Security Analysis of a Dynamic ID-based Authentication Scheme for Multi-server Environment Using Smart Cards

Debiao He[1], Weijing Zhao[2], and Shuhua Wu[3]
(Corresponding author: Debiao He)

School of Mathematics and Statistics, Wuhan University, Wuhan, China[1]
Faculty of Electronic Information and Electrical Engineering[2]
Dalian University of Technology, Dalian, China
Networks Engineering Department, Information Engineering University, Zhengzhou, China[3]
(Email: corresponding authors@email.address)
(Received Jan. 27, 2012; revised and accepted Apr. 27, 2012)

Abstract

To guarantee secure communications in multi-server environment, Lee et al. proposed a dynamic ID-based remote user authentication scheme using smart card. They also demonstrated that their scheme could withstand various attacks. This paper reviews Lee et al.'s scheme and provides a security analysis on it. Our analysis shows that Lee et al. is vulnerable to the impersonation attack, the server spoofing attack, and the off-line password guessing attack.

Keywords: Attack, authentication, dynamic ID, multi-server system, password, smart cards

1 Introduction

As one of the simplest and the most convenient mechanism to ensure secure communication in open networks, user authentication scheme has been studied widely. In 1981, Lamport [12] proposed the first authentication for single server environment. There is a password table is used in Lamport's scheme. Then the system will be broken once the table is compromised. To improve security, many authentication schemes [2, 3, 4, 5, 6, 7, 8, 14, 15, 19, 20] using smart cards have been proposed.

With the rapid increase of Internet services, multiple servers are required at different locations to provide different services since a single server cannot satisfy users' requirement. However, all the above authentication schemes cannot used in multi-server environment since the user not only needs to register for ever server, but also needs to remember various identities and passwords. To solve the problem, Li et al. [16] proposed a user authentication scheme for multi-server environment using neural networks. To improve performance, Lin et al. [18] proposed an efficient user authentication for multi-server environment using the discrete logarithm problem. However, Juang [11] pointed out that Lin et al.'s scheme is not efficient as they claimed. Juang also proposed an improved authentication scheme for multi-server environment using the hash function and symmetric key cryptosystem. However, Chang et al. [1] demonstrated that Juang' scheme is vulnerable to an off-line dictionary attack. Chang et al. also proposed a new scheme to overcome weaknesses in Juang's scheme. Unfortunately, Chang et al.'s scheme cannot withstand the insider attack, the spoofing attack and the registration center spoofing attack.

The users' identities in the above authentication schemes for multi-server environment are transmitted in plaintext form. So they cannot provide anonymity once the adversary intercepts the message sent by the user. To solve the problem, Liao et al. [17] proposed a dynamic ID-based authentication scheme for multi-server environment. However, Hsiang et al. [10] pointed out that Liao et al.'s scheme cannot resist the insider attack, the masquerade attack, the server spoofing attack and the registration center spoofing attack. Then, Hsiang et al. proposed an improved scheme to overcome the weaknesses in Hsiang et al.'s scheme. However, Hsiang et al.'s scheme is still vulnerable to the masquerade attack, the server spoofing attack and the password guessing attack [9, 13]. Recently, Lee et al. gave six requirements for password authentication scheme for multi-server environment [13]. They also proposed a new scheme using smart cards for password authentication over insecure networks and claimed that it satisfied all the six requirements and thus is immune to various attacks. In this paper, however, some security loopholes of their scheme will be pointed out and the corresponding attacks will be described.

The organization of the paper is sketched as follows. The Section 2 gives a brief review of Lee et al.'s scheme. The security flaws of Lee et al.'s scheme are shown in Section 3. Finally, we give some conclusions in Section 4.

2 Lee et al.' Scheme

In this section, we will briefly review Lee et al.'s scheme. Their scheme consists of four phases: registration phase, login phase, verification phase, and password change phase.

In order to facilitate future references, frequently used notations are listed below with their descriptions.

U_i: The ith user;
ID_i: The identity of U_i;
PW_i: The password of U_i;
S_j: The jth server;
RC: The registration center;
SC: A smart card;
SID_j: The identity of S_j;
CID_j: The dynamic ID of U_i;
x, y: Two secret keys maintained by registration center;
$h()$: A one-way hash function;
$\oplus$: The bitwise XOR operation;
$||$: String concatenation operation.

