Cryptanalysis of Liao-Lee-Hwang's Dynamic ID Scheme

Mohammed Misbahuddin[1] and C. Shoba Bindu[2]
(Corresponding author : Mohammed Misbahuddin)
Department of Computer Science and Information Technology, Maulana Azad National Urdu University[1]
Gachi bowli, Hyderabad, Andhra Pradesh, India (Email: mdmisbahuddin@yahoo.com)
Department of Computer Science and Engineering, JNTU College of Engineering[2]
Anantapur, Andhra Pradesh, India

(Received Mar. 14, 2006; revised and accepted May 7, 2006)

Abstract

Recently, Das, Saxena and Gulati proposed a dynamic Id based remote user authentication scheme that allows the users to choose and change their passwords freely and does not maintain verifier table. But their scheme has few weaknesses and cannot achieve mutual authentication. In 2005, Liao, Lee and Hwang showed that Das et al. scheme is vulnerable to guessing attack and proposed an enhanced scheme which also achieves mutual authentication. In this paper we show that Liao et. al's. scheme cannot withstand impersonation attack, reflection attack and it is completely insecure as a user can successfully log on to a remote system with a random password.

Keywords: Authentication, dynamic ID, impersonation attack, guessing attack, smartcard

1 Introduction

The smart card based remote user authentication is a very practical solution to create a secure distributed computer environment. Remote User Authentication schemes allow the user to login to the remote system to access the services offered. Ever since Lamport in 1981 proposed a remote user authentication scheme [5], several other remote user authentication schemes have been proposed. Most of those schemes were based on Static ID. There are numerous applications where static ID leaks partial information about the user's login message. In 2004 Das et al. proposed a dynamic ID based remote user authentication scheme [4]. They claimed that their scheme is secure against ID-theft, and can resist the replay attack, forgery attack, guessing attack, insider attack and stolen verifier attack.

In 2004 Awasthi and Lal [1] have shown that Das et al's scheme has several weaknesses and is completely insecure. In 2005 Wei-Chi Ku and Shen-Tein Chang [8] have shown that Das et al. scheme is insecure against Impersonation attack.

Recently, Liao, Lee and Hwang [6] analyzed the security of Das et al. scheme and showed that Das et al. scheme is vulnerable to guessing attack and does not provide mutual authentication. To enhance the security of Das et al. scheme Liao et al. proposed few modifications, moreover their scheme achieves mutual authentication.

In this paper, we show that though Liao et al. scheme is secure against guessing attack, but some weaknesses still exists [1, 8]. In addition, the scheme fails to achieve mutual authentication.

The paper is organized as follows. In Section 2 we review Liao et al's scheme. In Section 3 we analyze the security of Liao et al's scheme. Finally in Section 4 we will give a brief conclusion.

2 Review of Liao-Lee-Hwang Enhanced Scheme

The scheme is composed of two parts, namely, the registration phase and the authentication phase. The registration phase is performed only once, and the authentication phase is executed every time the user logs into the system. The notations used throughout this paper are as follows:

U:	The user.
ID:	The user identity
PW:	The password of U.
S:	The remote system.
$h(.)$:	A one-way hash function.
$\bigoplus$:	Bitwise XOR operation.
$\|$:	Concatenation
$A \Rightarrow B$:	A sends M to B through a secure channel.
$A \rightarrow B : M$:	A sends M to B through insecure channel.

Registration Phase:
This phase is invoked whenever a user U registers with the remote system. The user submits the identity ID and chooses password PW and submits ID and $h(PW)$ to the

remote system through secure channel. Upon receiving the registration request, the remote system performs the following steps:

Step R1: Computes a nonce $N = h(PW) \oplus h(x||ID)$, where x is a secret key of the remote system

Step R2: Personalizes the smart card with the parameters $h(.)$, N and y ; where y is the remote system's secret number stored in each registered user's smart card.

Step R3: S sends Smart card to U.

Authentication Phase:
The user U inserts his smart card to the card reader of a terminal, and keys his password PW. Then, the smart card will perform the following operations:

Step L1: Computes $CID = h(PW) \oplus h(N \bigoplus y \bigoplus T)$, where T is the current date and time of U's system.

Step L2: Computes $B = h(CID \oplus h(PW))$.

Step L3: Computes $C = h(T \oplus N \oplus B \oplus y)$.

Step L4: $U \rightarrow S : (CID, N, C, T)$.

Upon receiving the login message (CID, N, C, T) at time T', the remote system authenticates the user U with the following steps:

Step V1: Verify the validity of the time interval between T and T'. If $(T' - T) \leq \triangle T$, S accepts U's login request, otherwise rejects, where $\triangle T$ denotes the valid time interval.

Step V2: Computes $h(PW) = CID \oplus h(N \oplus y \oplus T)$.

Step V3: Computes $B = h(CID \oplus h(PW))$. Thereafter, checks whether $C = h(T \oplus N \oplus B \oplus y)$. If it holds, the remote system accepts the login request. Otherwise, rejects the login request and terminates the operation. Then S computes $D = h(T^* \oplus N \oplus B \oplus y)$, where T^* is the time stamp.

Step V4: $S \rightarrow U : (D, T^*)$.

