An Identity-Based Scheme for Ad Hoc Network Secure Routing Protocol from Pairing

Jue-Sam Chou*, Chu-Hsing Lin** and Chia-Hung Chiu**
*Department of Information management,
Nanhua university
No.32,Chung Keng Li, Dalin
Chaiyi, Taiwan
**Department of Computer Science and Information Engineering,
Tunghai University
No.181, Sec. 3, Taichung Port Rd., Situn District
Taichung, Taiwan

Abstract: - In this article, we discuss the key agreement proposed by Bohio and Miri to implement on the two well-known protocols, Dynamic Source Routing protocol（DSR）and Highly Dynamic Destination-Sequenced Distance-Vector Routing protocol（DSDV）, in an ad hoc network. We point out that the weakness existed in their scheme; it cannot resist the Key Compromise Impersonation (KCI) attack when routing. Moreover, we propose a novel scheme to get rid of this weakness.

Keyword: - Key agreement, Weil paring, Key compromise impersonation attack, Secure routing

1. Introduction

Since Boneh and Franklin proposed the first scheme for identity-based encryption using Weil pairing on elliptic curves [10], many researches designed their identity-based key agreement protocols and signature schemes based on the scheme [6,8,9,12,13]. In 2004, Bohio and Miri proposed an identity-based scheme [11] to be used as a routing protocol in an ad hoc network [1-5]. However, we find that their scheme cannot fullfill the requirements of a sound authenticated key agreement protocol (SAKAP)[16]. In this article, we will first introduce the weakness existed in their scheme [11] and then propose a new solution to solve the problem.

The organization of this article is as follows: in Section 2, we introduce Bilinear Weil paring and the four secure attributes [16] in the key agreement protocols [6-10,12,13]. In Section 3, we briefly review and point out the weakness in Bohio and Miri’s scheme [11]. After that, in Section 4, we remedy the problem and propose a new method. In

Section 5, we analyze the security of our proposed method based on the four secure attributes. Finally, a conclusion is given in Section 6.

2. Preliminaries

In this session, we introduce some related concepts such as Bilinear Weil Paring and the four secure attributes for a sound authenticated key agreement protocol (SAKAP)[16].

2.1. Bilinear Weil Pairing

Let $\mathbb{G}_1$ be a cyclic group generated by P, whose order is a prime q and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard. Let $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a pairing which satisfies the following conditions:

(1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, for any $a, b \in \mathbb{Z}$ and $P, Q \in \mathbb{G}_1$.

(2) Non-degenerate: there exists $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.

(3) Computability: there is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$

2.2. Security Attributes

Assume that there are two parties, A and B, intend to communicate to each other.

(1)Known-Key Security:

In each round of a key agreement protocol, A and B should generate a unique session key. In other words, each session key generated is independent to others and should not be revealed if other session keys are compromised.

(2) Forward Secrecy:

The forward secrecy property is that if A and B's current session key is compromised, the other session keys used before should not be recovered.

(3) Key-Compromise Impersonation (KCI) attacks:

A protocol that is secure against the KCI attack means that if A's long-term secret key is compromised, the adversary who knows this secret key can not impersonate the other party to A.

(4) Unknown Key-Share attack:

After the protocol, A believes that he shares a key with B, but B mistakenly believes that he shares the key with an adversary. A sound authenticated key agreement protocol should prevent this unknown key-share situation.

3. Review of Bohio and Miri's scheme

In this section, we will briefly review the main portion of the scheme proposed by Bohio and Miri, and then examine their scheme based on the four secure attributes in SAKAP [16].