Three entities: the user (U_i), the server (S_j), and the registration center (RC) are involved in Lee et al.'s scheme. First, RC chooses the master key x and secret number y to compute $h(x||y)$ and $h(y)$, and then shares them with S_j in the secure channel. Only RC knows the master secret key x and secret number y.

2.1 Registration Phase

In this phase, everyone who wants to register at the server should submit his identity and password to RC and obtain a smart card. The detail of the phase is described as follows.

1) U_i generates a random number b_i, chooses his identity ID_i and PW_i, and computes $h(b_i \oplus PW_i)$. Then U_i sends ID_i and $h(b_i \oplus PW_i)$ to the registration center RC through a secure channel.

2) After receiving ID_i and $h(b_i \oplus PW_i)$, RC computes $T_i=h(ID_i||x)$, $V_i=T_i \oplus h(ID_i||h(b_i \oplus PW_i))$, $B_i=h(h(b_i \oplus PW_i)||h(x||y))$ and $H_i=h(T_i)$. Then RC stores $\{V_i, B_i, H_i, h(), h(y)\}$, into a smart card and issue it to U_i.

3) When receiving the smart card, U_i keys b_i into it and finish the registration.

2.2 Login Phase

Once the user U_i wants to login to the server, as shown in Figure 1, he will perform the following login steps.

1) U_i inserts his smart card into the smart card reader and then inputs ID_i and PW_i.

2) The smart card computes $T_i=V_i \oplus h(ID_i||h(b_i \oplus PW_i))$ and $H'_i=h(T_i)$. If H'_i does not equal H_i, the smart card stops the request.

3) The smart card generates a random number N_i and computes $A_i=h(T_i||h(y)||N_i)$, $CID_i=h(b_i \oplus PW_i) \oplus h(T_i||A_i||N_i)$, $Q_i=h(B_i||A_i||N_i)$, and $P_{ij}=T_i \oplus h(h(y)||N_i||SID_j)$. Then, the smart card sends $M_1=\{CID_i, P_{ij}, Q_i, N_i\}$ to the serer S_j.

2.3 Verification Phase

This phase is executed by the server to determine whether the user is allowed to login or not. S_j executes the following steps to verify the legitimacy of U_i. We use Figure 1 to demonstrate the phase.

1). Upon receiving M_1, S_j computes $T_i = P_{ij} \oplus h(h(y)||N_i||SID_j)$, $A_i=h(T_i||h(y)||N_i)$, $h(b_i \oplus PW_i) = CID_i \oplus h(T_i||A_i||N_i)$ and $B_i=h(h(b_i \oplus PW_i)||h(x||y))$.
Then S_j computes $h(B_i||A_i||N_i)$ and checks it with Q_i. If they are not equal, S_j rejects the login request and terminates this session. Otherwise, S_j generates a random number N_j to compute $M'_{ij}=h(B_i||N_i||A_i||SID_j)$. Finally, S_j sends the message $M_2=\{M'_{ij}, N_j\}$ to U_i.

2). Upon receiving M_2, U_i checks whether $h(B_i||N_i||A_i||SID_j)$ equals M'_{ij}. If they are not equal, U_i stops the session. Otherwise, U_i computes $M''_{ij}=h(B_i||N_j||A_i||SID_j)$. At last, U_i sends $M_3=\{M''_{ij}\}$ to S_j.

3). Upon receiving M_3, S_j checks whether $h(B_i||N_j||A_i||SID_j)$ equals M''_{ij}. If they are not equal, U_i stops the request. Otherwise, U_i is authenticated successfully.

After finishing verification phase, U_i and S_j can compute $SK=h(B_i||N_i||N_j||A_i||SID_j)$ as the session key for securing communications with authenticator. The login phase and verification phase are depicted in Figure 1.

2.4 Password Change Phase

This phase will be invoked if the client wants to change his password from PW_i to PW_{new}.

1). U_i inserts his smart card into the smart card reader and then inputs ID_i and PW_i.

2). The smart card computes $T_i=V_i \oplus h(ID_i||h(b_i \oplus PW_i))$ and $H'_i=h(T_i)$. If H'_i does not equal H_i, the smart card stops the request.

