Attack on An ID-based Authenticated Group Key Exchange Protocol with Identifying Malicious Participants

Fushan Wei[1,2], Yun Wei[2], and Chuangui Ma[2]
(Corresponding author: Fushan Wei)
School of Computer Science and Technology, Xidian University Xi'an, China[1]
No. 2 South Taibai Road, Xian, Shanxi 710071, China
State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China[2]
No. 92, Kexue Road, Zhengzhou, Henan 450001, China
(Email: weifs831020@163.com)
(Received Dec. 25, 2013; revised and accepted Jan. 21 & Mar. 4, 2015)

Abstract

An authenticated group key exchange (AGKE) protocol allows a group of participants to establish a common session key and then provides secure group communications in collaborative and distributed applications. Recently, Wu et al. proposed an ID-based authenticated group key exchange protocol based on bilinear pairings. They claimed that their protocol can detect and identify the malicious participants, which means it not only can check whether malicious participants exist in the protocol or not, but also can find out who the malicious participants are. However, their protocol is not as secure as claimed. In this letter, we show that Wu et al.'s protocol is insecure against an insider colluding attack. Two malicious participants can collude to impersonate several honest participants to the rest participants in the group. In addition, we also figure out what has gone wrong with Wu et al.'s protocol and how to fix it.

Keywords: Authenticated group key exchange, bilinear pairings, ID-based, insider colluding attacks

1 Introduction

Establishing secure channels is one of the most important areas of network security [6, 7]. User authentication and key exchange protocols are often combined to establish shared secrets for the communication participants [2, 3, 9, 11]. Owing to the rapid development of group-oriented applications such as e-commerce and collaboration works [8, 15], authenticated group key exchange (AGKE) protocols have become an important research issue in network security. An AGKE protocol allows a group of participants to agree upon a common session key in an authenticated manner, which can subsequently be used to provide group secure communications [1, 10]. In the traditional certificate-based AGKE protocols, the public keys of the participants are issued by a trusted certificate authority (CA), which brings the problems of complex certificate management. In order to simplify the management of public keys and in particular the association of a public key to the identity of its holder, researchers pay more and more attention to ID-based AGKE protocols. Over the years, a few ID-based AGKE protocols based on bilinear pairings have been proposed.

In 2004, Choi et al. [4] proposed the first ID-based AGKE protocol using bilinear pairings. However, Zhang and Chen [17] showed Choi et al.'s proposal is vulnerable to an insider colluding attack, whereby two malicious participants can impersonate an honest participant to establish a session key in a new group if these two malicious participants have the previous authentication transcripts of the victim participant. In 2007, Shim [12] pointed out that Choi et al.'s ID-based AGKE protocol is insecure against another colluding attack. Shim also presented an improved protocol to resist the attack. In 2008, Choi et al. [5] demonstrated Shim's improvement suffered from other insider colluding attacks, they also suggested a modification to overcome the problem. Unfortunately, Wu and Tseng [13] have shown that Choi et al's modified protocol is still insecure against insider colluding attacks. Moreover, they also proved that the batch verification scheme used in [5] suffers from a forgery attack, in which some malicious participants can collude to impersonate a non-involved user to generate valid signatures to pass the batch verification. Recently, Wu et al. [14] proposed a 2-round ID-based AGKE protocol and proved its security in the random oracle model under the Computational Diffie-Hellman (CDH) and Decisional Bilinear

Diffie-Hellman (DBDH) assumptions. They claimed their protocol can resist insider attacks and identify malicious participants, which means it not only can detect whether malicious participants exist in the group but also find out "who are malicious participants". Their protocol heavily uses ID-based signature schemes. Almost all the messages are signed using the ID-based signature scheme proposed by Yoon et al. [16]. Consequently, the security of their protocol relies on the unforgeability of the signature scheme.

