International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.org & www.ijocit.ir
ISSN = 2345-3877

Cryptanalysis of an Attribute-based Key Agreement Protocol

Ziba Eslami[1], Nasrollah Pakniat[2], and Mahnaz Noroozi[3]
Department of Computer Sciences, Shahid Beheshti University
z_eslami@sbu.ac.ir[1], n_pakniat@sbu.ac.ir[2], m.noroozi@mail.sbu.ac.ir[3]

Abstract: A key agreement protocol allows two or more participants to establish a common key via exchanging messages over a public channel. In 2009, motivated by the problem of establishing a common key among participants who do not know each other's exact identity, Wang et al. proposed a two-party attribute-based key agreement protocol and claimed that it is secure in the random oracle model. In this paper, we show that their claim is not true and two outsiders who possess some special attribute sets are able to determine the secret key.

Keywords: Cryptography, Key Agreement Protocols, Security Analysis.

I. Introduction

Key agreement protocols, first proposed by Diffie and Hellman in 1976 [2], are one of fundamental cryptographic primitives which play an important role in many modern network-based applications such as collaborative or distributed applications. Such protocols allow two entities to share a key via exchanging messages over a public channel and this key can later be used to provide secure communication between them over a public channel.

In 1984, Shamir [3] introduced the concept of identity-based cryptography to simplify management of public keys in the certificate-based public key infrastructures (PKI). In the PKI setting, each user has a public key which is signed by a trusted authority to generate a

certificate that binds the user to his/her public key. Therefore, it is a heavy burden to generate, deliver, maintain, and verify certificates in these systems. As an alternative to certificate-based PKIs, in the identity-based cryptography, the user's public key is an easily calculated function of his/her identity (e.g., social security number, etc.), while the user's private key can be calculated by a trusted party referred to as Private Key Generator (PKG). Since identity-based cryptosystems simplify the process of key management, they have been considered extensively for designing key agreement protocols [4, 5].

In an Identity-Based Key Agreement (IBKA) protocol, each user is identified by a unique identifier, therefore, a set of users who want to have a private session should know identity of other users before running an IBKA protocol and obtaining a common key. However, this would not always be a realistic scenario since the users might only know the "attributes" of each other rather than the exact identities of others. For instance, suppose that A and B are members of Institute I , faculty F , department D and Institute I′ , faculty F′ , department D′ , respectively and they want to have a private session with each other. It is not important for them what is the exact identity of the second user and they only want the other party to have some special attributes. Hence, IBKA does not satisfy their requirement and therefore, they should use an Attribute-Based Key Agreement (ABKA) protocol.

Attribute-based encryption (ABE) schemes were put forwarded in 2005 by Sahai and Waters [6]. In an ABE system, user's keys and ciphertexts are labelled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. Since then some ABE schemes have been proposed [7, 8]. In an attribute-based key agreement protocol,

© 2014, IJOCIT All Rights Reserved

parties use attribute information of other entities (instead of traditional public keys) to generate the session key. These protocols not only preserve the advantages of traditional identity-based key agreement protocol, but they also have a new merit: hiding the identity information of the individuals. Note that in the setting of attribute-based cryptography, a set of attributes doesn't define a participant uniquely and there are many participants with those attributes.

The aim of this paper is to show that the key agreement protocol proposed by Wang et al. [1] has a security weakness. In [1], it is claimed that the scheme is a secure authenticated key agreement protocol in the random oracle model assuming that the bilinear Diffie-Hellman problem is hard. In this paper, we show that their protocol is not secure against collusion of some special outsiders.

The remainder of this paper is organized as follows. In Section 2, we briefly describe the preliminaries including bilinear pairing and Lagrange interpolation polynomial. A review of Wang et al.'s ABKA protocol will be presented in Section 3. The details of the proposed attack will be provided in Section 4. Finally Section 5 concludes the paper.

