ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2010, Vol. 39, No. 1

WEAKNESSES AND IMPROVEMENT OF HSU-CHUANG'S USER IDENTIFICATION SCHEME

Jia-Lun Tsai

Department of Information Management, National Taiwan University of Science and Technology
Taipei 106, Taiwan, R.O.C
e-mail: crousekimo@yahoo.com.tw

Abstract. In 2004, Yang *et al.* proposed an efficient user identification scheme with key distribution. The scheme provides user anonymity, so it is possible for the user to anonymously login the remote server. Unfortunately, Mangipudi and Katti found that Yang *et al.*'s scheme suffers from a Denial-of-Service (DoS) attack and then proposed an improvement of Yang *et al.*'s scheme. However, Hsu and Chuang demonstrated that Mangipudi-Katti's scheme is vulnerable to an identity disclosure attack, and further proposed a novel user identification scheme with key distribution preserving user anonymity for distributed computer networks. They claimed that their scheme can achieve the following advantages: (1) user anonymity, (2) key distribution, (3) mutual authentication, and (4) key confirm. In this study, the author shows that Hsu-Chuang's scheme is vulnerable to three impersonation attacks. Then, the improvement of Hsu-Chuang's scheme is proposed.

Keywords: anonymity, identification, key distribution, mutual authentication, key confirmation.

1. Introduction

In general, a user identification scheme would submit the user identities during the authentication process. As more and more e-commerce applications emerge on the insecure network, there is a growing demand for protecting user's identity, so it is important to maintain the user anonymity. The meaning of 'anonymity' is that only the user can be identified by the server. A protocol with user anonymity prevents an adversary from obtaining sensitive personal information. In 2000, Lee and Chang [4] proposed a user identification scheme with key distribution maintaining user anonymity for distributed computer networks. The security of the scheme is based on the factoring problem [6] and the one-way hash function [7]. The scheme can only let the service provider identify the legal user and establish a session key with the user. Moreover, the scheme does not require any password table. Latter, in 2004, Wu and Hsu [9] showed that the Lee–Chang's scheme is insecure under server spoofing attack and the identity of the user can be exposed. By using server spoofing attack, an adversary can masquerade as a service provider to exchange a session key with a user. In addition, an adversary can reveal the identity of the user with a release session key. Then, Wu and Hsu also proposed an improved version to withstand these two attacks. Unfortunately, Yang *et al.* [10] demonstrated that Wu-Hsu's scheme is vulnerable to a compromising attack. It is possible for an adversary to derive the private keys of users who request services. Yang *et al.* also proposed an improvement of Wu–Hsu scheme to overcome the security leak and achieve the same security requirements. However, Mangipudi and Katti [5] have shown that Yang *et al.*'s scheme suffers from a Denial-of-Service (DoS) attack. To withstand such a DoS attack, Mangipudi and Katti further proposed a secure identification and key agreement protocol with user anonymity (SIKA). Since this, many studies demonstrated that above schemes suffer from impersonation attacks [2, 3, 8, 11, 12]. By using these attacks, an adversary, who has been a user (or service provider), can easily get other user's private key or the service provider's private key and masquerade as the impersonated user to request the service from the service provider and gain access. All of them also proposed the improvements of user identification scheme with user anonymity.

In 2008, Hsu and Chuang [1] found an identity disclosure attack on Yang et al.'s scheme and Mangipudi-Katti's scheme. Then, they also proposed a novel user identification scheme with key distribution preserving user anonymity for distributed computer networks. In this paper, the author finds that Hsu-Chuang's scheme is vulnerable to three impersonation attacks. Further, the author presents an improvement to repair the security flaws of Hsu-Chuang's scheme.

The rest of this paper is organized as follows. Section 2 briefly reviews the Hsu-Chuang's scheme. In

Section 3, the author shows the security leaks of the Hsu-Chuang's scheme. Section 4 proposes an improvement of the Hsu-Chuang's scheme. Finally, we give the conclusions.

2. Review of Hsu-Chuang's scheme

This section reviews Hsu-Chuang's scheme. The scheme is composed of three phases: system initialization, registration, and user identification phase. All phases of the scheme are described as follows.