3). U_i inputs the new password PW_{new} and a new random number b_{new}, computes $h(b_{new} \oplus PW_{new})$, $V_{new}=T_i \oplus h(ID_i||h(b_{new} \oplus PW_{new}))$. At last, U_i sends ID_i and $h(b_{new} \oplus PW_{new})$ to RC through a secure channel.

4). Upon receiving ID_i and $h(b_{new} \oplus PW_{new})$, RC computes $B_{new}=h(h(b_{new} \oplus PW_{new})||h(x||y))$ and sends it to U_i.

5). The smart card replaces V_i and B_i with V_{new} and B_{new}.

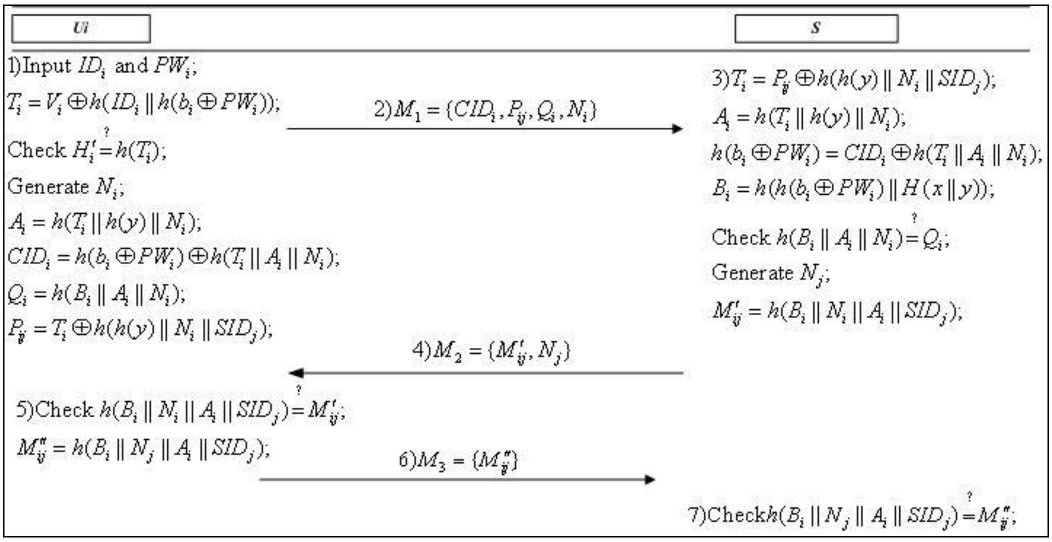

Figure 1: Login phase and verification phase of Lee et al.'s scheme

3 Lee et al.' Scheme

In this section, we will demonstrate that Lee et al.'s scheme is vulnerable to impersonation attack, server spoofing attack, and can not provide two-factor security.

3.1 Impersonation Attack

In this subsection, we first show that any malicious legal user can impersonate other legal users to log into remote server. Then we demonstrate that any malicious server also can impersonate any other legal users to log into remote server.

Malicious User's Impersonation Attack

We assume that the adversary Z is a legal user of the system, and then he can obtain a smart card containing $\{V_z, B_z, H_z, h(), h(y), b_z\}$. When another legal user U_i communicates with S_j, the adversary Z can intercept the login message $\{CID_i, P_{ij}, Q_i, N_i\}$ between U_i and S_j, and impersonate U_i though the following steps. We use Figure 2 to demonstrate the attack.

1). Z two random numbers r and N', sets $T'_i \leftarrow r$, computes

$$A_i' = h(T_i' \| h(y) \| N_i'),$$
$$CID_i' = h(b_Z \oplus PW_Z) \oplus h(T_i' \| A_i' \| N_i'),$$
$$Q_i' = h(B_Z \| A_i' \| N_i'), \text{ and}$$
$$P_{ij}' = T_i' \oplus h(h(y) \| N_i' \| SID_j).$$

Then, the smart card sends $M'_1=\{CID'_i, P'_{ij}, Q'_i, N'_i\}$ to the server S_j.

