Interleaving Attack on ID-based Conference Key Distribution Schemes

Junghyun Nam, Seungjoo Kim, and Dongho Won

School of Information and Communication Engineering,
Sungkyunkwan University, 300 Chunchun-dong, Jangan-gu, Suwon-si,
Gyeonggi-do 440-746, Korea
{jhnam, skim}@ece.skku.ac.kr, dhwon@dosan.skku.ac.kr

Abstract. Recently, Jung *et al.* have demonstrated the insecurity of Xu-Tilborg's ID-based conference key distribution scheme, and in addition, have improved the scheme to fix the security flaws discovered by them. In this paper, we point out another security flaw common to both the Xu-Tilborg's scheme and the Jung *et al.*'s improved scheme. We first show that the Jung *et al.*'s scheme is vulnerable to an interleaving attack, and then make suggestions for improvement in security.

Keywords: Conference key distribution, implicit key authentication, interleaving attack.

1 Introduction

The original idea of extending the 2-party Diffie-Hellman scheme [4] to the multi-party setting dates back to the classical paper of Ingemarsson *et al.* [6], and is followed by many works [2, 10, 1, 8] offering various levels of security and complexity. Despite all the work conducted over decades, designing secure protocols for group key exchange is a non-trivial task [3, 9], especially in contexts where active adversaries are to be considered.

In 2000, Xu and Tilborg [11] proposed an ID-based conference key distribution scheme which builds on earlier work of Harn and Yang in the 2-party setting [5]. However, Jung *et al.* [7] have recently pointed out that Xu and Tilborg's scheme does not meet forward secrecy and is vulnerable to impersonation attacks. Furthermore, they have proposed an improved version of the Xu-Tilborg scheme which appears to provide resistance against their attacks. But unfortunately, there is yet another critical security flaw which is common to both the Xu-Tilborg scheme and the Jung *et al.*'s improved version. In this paper, we point out the vulnerability by mounting an interleaving attack against the Jung *et al.*'s improved scheme. Also, we offer a simple patch to address the security problems found in the schemes.

2 Review of Jung *et al.*'s Improved Scheme

The scheme consists of three phases: the initiation phase, the user registration phase, and the application phase.

2.1 Initiation Phase

The key authentication center (KAC) selects a one-way function f, a large prime p, and a primitive element α of GF(p), which are all known to the public. Then KAC chooses as its private key a random $x \in [1, p-1]$ such that $\gcd(x, p-1) = 1$, and computes its public key y as:

$$y = \alpha^x \bmod p.$$

2.2 User Registration Phase

Let $\mathcal{P}$ denote the set of all potential users. Each user $U_i \in \mathcal{P}$ submits its identity ID_i to the KAC for registration. The KAC computes for user U_i an extended identity $\mathrm{EID}_i = f(ID_i)$ and the signature (r_i, s_i) of EID_i as

$$\begin{aligned} r_i &= \alpha^{k_i} \bmod p, \\ s_i &= (\mathrm{EID}_i - k_i r_i) x^{-1} \bmod p - 1, \end{aligned}$$

where k_i is chosen randomly from $[1, p-1]$ such that $\gcd(s_i, p-1) = 1$. Here, no k_i should be used repeatedly. Then, in the application phase, s_i and r_i will be used as user U_i's private and public keys, respectively.

2.3 Application Phase

Let $\mathcal{U} = \{U_1, \ldots, U_\ell\}$ be a subset of $\mathcal{P}$ who wish to share a conference key among them. Users are arranged in a star network, with user U_1 being the chairman who plays a central role in the protocol. Now, the users in $\mathcal{U}$ perform the following four steps to generate the conference key K_c.

1. User U_1 chooses two random values $v_1, e_1 \in [1, p-1]$ such that $\gcd(v_1, p-1) = 1$ and $\gcd(e_1, p-1) = 1$. Next, user U_1 computes

$$\begin{aligned} w_1 &= y^{v_1} \bmod p, \\ n_1 &= w_1^{e_1} \bmod p, \\ \eta_1 &= (m - v_1 w_1) s_1^{-1} \bmod p - 1, \end{aligned}$$

   where $m = f(n_1 \| \mathrm{ID}_1 \| \mathrm{time})$. Then, user U_1 sends (ID_1, r_1, w_1, n_1, η_1, time) to the rest of the users.
2. Upon receiving (ID_1, r_1, w_1, n_1, η_1, time), each user $U_i \in \mathcal{U} \setminus \{U_1\}$ verifies that the following congruence holds:

$$y^m \equiv w_1^{w_1} (\alpha^{\mathrm{EID}_1} r_1^{-r_1})^{\eta_1} \pmod p. \tag{1}$$

   If the verification succeeds, user U_i chooses two random values $v_i, e_i \in [1, p-1]$, such that $\gcd(v_i, p-1) = 1$ and $\gcd(e_i, p-1) = 1$, and computes

$$\begin{aligned} w_i &= y^{v_i} \bmod p, \\ n_i &= w_1^{e_i} \bmod p, \\ \eta_i &= (f(n_i) - v_i w_i) s_i^{-1} \bmod p - 1. \end{aligned}$$

