Security Analysis of a Pairing-free Identity-based Authenticated Group Key Agreement Protocol for Imbalanced Mobile Networks

Qingfeng Cheng[1,2]
Department of Language Engineering & Luoyang University of Foreign Languages[1]
Luoyang 471003, P.R. China
Science and Technology on Information Assurance Laboratory, Beijing 100072, P.R.China[2]
(Email: qingfengc2008@sina.com)
(Received Jan. 7, 2013; revised and accepted Aug. 27 & Nov. 10, 2013)

Abstract

Recently, Isalam and Biswas proposed a new group key agreement (GKA) protocol for imbalanced mobile networks. In this letter, we will first prove that Isalam and Biswas's GKA protocol cannot provide perfect forward secrecy. Then we will point out that their GKA protocol is vulnerable to ephemeral key compromise attack.

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

1 Introduction

Mobile network is an imbalanced wireless network, where users have different computing capability. For assuring secure communications in mobile network, in general it needs to encrypt the messages transmitted by users, which means that users must generate shared session keys before starting communications. There are many two-party and group authenticated key agreement (AKA) protocols [1, 2, 6, 7, 8, 12] for imbalanced wireless network. However, the design of secure AKA protocols for imbalanced mobile networks is not a trivial task.

In [9], Nam et al. proposed an efficient group key agreement (GKA) protocol based on the Decisional Diffie-Hellman assumption for imbalanced mobile networks. Nam et al.'s construction was simple, and met many security properties. However, Tseng [11] pointed out that Nam et al.'s protocol still had a weakness, i.e. lack of contributory property. Further, Tseng [11] proposed a new GKA protocol with contributory property, whereas Tseng's protocol did not consider mutual authentication due to Lee et al. [5]. For achieving mutual authentication, Lee et al. [5] presented a new GKA protocol proven secure in a security model. Unfortunately, Lee et al.'s protocol is not secure due to Cheng et al. [3] and Tsai [10] respectively.

Recently, Isalam and Biswas [4] also proposed a new GKA protocol for imbalanced mobile networks, called Isalam-Biswas protocol. They claimed that their protocol met various attributes, including perfect forward secrecy and ephemeral key compromise resilience. In this letter, however, we will show that the Isalam-Biswas protocol cannot provide perfect forward secrecy. In addition, we also prove that the Isalam-Biswas protocol 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 $H_0 : \{0,1\}^* \times G \longrightarrow Z_q^*$ and $H_1 : \{0,1\}^* \longrightarrow \{0,1\}^k$. The system parameters are $\{q, G, P, H_0, H_1\}$.

2.2 Key Extract Stage

The KGC first randomly chooses $v_i \in Z_q^*$ for each user $U_i (1 \leq i \leq n-1)$, whose identity is $ID_i \in \{0,1\}^*$. Then the KGC computes $R_i = v_i P, h_i = H_0(ID_i \parallel R_i)$ and $u_i = v_i + h_i s$. Finally, the user's private key is (u_i, R_i).

2.3 Group Key Agreement Stage

we suppose low-power user $U_i (1 \leq i \leq n-1)$ and powerful user U_n wish to agree a shared group session key.

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

$i \leq n-1$) computes

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

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

Step 2. Upon receiving $\{ID_i, M_i, S_i, R_i\}$, U_n checks the equations $S_iP - H_1(ID_i \parallel M_i)P_i = M_i$ for $1 \leq i \leq n-1$. If one of them fails, U_n terminates the session. Otherwise, U_n randomly chooses $r_n \in Z_q^*$, and computes $M_n = r_nu_nP$ and $Z_i = r_nu_n(M - M_i)(1 \leq i \leq n-1)$. Then U_n sets

$$\begin{aligned} M &= M_1 + M_2 + \cdots + M_{n-1}, \\ ID &= ID_1 \parallel ID_2 \parallel \cdots \parallel ID_n, \\ Z &= Z_1 \parallel Z_2 \parallel \cdots \parallel Z_{n-1}, \end{aligned}$$

and computes

$$\begin{aligned} K &= r_nu_nM \\ &= r_nu_n(r_1u_1 + r_2u_2 + \cdots + r_{n-1}u_{n-1})P, \\ S_n &= u_n(H_1(ID_n \parallel Z \parallel M_n) + r_n). \end{aligned}$$

Finally, U_n sends $\{ID_n, M_n, Z_1, \cdots, Z_{n-1}, S_n, R_n\}$ to each user $U_i(1 \leq i \leq n-1)$.