Step V5: Upon receiving the reply message at the time T", U verifies if whether $(T" - T^*) \leq \Delta T$, where ΔT is an expected valid time interval. If it holds, U computes $h(T^* \oplus N \oplus B \oplus y)$ and compares it with the received D. If it holds, U confirms that he/she communicates with valid S.

3 Security Analysis

Authentication Phase is Password Independent:
In Login phase if a user keys a random password P instead of his real password PW, then CID, B and C will be computed using the random password P as follows:

$$\begin{aligned} CID &= h(P) \oplus h(N \oplus y \oplus T) \\ B &= h(CID \oplus h(P)) \\ C &= h(T \oplus N \oplus B \oplus y). \end{aligned}$$

In verification phase:

$$\begin{aligned} h(P) &= CID \oplus h(N \oplus y \oplus T) \\ B' &= h(CID \oplus h(P)) \\ C' &= h(T \oplus N \oplus B' \oplus y). \end{aligned}$$

Since C' is equivalent to C the login request will be accepted. Hence even with any random password user may access the server.

Impersonation Attack:
In verification phase Impersonation Attack is possible as: Assume that an adversary has intercepted one of U's previous login messages; say $\{CID, N, C, T\}$. If the adversary attempts to impersonate U to login S at time $T^{**}(> T)$, an Impersonation attack can be performed as in the following:

Step I1: The adversary computes $\Delta t = T \oplus T^{**}$ and $N' = N \oplus \Delta t$.

Step I2: Adversary sends (CID, N', C, T^{**}) to S.

Step I3: Since T^{**} is valid, i.e., fresh, S will proceed to compute

$$\begin{aligned} h(PW) &= CID \oplus h(N' \oplus y \oplus T^{**}) \\ &= CID \oplus h((N \oplus \Delta t) \oplus y \oplus (T \oplus \Delta t))). \end{aligned}$$

Next, S computes

$$\begin{aligned} B &= h(CID \oplus h(PW)) \\ C &= h(T^{**} \oplus N' \oplus B \oplus y) \\ &= h((T \oplus \Delta t)(N \oplus \Delta t) \oplus B \oplus y)). \end{aligned}$$

Since the computed result equals the received C, S accepts the adversary's login request.

Reflection Attack:
When a user wants to login to the remote system, the user computes a login message and sends it to the remote system, upon receipt of the login message the remote system verifies it. On successful verification the remote system then computes a new message and sends it to the user which is then verified by the user to authenticate the server.

Assume that an adversary has intercepted and blocked the message transmitted in Step L4 i.e, (CID, N, C, T). He can then attempt to impersonate S to U by performing reflection attack as follows.

Step RA1: The adversary intercepts and blocks the message transmitted in step L4 i.e, (CID, N, C, T).

Step RA2: The Adversary then sends (C, T) to U.

Step RA3: Upon receipt of the message, if the timestamp T is valid the user U computes $h(T \oplus N \oplus B \oplus y)$ which is equivalent to the received C.

Therefore, the adversary can successfully impersonate S to make the user believe that user is communicating with the remote system. Hence, Liao et al's scheme fails to achieve mutual authentication.

4 Conclusion

In this paper we highlighted the vulnerabilities of Liao-Lee-Hwang's Dynamic ID scheme. Though modified scheme seems to do well against guessing attack, we showed that the scheme is completely insecure since the authentication phase is password independent and is prone to impersonation attack and reflection attack.

References

[1] A. K. Awasthi and S. Lal, "Comment on a dynamic ID-based remote user authentication scheme," *Transaction on Cryptology*, vol. 1, no. 2, pp. 15-16, Aug. 2004.

[2] C. C. Chang and K. F. Hwang, "Some forgery attack on a remote user authentication scheme using smart cards," *Informatics*, vol. 14, no. 3, pp. 189-294, 2003.

[3] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions Consumer Electronic*, vol. 46, pp. 992-993, 2000.

[4] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629 -631, May 2004.

[5] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[6] I. Liao, C. C. Lee, and M. S. Hwang, "Security enhancement for a dynamic ID based remote user authentication scheme," in *Proceedings of the national conference on Next Generation Web Services Practices (NWeSP'05)*, pp. 4, 2005

[7] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smartcard," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204-207, Feb. 2004.

[8] W. C. Ku and S. T. Chen, "Impersonation attack on a dynamic ID based remote user authentication using smartcards," *IEICE Transactions on Communications*, vol. e88-b, no. 5, pp. 2165-2167, May 2005.

Md. Misbahuddin received his B.Tech Degree in Computer Science & Engineering from K.B.N. College of Engineering, Gulbarga University, Gulbarga, Karnataka, India in 2001; Mater of Technology in Software Engineering from Jawahar Lal Nehru Technological University, Anantapur, India. He is presently working as System Administrator in Maulana Azad National Urdu University; Hyderabad, India. His area of interest includes Network Security, Image Processing, Pattern Recognition and Software Engineering.

C. Shoba Bindu received her B.Tech Degree in Electronics & Comm. Engineering from Jawahar Lal Nehru Technological University, Anantapur, India, in 1997; M.Tech in Computer Science & Engineering from Jawahar Lal Nehru Technological University, Anantapur, India, in 2002. She is currently pursuing her Ph.D in Computer Science at Jawahar Lal Nehru Technological University, Anantapur, A.P., India. Her Current Research Interest include Network Security and Wireless Communication Systems.