2. Preliminaries

Bilinear Pairing. Let G_1 and G_2 be two multiplicative groups with the same prime order p. A map $e: G_1 \times G_1 \to G_2$ is called a bilinear pairing if it satisfies the following properties:

Bilinearity: $e(g^a, h^b) = e(g,h)^{ab}$ for all $g, h \in G_1$, $a, b \in Z_p^*$.

Non-degeneracy: There exists $g, h \in G_1$ such that $e(g,h) \neq 1_{G_2}$, where 1_{G_2} is the identity element of G_2.

Computability: There exists an efficient algorithm to compute $e(g,h)$ for any $g, h \in G_1$.

© 2014, IJOCIT All Rights Reserved

Lagrange Interpolation Polynomial. A set of $n+1$ distinct points $(x_i, y_i)_{i=0,1,\ldots,n}$ is given. Let $S=\{0,1,\ldots,n\}$. Lagrange interpolation polynomial is computed using Lagrange coefficients as follows:

$$P(x)=\sum_{i=0}^{n}\Delta_{i,S}(x)y_i,$$

where

$$\Delta_{i,S}(x)=\prod_{j\in S, j\neq i}\frac{(x-x_j)}{(x_i-x_j)}.$$

3. Review of Wang et al.'s ABKA protocol

In this section, we briefly review Wang et al.'s ABKA protocol using the notation of [1]. Suppose that Alice (A) and Bob (B) want to share a session key and that ω_A and ω_B represent their attribute sets, respectively. Their attribute-based key agreement protocol consists of the following 3 algorithms:

Setup: Generate a group G_1 of prime order p. Construct a bilinear map $e: G_1 \times G_1 \to G_2$, where G_2 is a group of the same order p. Pick a generator g of the group G_1. Pick $g_1 \in G_1$ at random. Pick $y \in Z_p^*$ at random and compute $g_2 = g^y$. Choose three hash functions $H_1: Z_p^* \to G_1$ and $H_2: \{0,1\}^* \to \{0,1\}^k$, where k is the size of the session key (sk) which will be outputted by the protocol. Output the public parameters $params=(p,g,e,G_1,G_2,H_1,H_2,g_1,g_2)$ and a master key $mk=y$.

Key-Gen: To generate a private key for a set of attributes ω the following steps are performed. A $|\omega|-1$ degree polynomial $P_\omega(.)$ is randomly chosen such that $P_\omega(0)=y$. The private key correspond to a set of attributes ω is $\{D_i\}_{i\in\omega}$, where $D_i=(\gamma_i,\delta_i)=((g_1H_1(i))^{P_\omega(i)}, g^{P_\omega(i)})$.

Key-Agreement: Alice and Bob each randomly choose an ephemeral private key, $a,b \in Z_p$ and compute the values of the corresponding ephemeral public keys separately, $E_{A_1}=\{E_{A_{1,i}}\}_{i\in\omega_B}=\{H_1(i)^a\}_{i\in\omega_B}$, $E_{A_2}=g^a$ and $E_{B_1}=\{E_{B_{1,i}}\}_{i\in\omega_A}=\{H_1(i)^b\}_{i\in\omega_A}$, $E_{B_2}=g^b$.

© 2014, IJOCIT All Rights Reserved

They then exchange the ephemeral public keys as follow:

Alice $\rightarrow$ Bob: $E_A = E_{A_1} \| E_{A_2}$.

Bob $\rightarrow$ Alice: $E_B = E_{B_1} \| E_{B_2}$.

Alice then computes shared secret K_{AB} as follow:

$$K_{AB} = \frac{e\left(\prod_{i\in\omega_A} \gamma_i^{\Delta_{i,\omega_A}(0)}, E_{B_2}\right)}{\prod_{i\in\omega_A} e\left(E_{B_{1,i}}, \delta_i^{\Delta_{i,\omega_A}(0)}\right)} e(g_1, g_2)^a,$$

and Bob computes shared secret K_{BA} as follow:

$$K_{BA} = \frac{e\left(\prod_{i\in\omega_B} \gamma_i^{\Delta_{i,\omega_B}(0)}, E_{A_2}\right)}{\prod_{i\in\omega_B} e\left(E_{A_{1,i}}, \delta_i^{\Delta_{i,\omega_B}(0)}\right)} e(g_1, g_2)^b.$$