2). Upon receiving M'_1. S_j computes

$$T_i = P'_{ij} \oplus h(h(y)||N'_i||SID_j)$$
$$= T'_i$$
$$A_i = h(T_i||h(y)||N'_i)$$
$$= h(T'_i||h(y)||N'_i)$$
$$= A'_i$$
$$h(b_i \oplus PW_i) = CID'_i \oplus h(T_i||A_i||N'_i)$$
$$= h(b_z \oplus PW_z)$$

and,

$$B_i = h(h(b_i \oplus PW_i)||h(x||y))$$
$$= h(h(b_z \oplus PW_z)||h(x||y))$$
$$= B_z.$$

It is obvious that $h(B_i||A_i||N'_i)$ equals Q'_i since $Q'_i=h(B_z||A'_i||N'_i)$ and $B_i=B_z$. Then, S_j generates a random number N_j to compute $M'_{ij} = h(B_i|| N_i||A_i||SID_j)$. Finally, S_j sends the message $M'_2=\{M'_{ij},N_j\}$ to Z.

3). Upon receiving M', Z computes $M''_{ij} = h(B_z|| N_j||A'_i||SID_j)$ and sends $M'_3=\{M''_{ij}\}$ to S_j.

4). Upon receiving M'_3, S_j checks whether $h(B_i|| N_j||A_i||SID_j)$ equals M''_{ij}. It is obvious $h(B_i||N_j||A_i||SID_j)$ equals M''_{ij} since $B_i=B_z$ and $M''_{ij} = h(B_z|| N_j||A'_i||SID_j)$.

From the above description, the adversary Z impersonate U_i successfully. Moreover, Z and S_j can compute $SK = h(B_z||N'_i||N_j||A'_i||SID_j)$ as the session key for future communications. Then Lee et al.'s scheme cannot resist the impersonation attack.

Malicious Server's Impersonation Attack

We assume that S_j is a malicious server of the system, and then he can obtain $h(x||y)$ and $h(y)$ from RC. When a legal user U_i communicates with S_j, S_j can impersonate this user to obtain the services from other servers S_{j+1}. The detail of the attack, as shown in Figure 3, is described as follows.

