Cryptanalysis of a pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks

Qingfeng Cheng

Luoyang University of Foreign Languages
(Email: qingfengc2008@sina.com)

Abstract

Recently, Isalam and Biswas proposed a new group key agreement (GKA) protocol for imbalanced mobile networks. In this letter, we will show that Isalam et al.'s GKA protocol is not secure.

Keywords: group key agreement, imbalanced mobile networks, ephemeral key compromise attack, perfect forward secrecy

1 Introduction

Recently, Isalam and Biswas [1] proposed a new group key agreement protocol for imbalanced mobile networks, called Isalam-Biswas protocol. They claimed that their protocol was secure, efficient and contributory-based. In this letter, however, we will point out that the Isalam-Biswas protocol cannot provide perfect forward secrecy, and also cannot resist ephemeral key compromise attack.

2 Review of Isalam-Biswas Protocol

2.1 System Initialization Stage

Let k be a security parameter, G be an additive group of prime order q. P is a generator of group G. The key generation center (KGC) randomly chooses a value $s \in Z_q^*$ as the master private key and computes $P_{pub} = sP$ as its master public key. The KGC chooses two hash functions $H_0 : \{0,1\}^* \times G \to Z_q^*$ and $H_1 : \{0,1\}^* \to \{0,1\}^k$. The system parameters are $\{q, G, P, H_0, H_1\}$.

2.2 Key Extract Stage

This phase is run by the KGC for each user with an identity $ID_i \in \{0,1\}^*$. The KGC first chooses $v_i \in Z_q^*$ randomly. Then the KGC computes $R_i = v_i P$, $h_i = H_0(ID_i \| R_i)$ and $u_i = v_i + h_i s$. Finally, the user's private key is (u_i, R_i), which is sent via a secure channel by the KGC.

2.3 Group Key Agreement Stage

In the following description we suppose low-power user $U_i (1 \le i \le n-1)$ and powerful user U_n wish to generate the shared group session key.

Step1: Each user $U_i (1 \le i \le n-1)$ randomly chooses $r_i \in Z_q^*$, and computes $M_i = r_i u_i P$. Then $U_i (1 \le i \le n-1)$ computes

$$S_i = u_i (H_1(ID_i \| M_i) + r_i) .$$

Finally, $U_i (1 \le i \le n-1)$ sends $\{ID_i, M_i, S_i, R_i\}$ to powerful user U_n.

Step2: Upon receiving $\{ID_i, M_i, S_i, R_i\}$, U_n checks the equations $S_i P - H_1(ID_i \| M_i) P_i = M_i$ for $1 \le i \le n-1$. If one of them fails, U_n terminates the session. Otherwise, U_n randomly chooses $r_n \in Z_q^*$, and computes $M_n = r_n u_n P$ and $Z_i = r_n u_n (M - M_i)(1 \le i \le n-1)$. Then U_n sets

$$M = M_1 + M_2 + \cdots + M_{n-1}, \quad ID = ID_1 \| ID_2 \| \cdots \| ID_n, \quad Z = Z_1 \| Z_2 \| \cdots \| Z_{n-1},$$

and computes

$$K = r_n u_n M = r_n u_n (r_1 u_1 + r_2 u_2 + \cdots + r_{n-1} u_{n-1}) P ,$$

$$S_n = u_n (H_1(ID_n \| Z \| M_n) + r_n) .$$

Finally, U_n sends $\{ID_n, M_n, x_1, ..., x_{n-1}, S_n, R_n\}$ to each user $U_i (1 \le i \le n-1)$, and generates the group session key $GSK = H_1(ID \| Z \| K)$.

Step3: Upon receiving $\{ID_n, M_n, x_1, ..., x_{n-1}, S_n, R_n\}$, U_i checks the equation $S_n P - H_1(ID_n \| Z \| M_n) P_n = M_n$. If it fails, U_i terminates the session. Otherwise, U_i sets $ID = ID_1 \| ID_2 \| \cdots \| ID_n$ and computes

$$K = K_i = r_i u_i M_n + Z_i .$$

Finally, U_i generates the group session key as follows:

$$GSK = H_1(ID \| Z \| K) .$$

3 Analysis of Isalam-Biswas Protocol

3.1 Attack 1

In this subsection, we present our first attack against the Isalam-Biswas protocol. We will show that the Isalam-Biswas protocol cannot provide perfect forward secrecy.

We assume the adversary E has achieved U_1's private key u_1. Now, the adversary E can first compute u_1^{-1} and $H_1(ID_1 \| M_1)$. Then the adversary E can compute r_1 as follows:

$$r_1 = S_1 u_1^{-1} - H_1(ID_1 \| M_1) .$$

It means that the adversary E can use the random number r_1 and private key u_1 to compute K as follows:

$$K = K_1 = r_1 u_1 M_n + Z_1 .$$

Clearly, the adversary E now can generate the group session key $GSK = H_1(ID \| Z \| K)$ successfully, since ID and Z are public messages. So the Isalam-Biswas protocol cannot provide perfect forward secrecy.

3.2 Attack 2

In this subsection, we present our second attack, i.e. ephemeral key compromise attack, against the Isalam-Biswas protocol. In the original Isalam-Biswas protocol, the authors claimed even if all ephemeral values $(r_1, \ldots, r_n)$ are disclosed, the accepted group session key still is secure. We will show that the Isalam-Biswas protocol cannot resist ephemeral key compromise attack. Here, we only assume the adversary E has achieved U_1's ephemeral key r_1.

Now, the adversary E can first compute $H_1(ID_1 \| M_1) + r_1$ and $(H_1(ID_1 \| M_1) + r_1)^{-1}$. Then the adversary E can compute u_1 as follows:

$$u_1 = S_1 (H_1(ID_1 \| M_1) + r_1)^{-1} .$$

It means that the adversary E can use the random number r_1 and private key u_1 to compute K as follows:

$$K = K_1 = r_1 u_1 M_n + Z_1 .$$

Clearly, the adversary E now can generate the group session key $GSK = H_1(ID \| Z \| K)$ successfully, since ID and Z are public messages. So the Isalam-Biswas protocol cannot resist ephemeral key compromise attack.

4 Conclusions

In this letter, we have pointed out that Isalam et al.'s protocol is insecure. To avoid these security flaws, it must be carefully design Isalam et al.'s protocol again.

References

[1] S. Islam, G. Biswas. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. Annals of Telecommunications, vol. 67, no. 11-12, pp. 547-558, 2012.