If Alice and Bob follow the protocol, they will compute the same shared secret:

$$K = K_{AB} = K_{BA} = e(g_1, g_2)^{a+b}.$$

Then using a key derivation function $H_2 : \{0,1\}^* \rightarrow \{0,1\}^k$ a shared session key is generated: $sk = H_2(\omega_A \| \omega_B \| E_A \| E_B \| K)$, where $k = |sk|$.

4. The proposed attack on Wang et al.'s ABKA protocol

In this section, we show that Wang et al.'s ABKA protocol, denoted for short by (w-ABKA), does not provide security against collusion attack. The next theorem shows how public parameters and information publicly sent between two main participants allows two persons to collude and get the secret key.

Theorem 1. Let Alice and Bob be the users who run the protocol (w-ABKA) with ω_A and ω_B representing their attribute sets, respectively and let K be their shared key. Suppose that X is someone with attribute set ω_X such that $\omega_X = \omega_A$ and similarly Y is a person with attribute set $\omega_Y = \omega_B$. Then X and Y can compute K as well.

Proof. Let K'_X and K'_Y be defined as follows:

© 2014, IJOCIT All Rights Reserved

$$K'_X = \frac{e\left(\prod_{i\in\omega_X} \gamma_i^{\Delta_{i,\omega_X}(0)}, E_{B_2}\right)}{\prod_{i\in\omega_X} e\left(E_{B_{1,i}}, \delta_i^{\Delta_{i,\omega_X}(0)}\right)},$$

$$K'_Y = \frac{e\left(\prod_{i\in\omega_Y} \gamma_i^{\Delta_{i,\omega_Y}(0)}, E_{A_2}\right)}{\prod_{i\in\omega_Y} e\left(E_{A_{1,i}}, \delta_i^{\Delta_{i,\omega_Y}(0)}\right)}.$$

Note that X and Y have all the public parameters generated in the setup algorithm and they have their own private keys generated in the Key-Gen algorithm. Then, after exchanging information between Alice and Bob in the Key-Agreement algorithm of w-ABKA protocol, they get the ephemeral public keys of Alice and Bob, i.e. E_{A_1}, E_{A_2}, E_{B_1} and E_{B_2}. So X and Y are able to compute K'_X and K'_Y, respectively. Now we show that $K = K'_X.K'_Y$.

$$k'_X = \frac{e\left(\prod_{i\in\omega_X} (g_1 H_1(i))^{P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}, g^b\right)}{\prod_{i\in\omega_X} e\left(H_1(i)^b, g^{P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}\right)}$$

$$= \frac{\prod_{i\in\omega_X} e\left(g_1^{P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}, g^b\right)\prod_{i\in\omega_X} e\left(H_1(i)^{P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}, g^b\right)}{\prod_{i\in\omega_X} e\left(H_1(i)^{P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}, g^b\right)}$$

$$= e\left(g_1^b, \prod_{i\in\omega_X} g^{P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}\right)$$

$$= e\left(g_1^b, g^{\sum_{i\in\omega_X} P_{\omega_X}(i)\Delta_{i,\omega_X}(0)}\right)$$

$$= e\left(g_1^b, g^{P_{\omega_X}(0)}\right)$$

$$= e\left(g_1^b, g^y\right)$$

$$= e(g_1^b, g_2)$$

$$= e(g_1, g_2)^b.$$

$$k'_Y = \frac{e\left(\prod_{i\in\omega_Y} (g_1 H_1(i))^{P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}, g^a\right)}{\prod_{i\in\omega_Y} e\left(H_2(i)^a, g^{P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}\right)}$$

$$= \frac{\prod_{i\in\omega_Y} e\left(g_1^{P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}, g^a\right)\prod_{i\in\omega_Y} e\left(H_1(i)^{P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}, g^a\right)}{\prod_{i\in\omega_Y} e\left(H_1(i)^{P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}, g^a\right)}$$