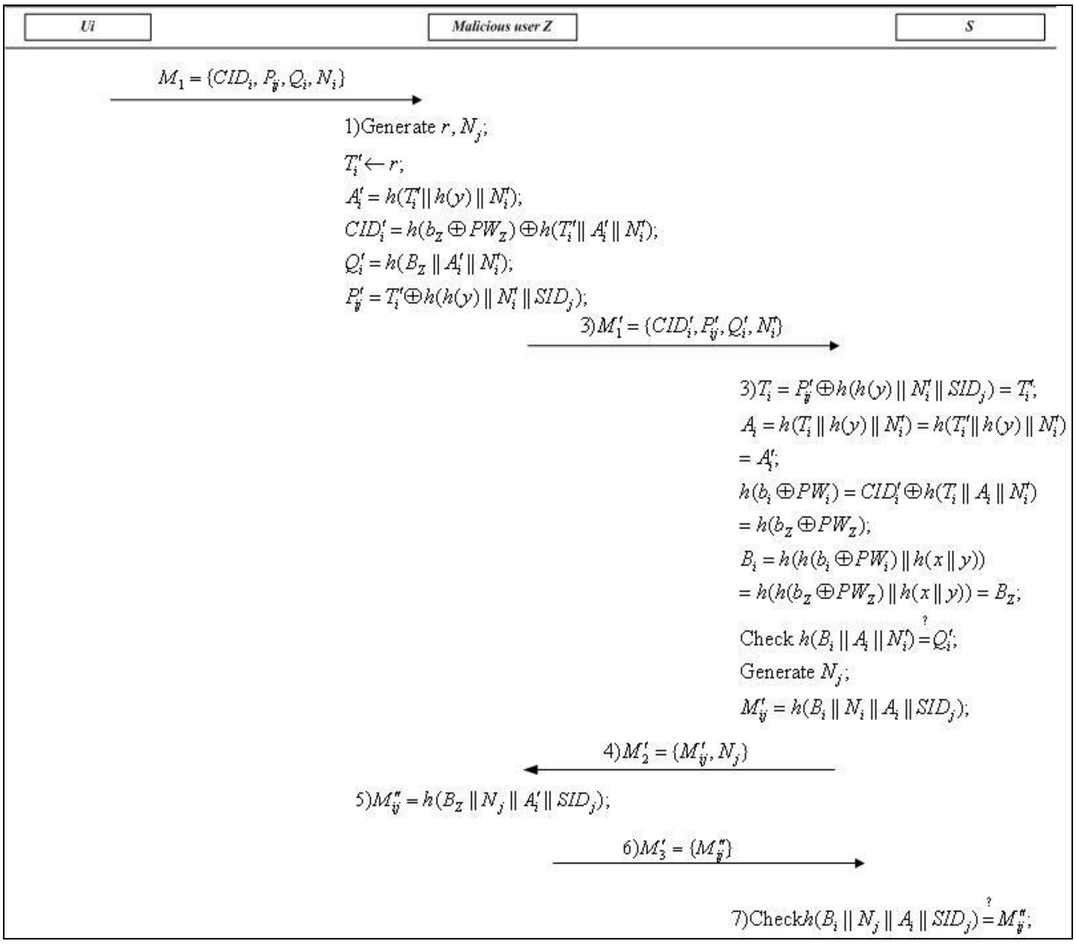

Figure 2: Malicious user's impersonation attack

1). When receiving $M_1=\{CID_i, P_{ij}, Q_i, N_i\}$ from U_i, S_j uses his $h(y)$ and $h(x||y)$ to compute $T_i=P_{ij} \oplus h(h(y)||N_i||SID_j)$, $A_i=h(T_i||h(y)||N_i)$, $h(b_i \oplus PW_i) =CID_i \oplus h(T_i||A_i||N_i)$, $B_i=h(h(b_i \oplus PW_i)|| H(x||y))$, and $P_{ij+1}=T_i \oplus h(h(y)||N_i||SID_{j+1})$. Then S_j sends $M'_1=\{CID_i, P_{ij+1}, Q_i, N_i\}$ to another server S_{j+1}.

2). Upon receiving M_1, S_{j+1} computes $T_i=P_{ij+1} \oplus h(h(y)||N_i||SID_{j+1})$, $A_i=h(T_i||h(y)||N_i)$, $h(b_i \oplus PW_i)=CID_i \oplus h(T_i||A_i||N_i)$ and $B_i=h(h(b_i \oplus PW_i)||H(x||y))$. Then S_{j+1} computes $h(B_i||A_i||N_i)$ and checks if it equals Q_i. It is obvious $h(B_i||A_i||N_i)$ equals Q_i. Then, S_{j+1} generates a random number N_{j+1} to compute $M'_{ij+1} = h(B_i ||N_i||A_i||SID_{j+1})$. Finally, S_{j+1} sends the message $M_2=\{M'_{ij+1}, N_{j+1}\}$ to S_j.

3). Upon receiving $\{M'_{ij+1}, N_{j+1}\}$, S_j computes $M''_{ij+1}=h(B_i||N_{j+1}||A_i||SID_{j+1})$ and sends $M_3 = \{ M''_{ij+1}\}$ to S_{j+1}.

4). Upon receiving M_3, S_{j+1} checks whether $h(B_i||N_{j+1}||A_i||SID_{j+1})$ equals M''_{ij+1}. From the computation of M''_{ij+1} we knows $h(B_i|| N_{j+1}|| A_i||SID_{j+1})$ equals M''_{ij+1}.

From the above description, the malicious server S_j could impersonate U_i successfully. S_j and S_{j+1} also could get $SK=h(B_i||N_i||N_{j+1}||A_i||SID_{j+1})$ as the session key for future communications. Then Lee et al.'s scheme cannot resist the impersonation attack.

3.2 Server Spoofing Attack

We assume that S_j is a malicious server of the system, and then he can obtain $h(x||y)$ and $h(y)$ from RC. When another legal user U_i communicates with S_{j+1}, S_j can intercept the login message $M_1=\{CID_i, P_{ij+1}, Q_i, N_i\}$ between U_i and S_{j+1}, and impersonate S_{j+1} though the following steps, where $CID_i=h(b_i \oplus PW_i) \oplus h(T_i||A_i||N_i)$, $Q_i=h(B_i||A_i||N_i)$, $P_{ij+1}=T_i \oplus h(h(y)||N_i||SID_{j+1})$ and $T_i=h(ID_i||x)$. We use Figure 4 to demonstrate the attack.