Step 3. Upon receiving $\{ID_n, M_n, Z_1, \cdots, Z_{n-1}, S_n, R_n\}$, $U_i(1 \leq i \leq n-1)$ checks the equation $S_nP - H_1(ID_n \parallel Z \parallel M_n)P_n = M_n$. If it fails, $U_i(1 \leq i \leq n-1)$ terminates the session. Otherwise, $U_i(1 \leq i \leq n-1)$ sets $ID = ID_1 \parallel ID_2 \parallel \cdots \parallel ID_n$ and computes

$$K = K_i = r_iu_iM_n + Z_i.$$

Finally, $U_i(1 \leq i \leq n-1)$ generates the group session key as follows:

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

3 Analysis of Isalam-Biswas Protocol

3.1 Attack 1

In this subsection, we present the 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 $H_1(ID_1 \parallel M_1)$. Then the adversary E can compute r_1 as follows:

$$r_1 = S_1u_1^{-1} - H_1(ID_1 \parallel M_1).$$

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

$$K = K_1 = r_1u_1M_n + Z_1.$$

Clearly, the adversary E now can generate the group session key $GSK = H_1(ID \parallel Z \parallel K)$ 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 $(r_1, \cdots, r_n)$ were disclosed, the accepted group session key still was secure. However, we will show that the Isalam-Biswas protocol cannot resist ephemeral key compromise attack. Here, we only assume the adversary E has obtained U_1's ephemeral key r_1.

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

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

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

$$K = K_1 = r_1u_1M_n + Z_1.$$

Clearly, the adversary E now can generate the group session key $GSK = H_1(ID \parallel Z \parallel K)$ 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 against ephemeral key compromise attack. Moreover, we show that Isalam et al.'s protocol cannot provide perfect forward secrecy. For overcoming these security flaws, it needs to carefully select a secure signature scheme to improve Isalam et al.'s protocol.

Acknowledgments

The author gratefully thanks Prof. Min-Shiang Hwang and the anonymous reviewers for their valuable comments. This study was supported by the Science Foundation of Luoyang University of Foreign Languages (No. 2011XYZ004) and Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-13-109).

References

[1] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices," *Computer Communications*, vol. 27, no. 17, pp. 1730–1737, 2004.

[2] Y. Chang, C. Chang, and J. Yang, "An efficient password authenticated key exchange protocol for imbalanced wireless networks," *Computers Standards and Interfaces*, vol. 27, no. 3, pp. 313–322, 2005.

[3] Q. Cheng, C. Ma, and F. Wei, "Analysis and improvement of a new authenticated group key agreement in a mobile environment," *Annals of Telecommunications*, vol. 66, no. 5–6, pp. 331–337, 2011.
[4] S. Islam and 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.
[5] C. Lee, T. Lin, and C. Tsai, "A new authenticated group key agreement in a mobile environment," *Annals of Telecommunications*, vol. 64, no. 11–12, pp. 735–744, 2009.
[6] J. Lo, "The improvement of ysyct scheme for imbalanced wireless network," *International Journal of Network Security*, vol. 3, no. 1, pp. 39–43, 2006.
[7] J. Lo, J. Lee, M. Hwang, and Y. Chu, "An advanced password authenticated key exchange protocol for imbalanced wireless networks," *Journal of Internet Technology*, vol. 11, no. 7, pp. 997–1004, 2010.
[8] J. Nam, S. Kim, and D. Won., "A weakness in the Bresson-Chevassut-Essiari-Pointcheval's group key agreement scheme for low-power mobile devices," *IEEE Communications Letters*, vol. 9, no. 5, pp. 429–431, 2005.
[9] J. Nam, J. Lee, S. Kim, and D. Won., "DDH-based group key agreement in a mobile environment," *Journal of Systems Software*, vol. 78, no. 1, pp. 73–83, 2005.
[10] J. Tsai, "A novel authenticated group key agreement protocol for mobile environment," *Annals of Telecommunications*, vol. 66, no. 11–12, pp. 663–669, 2011.
[11] Y. Tseng, "A resource-constrained group key agreement protocol for imbalanced wireless networks," *Computer Security*, vol. 26, no. 4, pp. 331–337, 2007.
[12] H. Yeh, H. Sun, C. Yang, B. Chen, and S. Tseng, "The improvement of password authenticated key exchange scheme based on RSA for imbalanced wireless network," *IEICE Transactions on Communications*, vol. E86-B, no. 11, pp. 3278–3282, 2003.

Qingfeng Cheng received his B.A. degree in 2000 and M.S. degree in 2004 from National University of Defense Technology, and Ph.D. degree in 2011 from Information Engineering University. He is now an Associate Professor with the Department of Language Engineering, Luoyang University of Foreign Languages. His research interests include cryptography and information security.