication Scheme for a Multi-server Environment

Chung-Huei LING[1], Wan-Yu CHAO[2], Shih-Ming CHEN[1] and Min-Shiang HWANG[1, 3 ,*]

[1]Department of Computer Science & Information Engineering, Asia University, Taichung, 41354, Taiwan

[2]Department of Management Information System, National Chung Hsing University, Taichung 402, Taiwan

[3]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan

*Email: mshwang@asia.edu.tw

*The corresponding author: Prof. Min-Shiang Hwang

Keywords: Smart card, user authentication, multi-server.

Abstract. It's an important research issue in a remote user authentication scheme for a multi-server environment. Recently, Li et al. proposed a scheme to remedy Lee et al.'s scheme to avoid the forgery attack, server spoofing attack and changing password easily. However, we find that Li et al.'s scheme is insecure against a server spoofing attack.

Introduction

In the information explosion age, the Internet has been a part of our life. We can do a lot of things through the Internet, like online-shopping, E-banking and online game etc. If we want to use the different services, we must register the different service servers provided. And then we must remember many pairs of ID and password. In order to solve this problem and make users convenient, Li et al. [6] proposed a remote password authentication scheme for a multi-server architecture using neural networks in 2001. The user only registers the registration center once and memorizes a pair of ID and password, and the user will get provided services. There are many related works with multi-servers [1, 2, 4, 10, 13, 14]. However, using static ID has the security weakness.

Therefore, in 2009, Liao et al. [11] proposed a secure dynamic ID based on a remote user authentication scheme for a multi-server environment. In 2009, Hsiang et al. [3] pointed that Liao et al.'s [9] scheme is still vulnerable to insider's attacks, masquerade attacks, and server spoofing attacks, so the scheme does not achieve mutual authentication. Therefore, Hsiang et al. [3] improved the scheme to remedy security holes. But in 2011, Sood et al. [12] and Lee et al. [5] respectively proved that Hsiang et al.'s [3] scheme was still vulnerable. Sood et al. [12] proposed an improved scheme that authenticates the user identity through a registration center. And Li et al. [8] and Xue et al. [16] keep going on researching into verifying by a registration center. On the contrary, Lee et al.'s [5] scheme verifies the user identity relying on a service server. In 2013, Li et al. [7] remedied Lee et al.'s scheme to avoid the forgery attack, server spoofing attack and changing password easily.

In this paper, we prove that Li et al.'s scheme is insecure against a server spoofing attack. The rest of the paper is organized as follows: Section 2 reviews the Li et al.'s scheme. In Section 3, we show how to attack Li et al.'s scheme. Finally, we make a conclusion in Section 4.

Review of Li et al.'s Scheme

In Table 1, we show the notations' meaning. There are four phases in Li's scheme [7]: registration phase, login phase, verification phase, and password change phase. We show these phase in Fig. 1. The following is the detailed description of each phase.

Table 1. Notations' meanings

Notation	meaning
U_i	The user
ID_i	The user's identity
PW_i	The user's password
CID_i	The user's dynamic identity
S_j	The Providing service server
SID_j	The Providing service server's identity
RC	Registration center
$h(\cdot)$	Hash function
$\oplus$	XOR
$\|\|$	Message concatenation operation

Registration phase:

In this phase, all sessions go through the secure channel. Firstly, RC chooses the secret key x and the secret number y. RC computes $h(x||y)$ and $h(SID_j||h(y))$, and share them with S_j. At the user part, it is as follows:

Step 1. U_i chooses ID_i and PW_i, and computes $B_i = h(r \oplus PW_i)$ by using a random number r. U_i sends $\{ID_i, B_i\}$ to RC.

Step 2. RC computes

$$C_i = h(ID_i \| x),$$
$$D_i = h(ID_i \| h(y) \| B_i),$$
$$E_i = h(C_i \| h(x \| y)),$$
$$F_i = C_i \oplus h(x \| y).$$