In this letter, we show that Wu et al.'s protocol is vulnerable to an insider colluding attack. Through this attack, two malicious participants can collude to impersonate several honest participants to the rest participants in the group. In [14], Wu et al. claimed that their protocol is provably secure against insider attacks. Our attack invalidates their claim of security. Wu et al.'s protocol fail to resist insider attacks, not to mention identifying the malicious participants. To remedy the problem, we first point out the flaw in the security proof, and then suggest countermeasures to thwart the attack.

The remainder of this paper is organized as follows. In Section 2, Wu et al.'s ID-based AGKE protocol is reviewed. In Section 3, we point out its vulnerability against insider colluding attacks. We suggest countermeasures to the insider colluding attack in Section 4. Concluding remarks are given in Section 5.

2 Review of Wu et al.'s ID-based Group Key Exchange Protocol

2.1 Notations

The notations used throughout the letter are summarized as follows:

- q: a large prime.
- G_1: a cyclic additive group of order q.
- G_2: a cyclic multiplicative group of order q.
- e: an admissible bilinear map, $e : G_1 \times G_1 \rightarrow G_2$.
- P: a generator of the group G_1.
- s: the system private key, where $s \in Z_q^*$.
- P_{pub}: the system public key, where $P_{pub} = s \cdot P$.
- ID_i: the identity of participant U_i.
- DID_i: the private key of participant U_i.
- H_G: a map-to-point hash function, $H_G : \{0,1\}^* \rightarrow G_1$.
- H_1: a one-way hash function, $H_1 : \{0,1\}^* \times G_1 \rightarrow Z_q$.
- H_2: a one-way hash function, $H_2 : \{0,1\}^* \times G_1^3 \rightarrow Z_q$.
- $\|$: concatenation operation.

2.2 Descriptions of Wu et al.'s Protocol

In this subsection, we briefly review Wu et al.'s ID-based authenticated group key exchange protocol [14]. In the setup phase, the Key Generation Center (KGC) generates the public parameters $\{G_1, G_2, e, q, P, P_{pub}, H_G, H_1, H_2\}$ and the system private key s. When a participant U_i with identity ID_i wants to obtain his private key DID_i, he submits his identity ID_i to KGC. KGC computes this user's private key as $DID_i = s \cdot H_G(ID_i)$.

Let $U_1, U_2, ..., U_n (n > 2)$ be a set of participants who want to establish a session key. The indices are subject to modulo n, e.g. U_{n+1} and U_0 denote U_1 and U_n, respectively. PID is defined as $ID_1 \| ID_2 \| ... \| ID_n$, which is the concatenation of the identities of participants taking part in a session. $M \in \{0,1\}^*$ is a pre-known message by all participants which contains some conference information such as the conference title, date and location. The details of Wu et al.'s protocol are described as follows.

Round 1. Each participant U_i randomly chooses an integer $a_i \in Z_q^*$, then computes $P_i = a_i \cdot P$, $h_i = H_1(M \| PID \| ID_i, P_i)$, and $V_i = a_i \cdot H_G(ID_i) + h_i \cdot DID_i$. Finally, each U_i broadcasts (ID_i, P_i, V_i).

Round 2. Upon receiving the messages $(ID_{i-1}, P_{i-1}, V_{i-1})$ and $(ID_{i+1}, P_{i+1}, V_{i+1})$, each participant U_i checks the equation $e(P, \sum_{k\in\{-1,1\}} V_{i+k}) = \prod_{k\in\{-1,1\}} e(P_{i+k} + h_{i+k} \cdot P_{pub}, H_G(ID_{i+k}))$. If the checking equation holds, each U_i uses the secret a_i to compute $D_i = e(P_{i+1} - P_{i-1}, P_{pub})^{a_i}$.

Then U_i generates a signature on the message $(PID \| ID_i \| D_i \| S)$ as follows: U_i chooses a random integer $r_i \in Z_q^*$, computes $\alpha_i = r_i \cdot P$, $\beta_i = r_i \cdot (P_{i+1} - P_{i-1})$, $k_i = H_2(PID \| ID_i \| D_i \| S, P_{i+1} - P_{i-1}, \alpha_i, \beta_i)$ and $\gamma_i = r_i \cdot P_i + k_i a_i \cdot P_{pub}$, where $S = P_1 \| P_2 ... \| P_n$. Finally, each U_i sends $\sigma_i = (ID_i, D_i, \alpha_i, \beta_i, \gamma_i)$ to all other participants.