3.1 Bohio and Miri's scheme

(1) Setup:

Let $E: y^2 = x^3 + 1$ over $\mathbb{F}_p$ where $p = 2 \bmod 3$, if the prime number $q > 3$, than $p = lq - 1$ and $q^2 \nmid p + 1$. Let $\mathbb{G}_1$ be an additive subgroup of points on $E(\mathbb{F}_p)$ of order q. The pairing mapping is defined as $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ where $\mathbb{G}_2$ be a multiplicative subgroup of points on $E(\mathbb{F}_{p^2})$ of order q on the elliptic curve. The operator

MapToPoint is defined as follows:
-Compute $x_0 = \left(y_0^2 - 1\right)^{1/3} = \left(y_0^2\right)^{(2p-1)/3} \in \mathbb{F}_p$
-Let $Q = \left(x_0, y_0\right) \in \mathbb{F}_p$
-Output MapToPoint $\left(y_0\right) = Q_{ID}$

(2) Extract:

Each node has his/her own identity, and then computes their own $Q_{id} = \text{MapToPoint}$ $\left(y_0 = H_1\left(ID\right)\right)$, where $H_1 : \{0,1\}^* \to \mathbb{F}_p$. It is assumed that every node would receive its own private key $D_{id}\left(= sQ_{ID}\right)$ based on its identity from the trusted authority (TA). The operations of the TA are as follows:

-TA chooses a secret key s.
-TA computes and sends $D_{id} = sQ_{id}$ to each node with identity (ID) through a secure channel.

(3) Key agreement:

Suppose node A wants to generate a broadcast key shared with a group of nodes to whom he want to broadcast message. Assume that node N is a member in the group, then A and N together compute as follows: (The other member performs the step 1 cooperatively with A in the same manner.)

Step1: A computes $D_{AN} = e\left(D_A, Q_N\right) = e\left(Q_A, Q_N\right)^s$, N computes $D_{NA} = e\left(D_N, Q_A\right) = e\left(Q_N, Q_A\right)^s$, then $D_{AN} = D_{NA} = e\left(Q_A, Q_N\right)^s$

Step2: After generated D_{AN}, node A generates B_{AN} (in [11], B_{AN} is written as k_{1N}) which can be generated in two ways as follows:

- B_{AN} is randomly selected.
- D_{AN} is first computed as $e\left(sQ_A, \sum Q_N\right)$ $= \prod D_{AN}$, N is the other node's ID and then B_{AN} $= H_2\left(D_{AN}\right)$, where $H_2 : \mathbb{G}_2 \to \{0,1\}^m$.

Step3: A computes parameter $P_{A\_brdcst} = B_{AN} \cdot P$.

Step4: A uses the session key, D_{AN}, generated in step 1 to encrypt and transmit the parameter P_{A_brdcst} generated in step3 to the nodes he wants to broadcast to . So that the broadcasted nodes can use it as an input parameter of the hash function H_3. They can compute the same broadcast key K_{A_brdcst} as A does using hash function $H_3 : \mathbb{G}_1 \times \mathbb{G}_1 \to \{0,1\}^m$, where m is the key length. For example, they each compute K_{A_brdcst} as $H_3\left(P_{A\_brdcst}\right)$.

(4) Signature generation and verification:

A uses the broadcast key K_{A_brdcst} to encrypt the broadcasted message M and its signature σ where $\sigma = \{U, V\} = \left\{rQ_A, k_{AN^{-1}}\left(r+h\right)Q_A\right\}$, $h = H_4\left(\mathrm{M}\right)$, and $H_4 : \{0,1\}^* \to \{0,1\}^m$. Any node who receives the encrypted message of (M, σ), and knows K_{A_brdcst} can use it to decrypt the received message and verify the result by the following equation (1)

$$e\left(P_{A\_brdcst}, V\right) \overset{?}{=} e\left(P, U + hQ_A\right) \qquad (1)$$

(5) Secure routing:

After the completion of the above step 1 through 4 in (1), they believe that using the negotiated key K_{A_brdcst} to implement DSR[14] and DSDV[15], the message can be protected well when routing.

3.2 Security weakness:

In this session, we will examine the scheme proposed by Bohio and Miri based on the four secure attributes in [15]. At least, we can come to the conclusion that it is vulnerable to the KCI attack. We show the reason below.

Assume that there is an attacker X who knows the secret key D_A of node A and there is a node B who is the one that X wants to impersonate. Then, X can use the identity of B to communicate with A (Note:

Node B may be the one who just leaves the network or belongs to the net but not login yet). He can launch a KCI attack as the following steps:

Step1: For X knows the secret key D_A of node A, he/she can also get D_{AB} through computing $D = \left(D_A, Q_B\right) \equiv D_{AB}$ which is a session key shared by A and B.

