Two Attacks on the Wu-Hsu User Identification Scheme

Cheng-Chi Lee

Department of Computer Science, National Chung Hsing University,
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Department of Computer & Communication Engineering, Taichung Healthcare and Management University,
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.

(Received April 20, 2005; revised and accepted May 18, 2005)

Abstract

In 2000, Lee and Chang proposed a user identification scheme with key distribution preserving anonymity for distributed computer networks. Recently, Wu and Hsu pointed out that there are two weaknesses in the Lee-Chang scheme. They further not only proposed a new scheme to remedy the security leaks of the Lee-Chang scheme, but also reduced computation complexities and communication cost as compared with the Lee-Chang scheme. However, in this article we show that there are two attacks in their scheme.

Keywords: Anonymity, distributed computer networks, key distribution, user identification

1 Introduction

In 2000 [3], Lee and Chang proposed a user identification scheme based on the security of the factoring problem and the one-way hash function [1, 2]. Their scheme can let the service provider identify the legal user and, in the meanwhile, agree on session key with the user for distributed computer networks.

There are four advantages in the Lee-Chang scheme. The first is that users can request services without revealing their identities to public. The second is that each user needs to maintain only one secret. The third is that it is not required for service providers to record the password files for the users. The fourth is that no master key updating is needed if a new service provider is added into the system.

However, in 2004 [4], Wu and Hsu showed that there are two weaknesses in the Lee-Chang scheme. To remedy theses two weaknesses, they further proposed an efficient scheme. Their scheme can reduce the computation complexities and communication cost as compared with the Lee-Chang scheme. However, in this article, we show that the Wu-Hsu scheme can not resist two attacks.

2 The Review of the Wu-Hsu User Identification Scheme

In Wu-Hsu scheme [4], it consists of two phases: key generation and anonymous user identification. In key generation phase, there is a Smart Card Producing Center, denoted as SCPC, whose initializes the system parameters, maintains public information, and assigns a secret token to each system member. In anonymous user identification phase, the service provider can identify a legal user and agree on a session key with the user. The details of these two phases are described in the following:

Keg Generation

First, SCPC selects two large primes p and q, computes $N = pq$, and picks an element $g \in Z_N^*$ and a hash function f. After, SCPC selects a secret key d and then computes a public key e such that $ed = 1 \bmod (p-1)(q-1)$. Finally, some parameters $N, e, g,$ and f are public. And d, p, and q are kept secret by SCPC. Each user can be assigned a secret token S_i by SCPC. SCPC computes

$$S_i = ID_i^d \bmod N,$$

where ID_i is the identity of user U_i or service provider P_i. Then SCPC sends S_i to each user U_i (or P_i) through a secure channel.

Anonymous User Identification

If U_i wants to request services from a service provider P_j, he/she submits a service request to P_j. Upon receiving the request, P_j chooses a random number k and computes $z = g^k S_j \bmod N$ which is then sent to U_i. After receiving the z, U_i chooses a random number t and computes $a = z^e/ID_j \bmod N$, $x = S_i f(a^t||T) \bmod N$, and $y = g^{et} \bmod N$, where T is the timestamp. After that, U_i sends (x, y, T) to P_j. Finally, P_j checks T and verifies the following equation:

$$ID_i = (x/f(y^k||T))^e \bmod N.$$

If it holds for some ID_i existing in the identity list, U_i is accepted as an authorized user and the service request will be granted. After the user identification, the user and the service provider can agree on a common session key as

$$K_{ij} = a^{tx} = y^{kx} = g^{ektx} \bmod N.$$

3 Two Attacks on the Wu-Hsu User Identification Scheme

In this section, we propose two attacks on the Wu-Hsu user identification scheme. The details of the two attacks are described in the following:

[**Attack 1**]
A legal user U_i can create a valid pair of (ID_f, S_f) without knowing the secure key d of the SCPC. If the created ID_f exists in the identity list of the service provider, U_i can forge U_f to login the service provider and request service from the service provider. Now, U_i has a valid pair of (ID_i, S_i), and he/she wants to create a valid pair of (ID_f, S_f) such that satisfies $S_f = ID_f^d \bmod N$. First, U_i can compute ID_f as follows:

$$ID_f = ID_i^n \bmod N,$$

where $n \geq 2$. After that, he/she can derive $S_f = ID_f^d \bmod N$. Although he/she does not know the secure key of the SCPC, he/she can easily create a valid pair of (ID_f, S_f). He/She computes S_f as follows:

$$\begin{aligned} S_f &= ID_f^d \bmod N \\ &= (ID_i^n \bmod N)^d \bmod N \\ &= (ID_i^n)^d \bmod N \\ &= (ID_i^d)^n \bmod N \\ &= (S_i)^n \bmod N. \end{aligned}$$

After that, U_i can use the self-constructed pair of (ID_f, S_f) to login the service provider.

[**Attack 2**]
An attacker U_f can forge a legal user U_i to login a service provider. He/She can derive the $S_i = ID_i^d \bmod N$ without knowing the secret key d of the SCPC. First, the attacker can choose a random number r such that $gcd(r, N) = 1$. Then, he/she computes ID_f as follows:

$$ID_f = ID_i^r \bmod N.$$

After that, the attacker submits the ID_f to the SCPC. The SCPC will assign a secret token $S_f = ID_f^d \bmod N$ to the U_f. Now, the attacker can derive S_i as follows:

$$\begin{aligned} S_f^{-r} \bmod N &= (ID_f^d)^{-r} \bmod N \\ &= ((ID_i^r)^d)^{-r} \bmod N \\ &= ID_i^d \bmod N \\ &= S_i \bmod N. \end{aligned}$$

After that, U_f can forge the legal user U_i to login the service provider.

4 Conclusion

In this article, we have shown that the Wu-Hsu user identification scheme is vulnerable to two attacks as shown in Section 3. An attacker can forge another legal user to login the service provider.

References

[1] C. C. Chang and M. S. Hwang, “Parallel computation of the generating keys for RSA cryptosystems,” *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[2] M. S. Hwang, Eric J. L. Lu, and Iuon-Chang Lin, “A practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, no. 6, pp. 1552–1560, 2003.

[3] W. B. Lee and C. C. Chang, “User identification and key distribution maintaining anonymity for distributed computer networks,” *Computer Systems Science and Engineering*, vol. 15, no. 4, pp. 113–116, 2000.

[4] T. S. Wu and C. L. Hsu, “Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks,” *Computers & Security*, vol. 23, no. 2, pp. 120–125, 2004.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from the Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He researched in Computer and Information Science from the National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He is currently pursuing his Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, Republic of China. He is a Lecturer of Computer and Communication, Taichung Healthcare and Management University (THMU), from 2004. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 25 articles on the above research fields in international journals.