Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080443

Cryptanalysis of a New Dynamic ID-based User Authentication Scheme to Resist Smart-Card-Theft Attack

Fengtong Wen[1,*], *Dianli Guo*[1] *and Xuelei Li*[2]

[1] School of Mathematical Sciences, University of Jinan, Jinan, 250022, China
[2] Institute of Network Technology, Beijing university of posts and Telecommunications, Beijing, 100876, China

Received: 12 Aug. 2012, Revised: 14 Feb. 2013, Accepted: 15 Feb. 2013
Published online: 1 Jul. 2014

Abstract: In a recent paper (AMIS, 6(2S), 2012), Lee proposed a dynamic ID-based user authentication scheme based on smart card which is believed to have many abilities to resist a range of network attacks. In this paper, we analyze the security of Lee's scheme and show that the scheme is in fact insecure against insider-assisted attack, even if the adversary doesn't know the secret information stored in the smart card. In addition, the adversary can perform off-line guessing attack and impersonation attack if the secret information stored in the smart card is compromised.

Keywords: Cryptanalysis, Dynamic ID, Smart card, Authentication, Password

1 Introduction

With the rapid development of Internet technology, people can easily access resources via distributed and complicated networks with kinds of portable equipments (e.g., mobile phones, PDAs and notebook computers). On the other hand, due to the open nature of the Internet, it also brings kinds of network security problems. To authenticate remote users, we need a more secure remote password authentication scheme to resist kinds of attacks.

In 1981, Lamport [1] proposed a password authentication scheme. However, it is based on static login ID. The static ID may lead to the compromise of the partial information in the login message. In 2004, Das et al. [2] proposed a remote user authentication scheme based dynamic ID using smart cards. The dynamic ID schemes can eliminate the risk of partial information leakage and avoid the ID-theft attack. Their scheme also allowed users to choose and change their passwords freely, and the server did not need to maintain a verifier table. They claimed that their scheme can resist ID-theft attack, forgery attack, replay attack, guessing attack, and insider attack. Unfortunately, after that, many researches have shown that Das et al.'s scheme is completely insecure and vulnerable to various of attacks. In 2004, Awasthi [3] analyzed several weaknesses of Das et al.'s scheme and showed that their scheme is completely insecure. Chien and Chen [4] pointed out that Das et al.'s scheme fails to protect the anonymity of users and proposed an improved remote authentication scheme in 2005. In the same year, Ku and Chang [5] also showed that the adversary can easily impersonate legal users to login the server using Das et al.'s scheme. Furthermore, Ku and Chang pointed out that Das et al.'s scheme is vulnerable to insider attack. In the same year, Liao et al. [6] demonstrated that Das et al.'s scheme is susceptible to guessing attack and proposed an improved scheme to remedy this security flaw. In 2009, Wang et al. [7] proposed an improved scheme based dynamic ID with mutual authentication, and proved that their scheme is more secure. However, many researches [8,9,10] demonstrated that Wang et al.'s proposal is vulnerable to various attacks such as randomly chosen password attack and impersonation attack, and the corresponding enhanced measures are proposed respectively. In 2012, Lee [11] identified that Das et al.'s scheme is insecure for guessing attack and impersonation attack, and proposed an improved scheme. His proposal not only remedied these weaknesses of Das et al.'s scheme but also kept the merits of the original scheme. Under the assumption that

[*] Corresponding author e-mail: wftwq@163.com

Table 1: Notations

Notation	Meaning
U_i	The *ith* user
S	The remote server
ID_i	The identity of the user U_i
P_i	The password of the user U_i
x	The master secret key of S
DID_i	The dynamic identity of U_i
T	The time stamp
$H(\cdot)$	A one-way hash function
$\oplus$	Exclusive-OR operation

smart cards were tamperproof, he/she proved that his/her scheme can resist impersonation attack, guessing attack and smart-card-theft attack. However, Kocher and Messages [12,13] have mentioned that the information stored in smart cards can be extracted by the adversary using monitoring the power consumption.

Our Contributions. In this paper, we mainly show there exist several serious security flaws in Lee's dynamic ID-based user authentication scheme, which are described as follows: 1) It is vulnerable to insider-assisted attack, even if the adversary doesn't know the secret information stored in the smart card. 2) It cannot resist impersonation attack and off-line guessing attack if the secret information stored in the smart card is compromised.