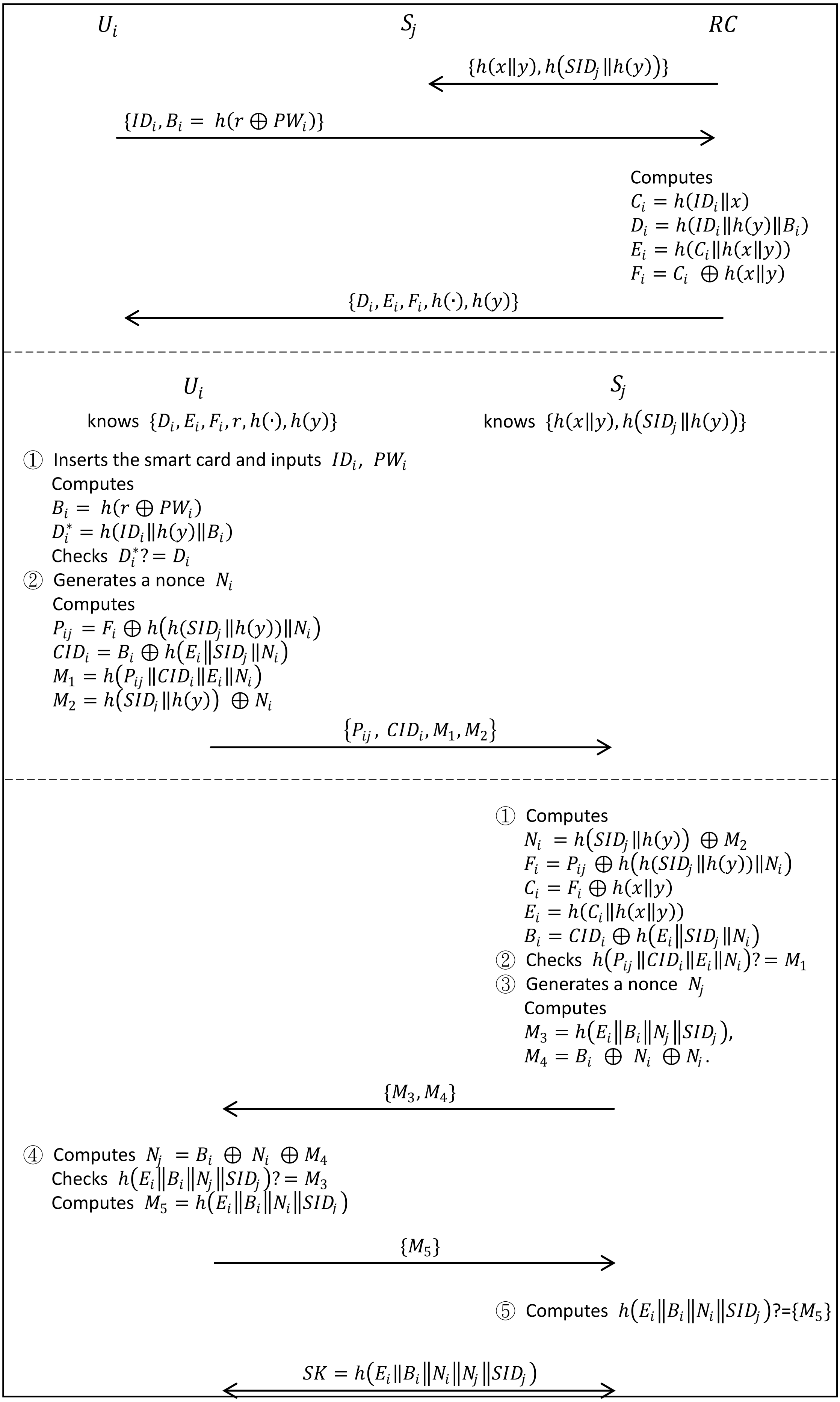

Fig. 1: Li et al.'s scheme

Step 3. RC sends $\{D_i, E_i, F_i, h(\cdot), h(y)\}$ to U_i.

Step 4. The smart card stores the following parameters: $\{D_i, E_i, F_i, r, h(\cdot), h(y)\}$.

Login phase:

Step 1. U_i inserts the smart card and inputs ID_i and PW_i. The smart card computes $B_i = h(r \oplus PW_i)$, $D_i^* = h(ID_i \| h(y) \| B_i)$. And then checks if D_i^* equals D_i. If no, the smart card denies the login request. Otherwise, it will continue the following steps.

Step 2. The smart card generates a nonce N_i, and computes

$$P_{ij} = F_i \oplus h\big(h(SID_j \| h(y)) \| N_i\big),$$
$$CID_i = B_i \oplus h\big(E_i \| SID_j \| N_i\big),$$
$$M_1 = h\big(P_{ij} \| CID_i \| E_i \| N_i\big),$$
$$M_2 = h\big(SID_j \| h(y)\big) \oplus N_i.$$

Step 3. U_i sends the login request $\{P_{ij}, CID_i, M_1, M_2\}$ to S_j.

Verification phase:

Step 1. S_j uses the login information and a known value to compute

$$N_i = h\big(SID_j \| h(y)\big) \oplus M_2,$$
$$F_i = P_{ij} \oplus h\big(h(SID_j \| h(y)) \| N_i\big),$$
$$C_i = F_i \oplus h(x \| y),$$
$$E_i = h(C_i \| h(x \| y)),$$
$$B_i = CID_i \oplus h\big(E_i \| SID_j \| N_i\big).$$

Step 2. S_j computes $h\big(P_{ij} \| CID_i \| E_i \| N_i\big)$, and checks whetherit is equals M_1, If it is not equal, S_j rejects the login request and stops this session. If yes, the following steps are continued.