Group Session Key Computation. Upon receiving all $\sigma_j = (ID_j, D_j, \alpha_j, \beta_j, \gamma_j)$ for $j = 1, 2, ..., n$ and $j \neq i$, each U_i checks $e(P, \gamma_j) = e(P_j, \alpha_j + k_j \cdot P_{pub})$ and $e(P_{j+1} - P_{j-1}, \gamma_j) = e(\beta_j, P_j) \cdot D_j^{k_j}$, where $k_j = H_2(PID \| ID_j \| D_j \| S, P_{j+1} - P_{j-1}, \alpha_j, \beta_j)$ and $S = P_1 \| P_2 ... \| P_n$. If the above equations hold, each participant U_i can compute the same session group key $SK = e(a_i \cdot P_{i-1}, P_{pub})^n \cdot D_i^{n-1} \cdot D_{i+1}^{n-2} ... D_{i-2}$.

Malicious Participant Identifying. If a participant U_m tries to send a wrong $\sigma_m = (ID_m, D_m, \alpha_m, \beta_m, \gamma_m)$ to interrupt the establishment of a group session, then he will be determined as a malicious participant because the two equations $e(P, \gamma_m) = e(P_m, \alpha_m + k_m \cdot P_{pub})$ and $e(P_{m+1} - P_{m-1}, \gamma_m) = e(\beta_m, P_m) \cdot D_m^{k_m}$ do not hold. If the malicious participant U_m is detected, then he will be deleted from the participant set. The other honest participants may return the protocol.

3 Insider Colluding Attack on Wu et al.' Protocol

In this section, we point out a simple but powerful insider colluding attack on Wu et al.'s ID-based AGKE protocol. Suppose U_{i-1} and U_{i+1} are two malicious participants. They collude and want to impersonate several honest participants in the group to fool a honest participant U_i. They proceed as follows:

1) In Round 1, the malicious participants U_{i-1} and U_{i+1} generate the messages $(ID_{i-1}, P_{i-1}, V_{i-1})$ and $(ID_{i+1}, P_{i+1}, V_{i+1})$ according to the description of the protocol, respectively. Meanwhile, for each participant $U_k, k \in \{1, 2, ..., n\}$ and $k \neq i-1, i, i+1$,the colluding participants U_{i-1} and U_{i+1} pick an integer a_k and computes $P_k = a_k \cdot P$, $h_k = (M \parallel PID \parallel ID_k, P_k)$, and $V_k = a_k \cdot H_G(ID_k) + h_k \cdot P_{k'}$, where $P_{k'}$ is an element randomly chosen from G_1. Finally, the malicious participants broadcast (D_j, P_j, V_j) for $j = 1, 2, ..., i-1, i+1, ..., n$.

2) In Round 2, the malicious participants U_{i-1} and U_{i+1} only check the following equation:

$$e(P, V_i) = e(P_i + h_i \cdot P_{pub}, H_G(ID_i))$$

where $h_i = H_1(M \parallel PID \parallel ID_i, P_i)$. If the above equation holds, the malicious participants proceed to the next step. Note that in this time, nobody except U_{k-1} and U_{k+1} knows the invalidity of $V_K, k \in \{1, 2, ..., n\}$ and $k \neq i-1, i, i+1$, since only U_{k-1} and U_{k+1} verify U_k's signature. The honest participant U_i cannot detect the invalidity of V_K, either.