Organization of the Paper. The rest of this paper is organized as follows. In section 2, a brief review of Lee's scheme is given. Then, we analyze the weaknesses of Lee's scheme in section 3. Section 4 concludes the paper.

2 Review of Lee's scheme

In this section, we only review the Registration phase and Authentication phase of Lee's scheme. Readers may refer to [11] for the password update phase. The notations used in Lee's scheme are summarized in Table 1.

2.1 Registration phase

The steps of the registration phase are as follows:

Step 1: U_i sends his/her password P_i to S via a secure communication channel.

Step 2: After receiving P_i, S computes

$$N_i = H(P_i) \oplus H(x),$$

and stores

$$\{N_i, H(\cdot),\ H(x)\}$$

in U_i's smart card. Then, S issues it to U_i over a secure channel.

2.2 Authentication phase

The authentication phase contains login phase and verification phase.

2.2.1 Login phase

Step 1: The user U_i inserts his/her smart card into the device and enters his/her password P_i.

Step 2: The smart card generates a random number R and computes the dynamic identity

$$DID_i = H(P_i) \oplus H(N_i \oplus H(x) \oplus R),$$
$$B_i = H(N_i \oplus H(N_i \oplus H(x) \oplus R)),$$
$$C_i = H(B_i \oplus H(x) \oplus T).$$

Step 3: U_i sends the login request message

$$\{DID_i,\ C_i,\ T\}$$

to the server.

2.2.2 Verification phase

Step 1: On receiving the login message

$$\{DID_i,\ C_i,\ T\},$$

S checks the validity of timestamp T by checking $T' - T \leq \triangle T$, where T' is time when S receives the login message. If $T' - T \leq \triangle T$ holds, S accepts the login request of U_i. Otherwise, S rejects the login request.

Step 2: S computes

$$\begin{aligned} B_i &= H(DID_i \oplus H(x)) \\ &= H(H(P_i) \oplus H(N_i \oplus H(x) \oplus R) \oplus H(x)) \\ &= H(N_i \oplus H(N_i \oplus H(x) \oplus R)). \end{aligned}$$

Step 3: S computes

$$C_i^* = H(B_i \oplus H(x) \oplus T)$$

and verifies whether it is equal to the received C_i. If yes, the legitimacy of U_i can be sure. Otherwise, S rejects the login request and terminates the operation.

3 Cryptanalysis of Lee's scheme

We assume that an attacker A has the ability to control over the communication channels between users and the remote server S, which means that he/she can insert, delete, or modify any messages in the channel. Firstly, we show that the attacker can perform an insider-assisted attack without knowing the secret information stored in the smart card. Secondly, we demonstrate that Lee's scheme is susceptible to impersonation attack and off-line password guessing attacks if the adversary A has the additional ability to reveal the secret information stored in smart cards.

3.1 Insider-assisted attack

If an adversary A is a legal user of S, he/she can imitate as another legal user U_i to login S without knowing U_i's passwords and secret information stored in the smart card. The concrete steps are as follows:

Step 1. A eavesdrops $U_i's$ login request message $\{DID_i,\ C_i,\ T\}$ and gets the information $\{H(\cdot),\ H(x)\}$ from his/her own smart card.

Step 2. A computes $B_i = H(DID_i \oplus H(x))$, $C_i' = H(B_i \oplus H(x) \oplus T')$, where T' is the current timestamp. Then A sends the forged login request message

$$\{DID_i,\ C_i',\ T'\}$$

to the remote server S.

Step 3. After receiving the login request message from A, S successfully verifies the validity of timestamp T', and computes

$$B_i = H(DID_i \oplus H(x)),$$
$$C_i'^{*} = H(B_i \oplus H(x) \oplus T').$$

It is easy to see that

$$C_i'^{*} = C_i'.$$

So the malicious user A can perform an impersonation attack.

3.2 Impersonation attack

In this section, we show that Lee's scheme is vulnerable to impersonation attacks if U_i's smart card is stolen and an attacker A has extracted all the information $\{H(\cdot),\ N_i,\ H(x)\}$ stored in the smart card.