1). Upon receiving M_1, S_j computes

$$T_i = P_{ij+1} \oplus h(h(y) \| N_i \| SID_{j+1}),$$
$$A_i = h(T_i \| h(y) \| N_i),$$
$$h(b_i \oplus PW_i) = CID_i \oplus h(T_i \| A_i \| N_i), \text{ and}$$
$$B_i = h(h(b_i \oplus PW_i) \| H(x \| y)) \quad .$$

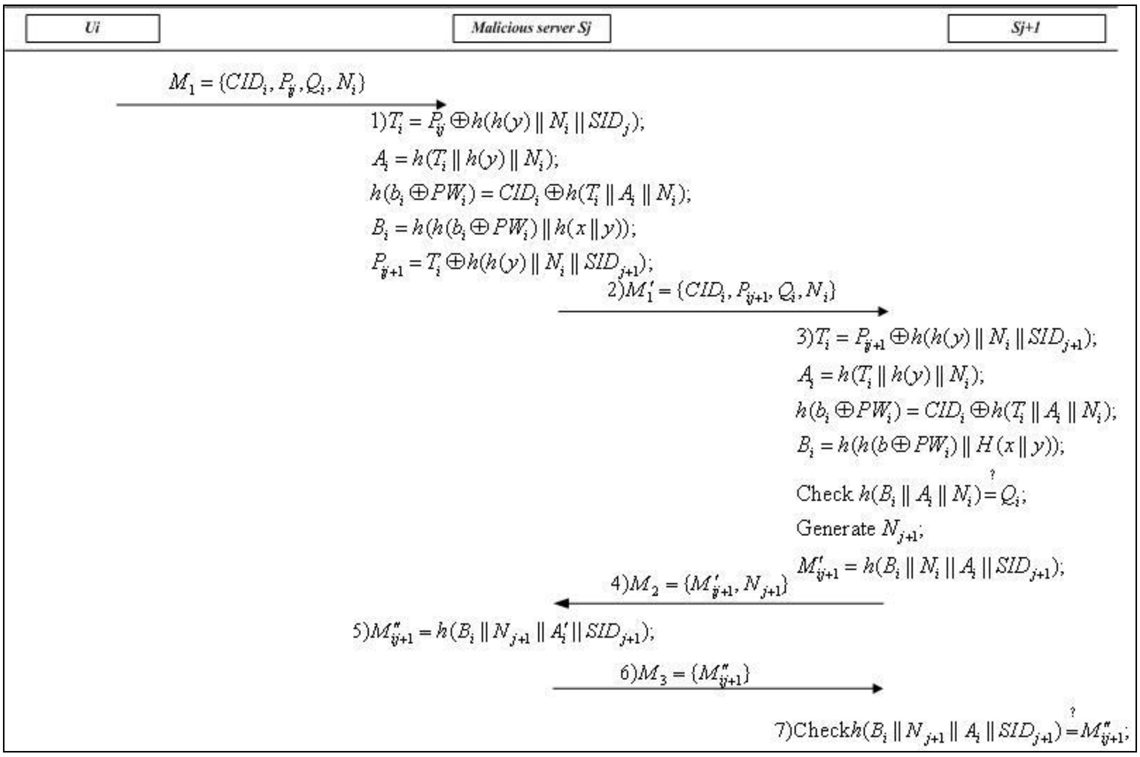

Figure 3: Malicious server's impersonation attack

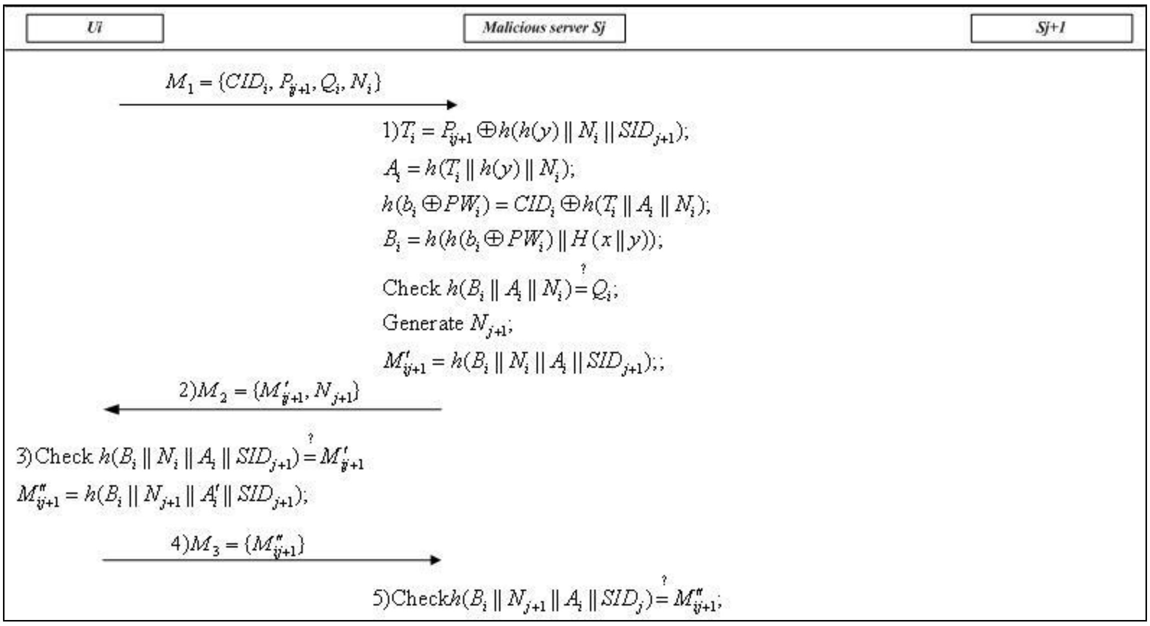

Figure 4: Server spoofing attack

Then S_j computes $h(B_i||A_i||N_i)$ and checks it with Q_i. If they are not equal, S_j rejects the login request and terminates this session. Otherwise, S_j generates a random number N_{j+1} to compute $M'_{ij+1} = h(B_i| \, |N_i \, ||A_i \, ||SID_{j+1})$. Finally, S_j sends the message $M_2=\{M'_{ij+1}, N_{j+1}\}$ to U_i.

2). Upon receiving M_2, U_i checks whether $h(B_i||A_i||SID_{j+1})$ equals M'_{ij+1}. If they are not equal, U_i stops the session. Otherwise, U_i computes $M''_{ij+1} = h(B_i| \, |N_{j+1} \, ||A_i \, ||SID_{j+1})$. At last, U_i sends $M_3=\{M''_{ij}\}$ to S_j.

It is easy to say that S_j could impersonate S_{j+1}

successfully. Besides, U_i and S_j can compute $SK = h(B_i|| N_i ||N_{j+1}||A_i||SID_{j+1})$ as the session key for future communications. Therefore, Lee et al.'s scheme cannot resist the server spoofing attack.

3.3 Off-line Password Guessing Attack