   Then user U_i sends (ID_i, r_i, w_i, n_i, η_i) to user U_1.
3. For $i \in [2, \ell]$, user U_1 verifies that the following congruence holds:

$$y^{f(n_i)} \equiv w_i^{w_i} (\alpha^{\mathrm{EID}_i} r_i^{-r_i})^{\eta_i} \pmod p. \tag{2}$$

   If the verifications are successful, user U_1 computes the conference key K_c as

$$K_c = n_1^{e_1} \bmod p.$$

Then, for $i \in [2, \ell]$, user U_1 also computes

$$z_i = K_c \cdot n_i^{e_1} \bmod p$$

and sends $(z_i, E_{K_c}(\mathrm{ID}_1))$ to user U_i, where $E_{K_c}(\mathrm{ID}_1)$ denotes the ciphertext of ID_1 encrypted using some secure symmetric cryptosystem under the key K_c.

4. After receiving $(z_i, E_{K_c}(\mathrm{ID}_1))$, each user $U_i \neq U_1$ computes the conference key K_c as

$$K_c = z_i \cdot (n_1^{e_i})^{-1} \bmod p,$$

and verifies it through decryption of $E_{K_c}(\mathrm{ID}_1)$.

3 Interleaving Attack on Jung *et al.*'s Improved Scheme

The fundamental security goal for a key distribution protocol to achieve is *implicit key authentication*. In protocols meeting this goal, each participant is assured that no one aside from the intended parties can learn the value of the session key.

In this section, we show that Jung *et al.*'s improved scheme does not provide implicit key authentication. As a simple scenario, we consider two concurrent runs of the protocol with the same participants, except that the adversary A participates only in the first run of the protocol. Namely, we assume that $\mathcal{U} = \{U_1, \ldots, U_\ell, A\}$ and $\mathcal{U}' = \{U_1, \ldots, U_\ell\}$, where $\mathcal{U}$ and $\mathcal{U}'$ denote two sets of users with respect to the first and second runs, respectively. The goal of adversary A is to share the same conference key with some of the participants of the second protocol run. To this end, the adversary A impersonates the chairman U_1 by exploiting a sequentially dependent relation among messages transmitted in the two different runs. The detailed attack scenario is as follows:

1. In the first step of the first protocol run, user U_1 sends (ID_1, r_1, w_1, n_1, η_1, time) to the other users, including the adversary A.

(1′) In the first step of the second run, the adversary A (pretending to be the user U_1) replaces the message

$$(\mathrm{ID}_1, r_1, w_1', n_1', \eta_1', \mathrm{time}')$$

sent by the second instance of U_1 with

$$(\mathrm{ID}_1, r_1, w_1, n_1, \eta_1, \mathrm{time})$$

which is sent to A by the first instance of U_1.

(2′) In the second step of the second run, each user $U_i \in \mathcal{U}' \setminus \{U_1\}$ computes w_i', n_i', and η_i' as per protocol specification, and sends

$$(\mathrm{ID}_i, r_i, w_i', n_i', \eta_i')$$

to user U_1. The honest users $U_2, \ldots, U_\ell$ should do so because the congruence (1) holds for (ID_1, r_1, w_1, n_1, η_1, time) and thus, the verification succeeds. Now, the adversary A eavesdrops on these messages sent to the second instance of U_1.

2. In the second step of the first run, for all $i \in [2, \ell]$, the adversary A replaces the message
$$(\mathrm{ID}_i, r_i, w_i, n_i, \eta_i)$$
sent by the first instance of user U_i with
$$(\mathrm{ID}_i, r_i, w'_i, n'_i, \eta'_i)$$
sent by the second instance of user U_i. In the same time period, the adversary A sends the message
$$(\mathrm{ID}_A, r_A, w_A, n_A, \eta_A)$$
to user U_1 as a participant of the first protocol run.
3. In the third step of the first run, user U_1 verifies that the congruence (2) holds for every $(\mathrm{ID}_i, r_i, w'_i, n'_i, \eta'_i)$ and for $(\mathrm{ID}_A, r_A, w_A, n_A, \eta_A)$. All these messages will pass the verification since they have been honestly formed as a response to the U_1's message. Therefore, for all $i \in [2, \ell]$, user U_1 will send
$$(z_i, E_{K_c}(\mathrm{ID}_1))$$
to user U_i, where z_i is computed as
$$z_i = K_c \cdot n_i'^{e_1} \bmod p.$$
User U_1 will also send
$$(z_A, E_{K_c}(\mathrm{ID}_1))$$
to the adversary A, where z_A is computed as
$$z_A = K_c \cdot n_A^{e_1} \bmod p.$$
4. In the fourth step of the first run, the adversary A receives $z_A = K_c \cdot n_A^{e_1} \bmod p$ from U_1 while eavesdropping on the messages sent to other users. Now, the adversary A recovers the conference key K_c as
$$K_c = z_A \cdot (n_1^{e_A})^{-1} \bmod p.$$

(3′) In the third step of the second run, the adversary A replaces each message
$$(z'_i, E_{K'_c}(\mathrm{ID}_1))$$
sent by the second instance of U_1 with
$$(z_i, E_{K_c}(\mathrm{ID}_1))$$
sent by the first instance of U_1 in the third step of the first protocol run.