Step 1. A computes $H(P_i) = N_i \oplus H(x)$,

Step 2. A generates a random number R' and compute

$$DID_i' = H(P_i) \oplus H(N_i \oplus H(x) \oplus R'),$$

$$B_i' = H(N_i \oplus H(N_i \oplus H(x) \oplus R')),$$
$$C_i' = H(B_i' \oplus H(x) \oplus T'),$$

where T' is the current timestamp.

Step 3. A sends the forged login request message

$$\{DID_i',\ C_i',\ T'\}$$

to the remote server S.

Step 4. Upon receiving $\{DID_i',\ C_i',\ T'\}$, S verifies the validity of T' and then computes

$$B_i' = H(DID_i' \oplus H(x))$$

$$= H(H(P_i) \oplus H(N_i \oplus H(x) \oplus R') \oplus H(x))$$
$$= H(N_i \oplus H(N_i \oplus H(x) \oplus R')),$$
$$C_i'^{*} = H(B_i' \oplus H(x) \oplus T'),$$

It is easy to see that $C_i'^{*} = C_i'$. Then the adversary can be authenticated by S.

3.3 Off-line password guessing attack

If the user's smart card is stolen and the secret information $\{H(\cdot),\ N_i,\ H(x)\}$ stored in the smart card is extracted. Then the adversary can compute $H(P_i) = N_i \oplus H(x)$. So he/she can perform the off-line password guessing attack.

4 Conclusion

In this paper, we review Lee's a new dynamic ID-based user authentication scheme to resist smart-card-theft attack. We show that his/her scheme does not satisfy some of their security claims. This protocol is vulnerable to insider-assisted attack, off-line guessing attack and impersonation attack.

Acknowledgement

The authors thank the anonymous referee for their helpful comments. This work is supported by Natural Science Foundation of Shandong Province (NO. ZR2013FM009).

References

[1] L. Lamport, Password authentication with insecure communication, Commun ACM, **24**, 770-772 (1981).

[2] M. L. Das, A. Saxena, V. P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Trans on Consumer Electronics, **50**, 665-667 (2004).

[3] A. K. Awasthi, Comment on a dynamic ID-based remote user authentication scheme, Transactions on Cryptology, **1**, 15-16 (2004).

[4] H. Y. Chien and C. H. Chen, A remote password authentication preserving user anonymity, In Proc. 19th International Conference on Advanced Information Networking and Applications (AINA'05), **2**, 245-248 (2005).

[5] W. C. Ku, S. T. Chang, Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards, IEICS Transactions on Communication, **E88-B**, 2165-2167 (2005).

[6] I. Liao, C. C. Lee, M. S. Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme, In:Proc. International Conference on Next Generation Web Services Practices (NWeSP'05), **1**, 437-440 (2005).

[7] Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications, **32**, 583-585 (2009).

[8] H. Lee, D. Choi, D. Won and S. Kim, Security weaknesses of dynamic ID-based remote user authentication protocol, In: Proc. World Academy of Engineering and Technology, **1**, 190-193 (2009).

[9] M. K. Khan, S. K. Kim, K. Alghathbar, Cryptanalysis and security enhancement of a'more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, **34**, 305-309 (2011).

[10] F. T. Wen, X. L. Li, An improved dynamic ID-based remote user authentication with key agreement scheme, Computers and Electrical Engineering, **38**, 381-387 (2011).

[11] Y. C. Lee, A new dynamic ID-based user authentication scheme to resist smart card theft attack, Applied Mathematics and Information Sciences, **6**, 355s-361s (2012).

[12] P. Kocher, J. Jaffe and B. Jun, Differential power analysis: 19th Annual international cryptology conference, 388-397 (1999).

[13] T. S. Messerges, E. A. Dabbish, and R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans Comput., **51**, 541-552 (2002).

Fengtong Wen is associate professor of school of mathematical sciences, university of jinan. He received the PhD degree in Cryptography at Beijing university of posts and Telecommunications. His main research interests are information security and cryptography.

Dianli Guo is Master student of school of mathematical sciences, university of jinan. He received the Bachelor degree in applied mathematics at Heze college. His main research interests is cryptography.

Xuelei Li is PhD student of Beijing university of posts and Telecommunications. He received the Master degree in applied mathematics of university of jinan. His main research interests is cryptography.