LETTER

Security Analysis of an ID-based Key Agreement for Peer Group Communication

Duc-Liem VO[†a)], ***Nonmember and*** **Kwangjo KIM**[†b)], ***Member***

SUMMARY Pairing based cryptography has been researched intensively due to its beneficial properties. In 2005, Wu *et al.* [3] proposed an identity-based key agreement for peer group communication from pairings. In this letter, we propose attacks on their scheme, by which the group fails to agree upon a common communication key.

key words: *group key agreement, cryptanalysis, pairings, impersonation attack.*

1. Introduction

A group key agreement protocol allows a group of users to share a key which can be used to provide secure communication among the group. To ensure that the key is only shared with legitimate users, a group key agreement protocol should provide an authentication mechanism. These authenticated key agreement protocols play an important role in many modern collaborative and distributed applications. Smart [1] presented an authenticated key agreement protocol which only works for two parties. Lee *et al.*'s protocol [2] used a tree approach to provide group key agreement without authentication using bilinear pairings. Recently, Wu *et al.* [3] proposed an identity-based key agreement protocol for peer group communication including user authentication. However, in this letter, we propose possible attacks on this ID-based group key agreement scheme with which the group members cannot agree upon a common group key.

2. Wu *et al.*'s ID-based Key Agreement Scheme

In this section, we give a short description of Wu *et al.*'s identity-based key agreement scheme. More details of the scheme can be found in the original paper [3]. We assume that the readers understand the tree based model and how to construct a session key from session random numbers in this model.

Wu *et al.*'s ID-based key agreement scheme can be divided into four phases: key initialization, group creation, member joining, and member leaving. The Key Information Center (KIC) sets up some secret parameters for the communicating group and its members during the key initialization phase. Once the secure group system is established, the services of KIC are no longer needed, except when new users register. In the group creation phase, the group creator authenticates each member's validity and the group common key is built cooperatively. The member joining and leaving phases are performed to update a new group common key and the related blinded keys when the membership is changed.

2.1 Key Initialization

The KIC is responsible for generating system parameters and creating public and private keys for each member.

1. Select an elliptic curve E over $GF(p)$ of order q and base point P, then make them public.
2. Choose the private key $s \in Z_q^*$ and compute the public key $P_{pub} = sP$.
3. Publish the public key P_{pub}.
4. The member with identity id applies for public/private key pair to the KIC. The public key is $Q_{id} = H(id)$, where $H(\cdot)$ is a hash-to-point function, and the corresponding private key is $S_{id} = sQ_{id}$.
5. The private key S_{id} is sent securely to the member.

Denote {public, private} key pairs of the member i and the group creator as $\{Q_i, S_i\}$ and $\{Q_G, S_G\}$, respectively.

2.2 Group Creation

The group creator prepares a member list and invites the members to participate in a group session. The group creator acts as an initial group sponsor to coordinate the group key agreement. Each member submits a session random number for computing the group key and prior to key agreement, the group sponsor authenticates the members as follows:

1. The member M_i, with identity id_i, selects an ephemeral private key a_i, a session random number r_i and computes the corresponding ephemeral data X_i, Y_i and z_i:

$$X_i = a_i P \quad (1)$$

$$Y_i = h_1(time_i) S_i + a_i Q_G \quad (2)$$

$$z_i = r_i \oplus h_1(\hat{e}(Q_G, a_i P_{pub})) \quad (3)$$

   where $time_i$ is timestamp information about when M_i calculated these data. Then M_i sends the message $\{id_i, time_i, X_i, Y_i, z_i\}$ to the group creator.
2. Receiving the message from M_i, the group creator will reject if the message arrived at a longer than valid transmission delay interval, otherwise, he/she verifies the

[†]The authors are with International Research center for Information Security (IRIS), Information and Communications University (ICU), Daejeon, 305-732, Korea
a) E-mail: vdliem@icu.ac.kr
b) E-mail: kkj@icu.ac.kr

following equation:

$$\hat{e}(Y_i, P) = \hat{e}(h_1(time_i)Q_i, P_{pub})\hat{e}(Q_G, X_i) \quad (4)$$

If this equation holds, the message is sent from M_i, and he computes the session random number r_i by:

$$r_i = z_i \oplus h_1(\hat{e}(S_G, X_i)) \quad (5)$$

3. The group creator does the same step to authenticate all members and get their session random numbers.
4. The group creator computes the keys and corresponding blinded keys for each node of the key tree, then broadcasts the key tree topology and all blinded keys to all members of the group.
5. Receiving the broadcast message from the group creator, each member can compute the group communicating session key by itself.