3) For each participant $U_j (j = 1, 2, ..., n, j \neq i)$, the malicious participants compute $D_j = e(P_{j+1} - P_{j-1}, P_{pub})^{a_j}$, and generates $(\alpha_j, \beta_j, \gamma_j)$ according to the description of the protocol. More precisely, the malicious participants choose a random integer $r_j \in Z_q^*$ and computes $\alpha_j = r_j \cdot P$, $\beta_j = r_j \cdot (P_{j+1} - P_{j-1})$, $k_j = H_2(PID \parallel ID_j \parallel D_j \parallel S, P_{j+1} - P_{j-1}, \alpha_j, \beta_j)$, and $\gamma_j = r_j \cdot P_j + k_j a_j \cdot P_{pub}$, where $S = P_1 \parallel P_2 ... \parallel P_n$. Finally, the malicious participants broadcast the message $(ID_j, \alpha_j, \beta_j, \gamma_j)$.

4) In group session key computation stage, γ_j will pass the verification because γ_j is generated using the ephemeral key a_j and a_j is chosen by the malicious participants. The malicious participants can compute the group session key since they know $a_j (j = 1, 2, ..., i-1, i+1, ..., n)$. Finally, The malicious participants U_{i-1} and U_{i+1} succeed in impersonating other participants in the group to the honest entity U_i.

Note that the above attack can be easily extended to the case in which two malicious participants U_{i-m} and U_{i+m} try to fool the honest participants $U_{i-m+1}, ..., U_{i+m-1}$ by impersonating other participants in the group, where $m > 1$. In this way, two malicious participants can collude to fool m honest participants by impersonating the rest participants in the group. The attack is powerful since it only needs two malicious participants collude to impersonate several participants in a session without being detected.

4 Discussions and Countermeasure

Although Wu et al.'s protocol heavily relies on ID-based signature scheme, the insider colluding attack is still possible. The reason lies in two points: first, each participants U_i is only authenticated by its neighbors U_{i-1} and U_{i+1} in Round 2, nobody except U_{i-1} and U_{i+1} knows the validity of U_i. Second, the message $(PID \parallel ID_j \parallel D_j \parallel S)$ is signed using the ephemeral secret a_j. As long as the malicious participants impersonate an honest participant in Round 1, they can easily generate the signature in Round 2 because the ephemeral secret a_j is chosen by the malicious participants.

An intuitive countermeasure to our insider colluding attack would be let the participant U_i check the validity of all the signatures of other participants in Round 2. However, this would make the protocol very inefficient and impractical. We suggest that the message $(PID \parallel ID_j \parallel D_j \parallel S, P_{j+1} - P_{j-1}, \alpha_j, \beta_j)$ be signed using the private key DID_j of participant U_j. In this way, the malicious participants could not forge an honest participant's signature in Round 2.

In fact, Wu et al. [14] proved the security of their protocol in a formal security model. They also claimed their protocol could resist insider attacks. It fails because of the incorrect announcement in its security proof. In Theorem 1 of [14], the authors simply conclude that their protocol is secure against ID and forgery attacks due to the unforgeability of the signature scheme of Yoon et al. [16]. However, a signature scheme may be secure alone, but when it is used in a group key exchange protocol, the security of the group key exchange protocol can not be derived simply from the security of the signature scheme. This attack warns us that we should consider the security of the group key exchange in a whole framework, not separately. It also emphasis the importance of rigorous security proof for group key exchange protocols.

5 Conclusions

In this letter, we have shown that Wu et al.'s ID-based authenticated group key exchange protocol is insecure against an insider colluding attack. Two malicious participants can collude to impersonate several honest participants without being detected. We also analyzed the reason to the attack and suggested a countermeasure.

Acknowledgments

The authors would like to thank the anonymous referees for their helpful comments. This work is supported by the National Natural Science Foundation of China (Nos. 61309016,61379150,61201220,61103230), Postdoctoral Science Foundation of China (No. 2014M562493), Postdoctoral Science Foundation of Shanxi Province, the Funding of Science and Technology on Information Assurance Laboratory (No. KJ1302) and Key Scientific and Technological Project of Henan Province (No. 122102210126,092101210502).