Step2: After obtaining D_{AB}, X can impersonate B to communicate with A, and subsequently he can successfully get the broadcasted parameter P_{A_brdcst} that A uses to generate the broadcast key K_{A_brdcst}. More precisely, X can compute key K_{A_brdcst} by the equation $K_{A\_brdcst} = H_3\left(P_{A\_brdcst}\right)$, thus and he/she is able to know all the information A broadcasted using the key K_{A_brdcst}.

Therefore, through above analysis, we know that Bohio and Miri's scheme is unable to resist KCI attack. In the next section, we would propose a method to solve this problem.

4. Proposed Scheme

Our scheme uses the same assumption as in Bohio and Miri's protocol. In addition, the TA must also computes and publishes the parameter P_{KGC}, where $P_{KGC} = s \cdot P$, and P is a point of group $\mathbb{G}_1$. Under this assumption, we will show our novel key agreement protocol as follows:

Assume that node A wants to inform the other parties (We take node B as an example) to whom he wants to broadcast the parameter, P_{A_brdcst}, to generate the broadcast key K_{A_brdcst}. We display our scheme step by step and show its diagram in figure 1:

Step1: A and B each randomly select a random number, a and b respectively

Step2: A computes $<T_A, P_A>$ and sends it to B where $T_A = aP_{KGC}$, $P_A = H\left(e\left(Q_B, T_A\right)\right)S_A$.

B computes $<T_B, P_B>$ and sends it to A where $T_B = bP_{KGC}$, $P_B = H\left(e\left(Q_A, T_B\right)\right)S_B$.

Step3: After receiving the other party's parameters, each node can verify it as follows:

A check to see if $e\left(Q_A, P_B\right) = e\left(S_A, H\left(e\left(Q_A, T_B\right)\right)Q_B\right)$ holds.

B check to see if $e\left(Q_B, P_A\right) = e\left(S_B, H\left(e\left(Q_B, T_A\right)\right)Q_A\right)$ holds.

Step4: If both above equations hold, then A and B can assure that they are communicating to the intended party they wish. Then,

A computes $K_{AB} = e\left(Q_A, T_B\right)^a e\left(Q_B, T_B\right)^a$ as the session key shared with B, and

B computes $K_{BA} = e\left(Q_B, T_A\right)^b e\left(Q_B, T_A\right)^b$ as the session key shared with A.

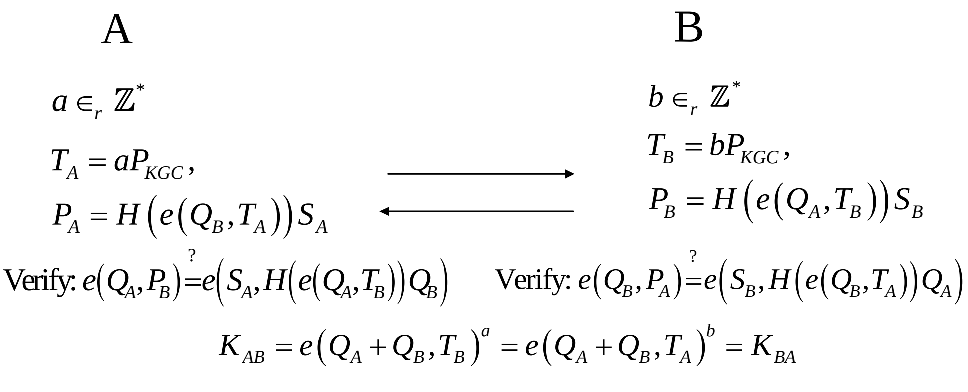
A
B
$a \in_r \mathbb{Z}^*$
$T_A = aP_{KGC}$,
$P_A = H\left(e\left(Q_B, T_A\right)\right)S_A$
$b \in_r \mathbb{Z}^*$
$T_B = bP_{KGC}$,
$P_B = H\left(e\left(Q_A, T_B\right)\right)S_B$
Verify: $e\left(Q_A, P_B\right) \overset{?}{=} e\left(S_A, H\left(e\left(Q_A, T_B\right)\right)Q_B\right)$
Verify: $e\left(Q_B, P_A\right) \overset{?}{=} e\left(S_B, H\left(e\left(Q_B, T_A\right)\right)Q_A\right)$
$K_{AB} = e\left(Q_A + Q_B, T_B\right)^a = e\left(Q_A + Q_B, T_A\right)^b = K_{BA}$