(4′) Finally, in the fourth step of the second run, all but U_1 in $\mathcal{U}'$ share with the adversary A the same conference key:
$$K_c = K_c \cdot n_i'^{e_1} \cdot (n_1^{e'_i})^{-1} = z_i \cdot (n_1^{e'_i})^{-1} \bmod p,$$
while believing that the key has been established with the user U_1.

Consequently, implicit key authentication is not guaranteed in the Jung *et al.*'s improved scheme, as soon as the adversary participates in a protocol execution and is intended to be excluded from another concurrent execution with the same other participants. It can be easily observed that a similar scenario can be applied against the Xu-Tilborg scheme.

4 Improvement

The weakness of the Xu-Tilborg scheme and the Jung *et al.*'s improved scheme against the interleaving attack is mainly because the first message sent by U_1 in one protocol execution can be replayed in another concurrent execution even with a different set of participants. This allows the adversary to use her true identity in one of two sessions and to successfully masquerade as the chairman in the other session. Our simple patch to this security flaw is to modify the computation of m and the first message in the application phase to the following:

$$m = f(n_1 \| \mathrm{ID}_1 \| \ldots \| \mathrm{ID}_\ell \| \mathrm{time}),$$
$$(\mathrm{ID}_1, \ldots, \mathrm{ID}_\ell, r_1, w_1, n_1, \eta_1, \mathrm{time}).$$

With this modification, the messages transmitted in each protocol session become bounded to the identities of all the participants of that session. This prevents the adversary from mounting such an attack presented above, without compromising the efficiency of the scheme.

However, we note that both the Xu-Tilborg scheme and the Jung *et al.*'s improved scheme are still insecure in terms of semantic security since the conference key K_c is used as the encryption key in constructing the "authenticator" $Auth_{U_1} = E_{K_c}(\mathrm{ID}_1)$. This leaks some information about the conference key — the ciphertext of the known message ID_1 encrypted using some known algorithm under the key K_c — which allows the adversary A to distinguish K_c from a random key chosen from the conference-key space. The well-known approach to avoid this common error is to compute the authenticator $Auth_{U_1}$ as

$$Auth_{U_1} = H(K_c, 1)$$

and to establish a new shared conference key K as

$$K = H(K_c, 0),$$

where H is a one-way hash function.

5 Conclusion

We have presented an interleaving attack which can be applied to both the Xu-Tilborg scheme [11] and the Jung *et al.*'s improved scheme [7]. This attack highlights again the necessity that active adversaries are to be considered carefully in designing a key establishment protocol, especially in a group setting. We have also presented simple solutions to the security problems discovered in the schemes.

References

1. E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, "Provably authenticated group Diffie-Hellman key exchange," in *Proc. of 8th ACM Conf. on Computer and Communications Security (CCS'01)*, 2001, pp. 255–264.
2. M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," *Eurocrypt'94*, LNCS 950, 1994, pp. 275–286.

3. C. Boyd and J. M. G. Nieto, "Round-optimal contributory conference key agreement," in *Proc. of 6th International Workshop on Practice and Theory in Public Key Cryptography (PKC'03)*, LNCS 2567, 2003, pp. 161–174.
4. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. on Information Theory*, vol. 22, no. 6, pp. 644–654, November 1976.
5. L. Harn and S. Yang, "ID-based cryptographic schemes for user identification, digital signature, and key distribution," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 757–760, June 1993.
6. I. Ingemarsson, D. Tang, and C. Wong, "A conference key distribution system," *IEEE Trans. on Information Theory*, vol. 28, no. 5, pp. 714–720, September 1982.
7. B. Jung, S. Paeng, and D. Kim, "Attacks to Xu-Tilborg's conference key distribution scheme," *IEEE Communications Letters*, vol. 8, no. 7, pp. 446–448, July 2004.
8. J. Katz and M. Yung, "Scalable protocols for authenticated group key exchange," *Crypto'03*, LNCS 2729, 2003, pp. 110–125.
9. O. Pereira and J. J. Quisquater, "A security analysis of the Cliques protocols suites," in *Proc. of 14th IEEE Computer Security Foundations Workshop*, 2001, pp. 73–81.
10. M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *Proc. of 3rd ACM Conf. on Computer and Communications Security (CCS'96)*, 1996, pp. 31–37.
11. S. Xu and H. Tilborg, "A new identity-based conference key distribution scheme," in *Proc. of IEEE International Symposium on Information Theory*, 2000, p. 269.