Although Lee et al. claim that their scheme can provide two-factor security, i.e. the user's password is secure even when the client's smart card is lost and the parameters in the card are derived [13], an off-line password guessing attack will be given here.

Suppose the client's smart card is lost, an attacker A can read all the data, including $\{V_i, B_i, H_i, h(), h(y), b\}$, from the smart card via physically access to the storage medium. He can get the password through the following steps.

1). A selects a password PW' from a uniformly distributed dictionary.

2). A computes $T_i=V_i \oplus h(ID_i||h(b \oplus PW'))$ and $H'_i=h(T_i)$.

3). A check if H'_i equals H_i. If H'_i equals H_i, then A find the correct passwords. Otherwise, A repeats Steps 1, 2 and 3 until the correct password if found.

From the description we know that Lee et al.'s scheme could get user's password once user's smart card is lost. Therefore, Lee et al.'s scheme cannot resist the off-line password guessing attack.

4 Conclusion

In [13], Lee et al. proposed a dynamic ID-based remote user authentication scheme for multi-server environment using smart cards and demonstrated its immunity against various attacks. However, after review of their scheme and analysis of its security, three kinds of attacks, i.e., impersonation attack, server spoofing attack, and off-line password guessing attack, are presented in different scenarios. The analyses show that the scheme is insecure for practical application.