References

[1] T. Yi Chang, M. S. Hwang, "User-anonymous and short-term Conference Key Distribution System via link-layer routing in mobile communications," *International Journal of Mobile Communication*, vol. 9, no. 2, pp. 144–158, 2011.

[2] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.

[3] Q. F. Cheng, "Cryptanalysis of a new efficient authenticated multiple-key exchange protocol from bilinear pairings," *International Journal of Network Security*, vol. 16, no. 6, pp. 494–497, 2014.

[4] K. Choi, J. Hwang, and D. H. Lee, "Efficient ID-based group key agreement with bilinear maps," in *Public Key Cryptography (PKC'04)*, LNCS 2947, pp. 130–144, Springer, 2004.

[5] K. Choi, J. Hwang, and D. H. Lee, "ID-based authenticated group key agreement secure against insider attacks," *IEICE Transactions on Fundamentals*, vol. E91-A, no. 7, pp. 1828–1830, 2008.

[6] S. K. Chong, C. C. Lee, and M. S. Hwang, "An authentication scheme for the global mobility network," *Parallel Processing Letters*, vol. 23, no. 3, 2013.

[7] L. C. Huang, C. C. Lee, and M. S. Hwang, "A n^2+n MQV key agreement protocol," *International Arab Journal of Information Technology*, vol. 10, no. 2, pp. 137–142, 2013.

[8] M. S. Hwang, C. C. Lee, and S. F. Tzeng, "A new proxy signature scheme for a specified group of verifiers," *Information Sciences*, vol. 227, pp. 102–115, 2013.

[9] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[10] W. T. Li, C. H. Ling, and M. S. Hwang, "Group rekeying in wireless sensor networks: a survey," *International Journal of Network Security*, vol. 16, no. 6, pp. 400–410, 2014.

[11] H. H. Ou, M. S. Hwang, "Double delegation-based authentication and key agreement protocol for PCSs," *Wireless Personal Communications*, vol. 72, no. 1, pp. 437–446, 2013.

[12] K. A. Shim, "Further analysis of ID-based authenticated group key agreement protocol from Bilinear maps," *IEICE Transactions on Fundamentals*, vol. E90-A, no. 1, pp. 231–233, 2007.

[13] T. Y. Wu, Y. M. Tseng, "Comment on an ID-based authenticated group key agreement protocol with withstanding insider attacks," *IEICE Transactions on Fundamentals*, vol. E92-A, no. 10, pp. 2638–2640, 2009.

[14] T. Y. Wu, Y. M. Tseng, "Towards ID-based authenticated group key exchange protocol with identifying malicious participants," *Informatica*, vol. 23, no. 2, pp. 315–334, 2012.

[15] C. C. Yang, T. Y. Chang, and M. S. Hwang, "A new group signature scheme based on RSA assumption," *Information Technology and Control*, Vol. 42, no. 1, pp. 61–66, 2013.

[16] H. J. Yoon, J. H. Cheon, and Y. Kim, "Batch verifications with ID-based signatures," in *Information Security and Cryptology (ICISC'04)*, LNCS 3506, pp.233–248, Springer, 2005.

[17] F. G. Zhang, X. F. Chen, "Attack on an ID-based authenticated group key agreement scheme from PKC 2004," *Information Processing Letters*, vol. 91, no. 4, pp. 191–193, 2004.

Fushan Wei received his M.S. and Ph.D. degrees in applied mathematics from the Zhengzhou Information Science and Technology Institute, China, in 2008 and 2011, respectively. He is currently a lecturer in department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research fields include cryptography and information security.

Yun Wei received her B.S. degree in applied mathematics from the Zhengzhou Information Science and Technology Institute, China, in 2010. She is currently pursuing his M.S. degree in department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. Her research fields include cryptography and information security.

Chuangui Ma received the B.E. degree in mathematics in 1982 from Zhengzhou University of China, the M.S. degree in mathematics in 1985 from Liaocheng University of China, and the Ph.D. degree in mathematics in 1998 from Zhejiang University of China. Since December 2002, he has been a Professor with the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research field is information security.