2.3 Member Joining and Leaving

When a member sends a joining or leaving request, the joining or leaving sponsor is responsible for updating the session random number, renewing and sending key information to the group. In the joining case, the joining sponsor has to authenticate a new member as in the group creation before accepting the new member.

3. Attacks

In this section, we devise appropriate attacks on Wu *et al.*'s scheme which leads to a disagreement among the group members over a common group communication key. Our attacks include an impersonation attack and a modification of z_i attack.

3.1 Impersonation Attack

An impersonation attack on Wu *et al.*'s scheme is applied when new members authenticate themselves to the group creator or the joining sponsor in order to join the group.

Let us assume that an adversary A wants to impersonate the member M_i, A eavesdrops on an authentication message from M_i as $\{id_i, t_1, X_i, Y_i, z_i\}$. By recomputing the authentication message, A can perform an impersonation attack at time t_2 as follows:

$$\begin{aligned} Y_i' &= h_1(t_2)h_1^{-1}(t_1)Y_i \\ &= h_1(t_2)h_1^{-1}(t_1)(h_1(t_1)S_i + a_iQ_G) \\ &= h_1(t_2)S_i + h_1(t_2)h_1^{-1}(t_1)a_iQ_G \\ X_i' &= h_1(t_2)h_1^{-1}(t_1)X_i \\ &= h_1(t_2)h_1^{-1}(t_1)a_iP \end{aligned}$$

With the authentication message $\{id_i, t_2, X_i', Y_i', z_i\}$, the adversary A will pass the verification process in Eq. (4) carried out by the joining sponsor or the group creator. The correctness is shown below:

$$\begin{aligned} \hat{e}(Y_i', P) &= \hat{e}(h_1(t_2)S_i + h_1(t_2)h_1^{-1}(t_1)a_iQ_G, P) \\ &= \hat{e}(h_1(t_2)S_i, P)\hat{e}(h_1(t_2)h_1^{-1}(t_1)a_iQ_G, P) \\ &= \hat{e}(h_1(t_2)Q_i, P_{pub})\hat{e}(Q_G, h_1(t_2)h_1^{-1}(t_1)a_iP) \\ &= \hat{e}(h_1(t_2)Q_i, P_{pub})\hat{e}(Q_G, X_i') \end{aligned}$$

Therefore, the member M_i is believed to have passed authentication stage and the joining sponsor retrieves a session random number by computing the following equation:

$$r_i' = z_i \oplus h_1(\hat{e}(S_G, X_i'))$$

This session random number obviously differs from the original value computed by Eq. (5). The adversary A cannot derive the genuine session random number because he has no knowledge about how to compute Eq. (3) or Eq. (5). An adversary can mount this impersonation attack at a time when members join the group and intercepts their authentication messages. Consequently, although new members are authenticated by the sponsor, the session random numbers between the sponsor and joining members are not synchronized. Due to mismatching session random numbers, the group key cannot be agreed. As a result, the group members cannot communicate among themselves properly.

3.2 Modification of z_i Attack

Besides the impersonation attack, Wu *et al.*'s scheme also suffers from a simpler attack having the same effect. In this attack, the adversary intercepts and modifies directly the value z_i in the authentication message $\{id_i, time_i, X_i, Y_i, z_i\}$. The value z_i in the authentication message is never verified, so the group creator or sponsor could not know whether the z_i value is valid or not. Similar to the previous attack, the session random numbers are mismatched, causing a disagreement over the group communication key.

4. Concluding Remarks

In this letter, we have shown that Wu *et al.*'s ID-based key agreement for peer group communication is not as secure as stated by the authors [3]. Our proposed attacks, such as an impersonation attack and a modification of z_i attack, compromised Wu *et al.*'s scheme, causing the group to fail to agree upon a common communication key. Thus, the group members cannot communicate together.

References

[1] N.P. Smart, "Identity-based Authenticated Key Agreement Protocol based on Weil Pairing," Electron. Lett., vol. 38, no. 13, pp. 630–632, 2002.

[2] S. Lee, Y. Kim, K. Kim, and D.-H. Ryu, "An Efficient Tree-based Group Key Agreement using Bilinear Map," Applied Cryptology and Network Security, LNCS 2846, pp. 357–371, 2003.

[3] S.-T. Wu, J.-H. Chiu, and B.-C. Chieu, "Identity-based Key Agreement for Peer Group Communication from Pairings," IEICE Trans. Fundamentals E88-A, no. 10, pp. 2762–2768, Oct. 2005.