2.1. System initialization phase

The Smart card producing center (SCPC) computes $N = pq$, where p and q are two prime numbers, and chooses (e, d) such that $ed = 1 \bmod \Phi(N)$, where $\Phi(N) = (p-1)(q-1)$. The SCPC randomly chooses g, which is the generator in Z_N. Then, the SCPC chooses an one-way hash function $H(.)$, and a symmetric-key cryptosystem, where $E_K(m)$ and $D_K(m)$ denote the encryption and decryption of the message m with a key K. The SCPC then publishes (e, N, g) as its public system parameters, and holds the secrecy of (d, p, q).

2.2. Registration phase

Each user U_i (or service provider P_i) must submit his/her ID_i to the SCPC for registration. Upon receiving ID_i form U_i, the private key S_i is computed as:

$$S_i = ID_i^d \bmod N . \quad (1)$$

Then, the SCPC sends S_i back to U_i (or P_i) through a secure channel.

2.3. User identification phase

All steps of user identification phase are described as follows.

Step 1. U_i submits the service request to P_j.

Step 2. P_j chooses k and then computes:

$$Z = g^k S_j \bmod N . \quad (2)$$

Step 3. P_j sends Z back to U_i.

Step 4. Upon receiving Z from P_j, U_i chooses t and computes:

$$a = Z^e ID_j^{-1} \bmod N, \quad (3)$$

$$K_{ij} = a^t \bmod N, \quad (4)$$

$$w = g^{et} \bmod N, \quad (5)$$

$$y = E_{K_{ij}}(ID_i), \quad (6)$$

$$x = S_i^{h(K_{ij}\|Z\|w\|T)} \bmod N, \quad (7)$$

where T is the current timestamp.

Step 5. U_i sends (w, x, y, T) to P_j.

Step 6. After receiving (w, x, y, T) from U_i, P_j first checks the validity of timestamp T. If it holds, P_j computes K_{ij} as follows.

$$K_{ij} = w^k \bmod N . \quad (8)$$

Step 7. P_j computes $ID_i = D_{K_{ij}}(y)$, where K_{ij} is used to decrypt y. Then, P_j checks

$$ID_i^{h(K_{ij}\|Z\|w\|T)} ?= x^e \bmod N . \quad (9)$$

If they are equal, the validity of U_i is authenticated.

Step 8. P_j computes

$$D_i = h(K_{ij} \| T' \| Z \| ID_i \| ID_j) \quad (10)$$

and then sends (D_i, T') to U_i, where T' is the current timestamp.

Step 9. After receiving (D_i, T') from P_j, U_i first checks the validity of T'. If so, U_i computes

$$D_i' = h(K_{ij} \| T' \| Z \| ID_i \| ID_j) \quad (11)$$

If they are equal, the validity of P_j is authenticated.

3. Weaknesses of Hsu-Chuang's scheme

In this section, the author shows that Hsu-Chuang's scheme is vulnerable to three impersonation attacks.

Attack-1:

Assume that an adversary, denoted as U_k, wants to obtain the private key of other legal user U_i (or service provider P_i). This adversary must first choose a random number $t \in Z_N$ and compute his identity $ID_k = ID_i \cdot t^e \bmod N$. Then, this adversary submits his identity (ID_k) to the SCPC. The SCPC uses d to generate U_k's private key S_k. The private key is computed as:

$$S_k = ID_k{}^d \bmod N = (ID_i \cdot t^e)^d \bmod N = ID_i^d \cdot t \bmod N .$$

Then, the SCPC sends S_k back to U_k through a secure channel.

Upon receiving S_k, the U_i's private key $S_i = ID_i^d \bmod N$ can be computed as follows:

$$\frac{S_k}{t} \bmod N = \frac{ID_i^d \cdot t}{t} \bmod N = ID_i^d \bmod N .$$

Now, the adversary obtains the private key $S_i = ID_i^d \bmod N$ of other legal user U_i (or service provider P_i).

Attack-2:

Assume that an adversary, who has been a legal user U_j with his identity ID_j, masquerades as the user U_i (or service provider P_i) with identity ID_i where

satisfies $ID_i = ID_j \cdot ID_j$. The U_i's private key $S_i = ID_i^d \bmod N$ can be computed as follows:

$$S_i = ID_i^d = S_j \cdot S_j = ID_j^d \cdot ID_j^d \bmod p .$$

Now, the adversary obtains the private key $S_i = ID_i^d \bmod N$ of other legal user U_i (or service provider P_i).