$$= e\left(g_1^a, \prod_{i\in\omega_Y} g^{P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}\right)$$

$$= e\left(g_1^a, g^{\sum_{i\in\omega_Y} P_{\omega_Y}(i)\Delta_{i,\omega_Y}(0)}\right)$$

$$= e\left(g_1^a, g^{P_{\omega_Y}(0)}\right)$$

$$= e\left(g_1^a, g^y\right)$$

$$= e\left(g_1^a, g_2\right)$$

$$= e(g_1, g_2)^a$$

So we have:

© 2014, IJOCIT All Rights Reserved

$K'_X.K'_Y = e(g_1,g_2)^b.e(g_1,g_2)^a = e(g_1,g_2)^{a+b} = K,$ which completes the proof. ■

5. Conclusion

In this paper, the security of a two-party attribute-based key agreement protocol (proposed by Wang et al.) is analysed. It is shown that two outsiders who possess some special attributes can collude and obtain the established key. Therefore, the insecurity of Wang et al.'s protocol is concluded.

6. References

[1] H. Wang, Q. Xu, T. Ban, "A Provably Secure Two-Party Attribute-based Key Agreement Protocol," Proceeding of Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE Press, pp. 1042-1045, 2009.

[2] W. Diffie, M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, Vol. 22, pp. 644-654, 1976.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," Lecture Notes in Computer Science, Springer-Verlag, Vol. 196, pp. 47-53, 1984.

[4] H. Guo, Y. Mu, X. Zhang, Z. Li, "Novel and efficient identity-based authenticated key agreement protocols from weil pairings," Lecture Notes in Computer Science, Springer-Verlag, Vol. 5585, pp. 309-323, 2009.

[5] X. Cao, W. Kou, X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," Information Sciences, Vol. 180, pp. 2895-2903, 2010.

[6] A. Sahai, B. Waters, "Fuzzy Identity-Based Encryption," Lecture Notes in Computer Science, Springer-Verlag, Vol. 3494, pp. 457-473, 2005.

[7] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute based encryption for fine-grained access control of encrypted data," Proceeding of the 13th ACM conference on Computer and communications security (CCS 2006), ACM, New York, NY, USA, pp. 89-98, 2006.

[8] J. Baek, W. Susilo, J. Zhou, "New constructions of fuzzy identity-based encryption," ACM Symposium on Information, Computer and Communications Security, ACM New York, NY, USA, pp. 368-37, 2007.

Authors Profile:

Dr Ziba Eslami received her B.S., M.S., and Ph.D. in Applied Mathematics from Tehran University in Iran. She received her Ph.D. in 2000. From 1991 to 2000, she was a resident researcher in the Institute for Studies in Theoretical Physics and Mathematics (IPM), Iran. During the academic years 2000-

© 2014, IJOCIT All Rights Reserved

2003, she was a Post Doctoral Fellow in IPM. She served as a non-resident researcher at IPM during 2003-2005. Currently, she is an associate professor in the Department of Computer Sciences at Shahid Beheshti University in Iran. Her research interests include design theory, combinatorial algorithms, cryptographic protocols, and steganography.

Nasrollah Pakniat received his B.S. degree in Computer Science in 2008 from Shahid Bahonar University, Kerman, Iran. In 2011, he received his M.S. degree in Computer Sciences from Shahid Beheshti University, Tehran, Iran. He is currently a Ph.D. candidate in Mathematics at Shahid Beheshti University, Tehran, Iran. His research interests include applied cryptography and network security.

Mahnaz Noroozi received her B.S. degree in Computer Sciences in 2010 from Sharif University of Technology, Tehran, Iran. In 2012, she received her M.S. degree in Computer Sciences from Shahid Beheshti University, Tehran, Iran. She is currently doing research on cryptographic protocols and their security.

© 2014, IJOCIT All Rights Reserved