Acknowledgments

The authors thank Prof. Min-Shiang Hwang and the anonymous reviewers for their valuable comments. This research was supported by the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20110141120003), the National Natural Science Foundation of China (No. 61101112), and the China Postdoctoral Science Foundation (No. 2011M500775).

References

[1] C. Chang and J. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in *Proceedings of the IEEE international conference on cyberworlds*, pp. 417-422, 2004.

[2] D. He, "An efficient remote user authentication and key exchange protocol for mobile client-server environment from pairings," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1009-1016, 2012.

[3] D. He, "Cryptanalysis of an authenticated key agreement protocol for wireless mobile communications," *ETRI Journal*, vol. 34, no. 3, pp. 482-484, 2012.

[4] D. He, J. Chen and J. Hu, "Further improvement of Juang et al.'s password-authenticated key agreement scheme using smart cards," *Kuwait Journal of Science & Engineering*, vol. 38, no. 2A, pp. 55-68, 2011.

[5] D. He, J. Chen and J. Hu, "An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security," *Information Fusion*, vol. 13, no. 3, pp. 223-230, 2012.

[6] D. He, J. Chen, J. Hu, "Improvement on a smart card based password authentication scheme," *Journal of Internet Technology*, vol. 13, no. 3, pp. 405-409, 2012.

[7] D. He, J. Chen and R. Zhang, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989-1995, 2010.

[8] D. He, Y. Chen and J. Chen, "Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol," *Nonlinear Dynamics*, vol. 69, pp. 1149-1157, 2012.

[9] D. He and Y. Huang, "Weaknesses in a dynamic ID-based remote user authentication scheme for multi-server environment," *International Journal of Electronic Security and Digital Forensics*, vol. 4, no. 1, pp. 43-53, 2012.

[10] H. Hsiang and W. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standard & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[11] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Transaction on Consumer Electronics*, vol. 50, no. 1, pp. 251–255, 2004.

[12] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, vol. 24, pp. 770-772, 1981.

[13] C. Lee, T. Lin, and R. Chang, "A Secure Dynamic ID based Remote User Authentication Scheme for Multi-server Environment using Smart Cards," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13863-13870, 2011.

[14] S. Lee and K. Sivalingam, "An efficient one-time password authentication scheme using a smart card," *International Journal of Security and Networks*, vol. 4, no. 3, pp. 145-152, 2009.

[15] Y. Li, J. Ma and Q. Jiang, “Mutual authentication scheme with smart cards and password under trusted computing,” *International Journal of Network Security*, vol. 14, no. 3, pp. 156-163, 2012.

[16] L. Li, I. Lin and M. Hwang, “A remote password authentication scheme for multi-server architecture using neural networks,” *IEEE Transactions on Neural Network*, vol. 12, no. 6, pp. 1498–1504, 2001.

[17] Y. Liao, and S. Wang, “A secure dynamic ID based remote user authentication scheme for multi-server environment,” *Computer Standard & Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.

[18] I. Lin, M. Hwang and L. Li, “A new remote user authentication scheme for multi-server architecture,” *Future Generation Computer Systems*, vol. 1, no. 19, pp. 13–22, 2003.

[19] R. Ramasamy, A. Muniyandi, “An efficient password authentication scheme for smart card,” *International Journal of Network Security*, vol. 14, no. 3, pp. 180-186, 2012.

[20] S. Sood, “An improved and secure smart card based dynamic identity authentication protocol,” *International Journal of Network Security*, vol. 14, no. 1, pp. 39-46, 2012.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a lecturer of Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Weijing Zhao received his B.S. and M.S. degrees in Mathematics from Tianjin Normal University in 2006 and 2009, respectively. Currently, he is a Ph.D. candidate at the Dalian University of Technology. His research interests are information security and fuzzy systems.

Shuahua Wu is a lecture of Networks Engineering Department, Information Engineering University, Zhengzhou, China. Currently, he is a postdoctor at the Department of Computer Science and Engineering, Shanghai Jiaotong University. His research interests include cryptology and communication protocols.