Attack-3:

Assume that many adversaries, who have been legal users U_k, k =1…l, cooperatively masquerade as other legal user U_i (or service provider P_i) where satisfies $ID_i = \prod_{k=1}^{l} ID_k \bmod p$. The U_i's private key $S_i = ID_i^d \bmod N$ can be computed as follows:

$$S_i = ID_i^d = \prod_{k=1}^{l} ID_k^{\ d} \bmod p .$$

Now, these adversaries obtain the private key $S_i = ID_i^d \bmod N$ of other legal user U_i (or service provider P_i).

4. Improvement of Hsu-Chuang's scheme

As stated above, the author has shown that the Hsu-Chuang's scheme is insecure against the impersonation attacks. The security leak of Hsu-Chuang's scheme comes from that the user's (or service provider's) private key $S_i = ID_i^d \bmod N$ could be computed with other user's private key (or service provider's) $S_j = ID_j^d \bmod N$. To improve these weaknesses of the scheme, the author suggests to replace the private key $S_i = ID_i^d \bmod N$ with the private key $S_i = H(ID_i)^d \bmod N$. Correspondingly, the *Eq.* (3), *Eq.* (6), *Eq.* (9), and *Eq.* (11) of user identification phase should also be modified as

$$a = Z^e H(ID_j)^{-1} \bmod N , \quad \text{(modified } Eq. \text{ (3))}$$

$$y = E_{K_{ij}}(H(ID_i)), \quad \text{(modified } Eq. \text{ (6))}$$

$$H(ID_i)^{h(K_{ij}\|Z\|w\|T)} ? = x^e \bmod N , \text{ (modified } Eq. \text{ (9))}$$

$$D_i' = h(K_{ij} \| T' \| Z \| H(ID_i) \| H(ID_j)) .$$

(modified *Eq.* (11))

With these modifications, the attacks of Section 3 will not work again.

5. Conclusion

The work shows that there are three impersonation attacks in Hsu-Chuang's scheme. An adversary can easily get other legal user's private key and masquerade as other user to gain access from service provider or get the service provider's private key to masquerade as a service provider. To cope with these weaknesses, an improvement of Hsu-Chuang's scheme is proposed to repair the security flaws of Hsu-Chuang's scheme in this paper.

References

[1] **C.L. Hsu, Y.H. Chuang.** A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks. *Information Sciences*, 179 (4), 2009, 422-429.

[2] **W.H. Kim, K.Y. Yoo.** New Anonymous User Identification and Key Establishment Protocol in Distributed Networks, Distributed Computing – IWDC 2005. *Lect. Notes Comput. Sci.* 3741, 2005, 410-415.

[3] **C.C. Lee.** Two attacks on the Wu-Hsu User Identification Scheme. *International Journal of Network Security*, 1 (3), 2005, 147-148.

[4] **W.B. Lee, C.C. Chang.** User identification and key distribution maintaining anonymity for distributed computer networks. *International Journal of Computer Systems Science and Engineering*, 15 (4), 2000, 211–214.

[5] **K. Mangipudi, R. Katti.** A secure identification and key agreement protocol with user anonymity (SIKA). *Computers and Security*, 25 (6), 2006, 420–425.

[6] **R.L. Rivest, A. Shamir, L. Adleman.** A Method for Obtaining Digital Signature and Public-key Cryptosystems. *Communications of the ACM* , 21 (2), 1978, 120-126.

[7] **B. Schneier.** Applied Cryptoraphy. 2*nd ed. John Wiley & Sons. Inc.*, 1996.

[8] **R.C. Wang, W.S. Juang, C.C. Wu, C.L. Lei.** A Lightweight Key Agreement Protocol with User Anonymity in Ubiquitous Computing Environments. *International Conference on Multimedia and Ubiquitous Engineering* (*MUE*'07), 2007, 313–318.

[9] **T.S. Wu, C.L. Hsu.** Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks. *Computers and Security*, 23 (2), 2004, 120–125.

[10] **Y. Yang, S. Wang, F. Bao, J. Wang, R.H. Deng.** New efficient user identification and key distribution scheme providing enhanced security. *Computers and Security*, 23 (8), 2004, 697–704.

[11] **E.J. Yoon, K.Y. Yoo.** Cryptanalysis of Two User Identification Schemes with Key Distribution Preserving Anonymity. *Information and Communications Security* (*ICICS* 2005), *December* 10-13, 2005, *Lect. Notes Comput. Sci.* 3783, 315–322.

[12] **E.J. Yoon, K.Y. Yoo.** Vulnerability of User Identification and Key Agreement Protocol with User Anonymity. *Future generation communication and networking* (*FGCN* 2007), 1, 2007, 516–521.

Received April 2009.