Step 3. S_j generates a nonce N_j and computes

$$M_3 = h\big(E_i \| B_i \| N_j \| SID_j\big),$$
$$M_4 = B_i \oplus N_i \oplus N_j.$$

Step 4. S_j sends $\{M_3, M_4\}$ to U_i

Step 5. U_i computes $N_j = B_i \oplus N_i \oplus M_4$, and checks $h\big(E_i \| B_i \| N_j \| SID_j\big)$ if it is equal M_3. If it is equal, computes $M_5 = h\big(E_i \| B_i \| N_i \| SID_j\big)$ and sends $\{M_5\}$ to S_j. Otherwise, the communication is rejected and stoped.

Step 6. S_j computes $h\big(E_i \| B_i \| N_i \| SID_j\big)$ and checks the received message $\{M_5\}$. After successful mutual authentication, U_i and S_j commonly negotiate a session key $SK = h\big(E_i \| B_i \| N_i \| N_j \| SID_j\big)$ for the future secure session.

Change password phase:

Step 1. U_i inserts the smart card and inputs ID_i and PW_i. The smart card computes $B_i = h(r \oplus PW_i)$, $D_i^* = h(ID_i \| h(y) \| B_i)$ and checks if D_i^* equals D_i.

Step 2. If equal, U_i chooses the new password PW_i^{new}, and the smart card generates new random value r_{new}. The smart card computes $B_i^{new} = h(r_{new} \oplus PW_i^{new})$, $D_i^{new} = h(ID_i \| h(y) \| B_i^{new})$.

Step 3. The smart card replaces the stored information D_i with D_i^{new}.

Attack on Li et al.'s Scheme

At first, we assume that the attacker is a legal user and the legal providing service server, too. Secondly, the attacker can extract the stored information $\{D_i, E_i, F_i, r, h(\cdot), h(y)\}$ in the smart card. We give the attacker the notation S_k. And then we show how to masquerade server S_j.

Step 1. S_k is a legal user, so S_k extracts $h(y)$ from his/her smart card. And S_k uses public

SID_j to compute $h(SID_j \| h(y))$.

Step 2. Because S_k is a legal server, S_k also knows $h(x \| y)$.

Step 3. S_k intercepts U_i's login request message to S_j, so S_k can achieve mutual authentication with U_i and successfully establish communication.

Therefore, S_k can masquerade other providing service server. Li et al.'s scheme thus cannot resist a server spoofing attack.

Conclusion

In this paper we show that Li et al.'s scheme is not secure. Li et al.'s scheme cannot resist a legal server to masquerade another server. Therefore, we can research how to remedy Li et al.'s the scheme in the future.

Reference

[1] 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.

[2] 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.

[3] H.C. Hsiang, W.K. Shih, Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces 31 (6) (2009) 1118–1123.

[4] W.S. Juang, Efficient multi-server password authenticated key agreement using smart cards, IEEE Transactions on Consumer Electronics 50 (1) (2004) 251–255.

[5] C.C. Lee, T.H. Lin, R.X. Chang, A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards, Expert Systems with Applications 38 (11) (2011) 13863–13870.

[6] 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 12 (6) (2001) 1498–1504.

[7] X. Li, J. Ma, W.D. Wang, Y.P. Xiong, J.S. Zhang, A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments, Mathematical and Computer Modelling 58 (2013) 85–95.

[8] X. Li, Y.P. Xiong, J. Ma, W.D. Wang, An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards, Journal of Network and Computer Applications 35 (2) (2012) 763–769.

[9] Y.P. Liao, S.S. Wang, A secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces 31 (1) (2009) 24–29.

[10] I.C. Lin, M.S. Hwang, L.H. Li, A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems 19 (1) (2003) 13–22.

[11] R. Madhusudhan, R.C. Mittal, Dynamic ID-based remote user password authentication schemes using smart cards: A review, Journal of Network and Computer Applications 35 (2012) 1235-1248.

[12] S.K. Sood, A.K. Sarje, K. Singh, A secure dynamic identity based authentication protocol for

multi-server architecture, Journal of Network and Computer Applications 34 (2) (2011) 609–618.

[13] J.L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, Computers & Security 27 (3–4) (2008) 115–121.

[14] W.J. Tsaur, C.C. Wu, W.B. Lee, A smart card-based remote scheme for password authentication in multi-server Internet services, Computer Standards & Interfaces 27 (1) (2004) 39–51.

[15] D. Wang, C.G. MA, Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards, The Journal of China Universities of Posts and Telecommunications, 19 (5) (2012) 104–114.

[16] K.P. Xue, P.L. Hong, C.S. 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.