Fig 1. Key Agreement protocol

Step5: After step 4, both A and B are able to transmit the parameter, P_{A_brdcst} , to each other securely using the computed session key $K_{AB}\left(=K_{BA}\right)$. Thus, A and B can use it to generate the broadcast key K_{A_brdcst}.

After completing the above key agreement protocol, node A can use the broadcast key, K_{A_brdcst} encrypted using the computed session key, K_{AB}, to do the secure routing in the same way as Bohio and Miri's protocol does. In the next section, we will show the security analysis of our scheme and we conclude that it can make the routing information more secure when routing.

5. Security Analysis

We analyze our protocol using the four security attributes in [16] as follows:

(1) Known-Key Security：

Because each node generates a unique random number, any attacker cannot compute the current session key even if he knows any of the previously compromised ones.

(2) Forward Secrecy：

For the use of the random numbers a and b used by A and B respectively, the attacker cannot compute any one of the previously used session keys under the assumption that the current session key K_{AB} is compromised.

(3) Key-Compromise Impersonation attack：

Assume that an adversary X have got user A's secret key $S_A\left(=sQ_A\right)$, and he/she wants to impersonate B to communicate with A to get the broadcast key parameter, P_{A_brdcst}. He and A may together do the following steps.

Step1: X randomly selects a number b', computes $T'_B=b'P_{KGC}$, $P'_B= \ H\left(Q_A,T'_B\right)Q_B$ and then sends $\left(T'_B,P'_B\right)$ to A.

Step2: A check to see if $e\left(Q_A,P_B\right)=e\left(S_A,H\left(e\left(Q_A,T_B\right)\right)Q_B\right)$ holds. If it so, X can then can compute the session key shared with A. But we can easily see that the equations cannot hold because $e\left(Q_A,P'_B\right)=e\left(Q_A,H\left(e\left(Q_A,T'_B\right)\right)Q_B\right)$ $\neq e\left(S_A,H\left(e\left(Q_A,T'_B\right)\right)Q_B\right)$

(4) Unknown-key share attack：

If an adversary X eavesdropping on the information transmitted between A and B intends to obtain P_{A_brdcst}. X and A may together do the following steps:

Step1: X intercepts A's information $\left(T_A,P_A\right)$ intended to B, replaces it with $\left(T'_A,P'_A\right)$, where $T'_A=a'T_A$, $P'_A=a'P_A$ and then sends to B.

Step2: User B verifies to see if $e\left(Q_B,P_A\right)=e\left(S_B,H\left(e\left(Q_B,T_A\right)\right)Q_A\right)$ holds.

But it can easily be seen that the equation will not hold since $e\left(Q_B,P'_A\right)=e\left(Q_B,a'P_A\right)=e\left(Q_B,\ a'H\left(e\left(Q_B,T_A\right)\right)S_A\right)\neq e\left(S_B,H\left(e\left(Q_B,T'_A\right)\right)Q_A\right)$.

Hence, our scheme is secure from this attack.

6. Conclusion

In this article, we inspect Bohio and Miris' scheme[11] proposed in 2004 and find that their scheme is vulnerable to the KCI attack. After that, we propose a novel scheme to improve the problem. We also examine our scheme using the four security attributes and conclude that it is secure from the possible attacks.

References:

[1] Yih-Chun Hu, Johnson David B, Perrig Adrian, “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks”, Ad Hoc Networks Volume 1, Issue 1, July, 2003, pp. 175-192.

[2] Gupte Siddhartha, Singhal Mukesh, “Secure routing in mobile wireless ad hoc networks”, Ad Hoc Networks Volume 1, Issue 1, July, 2003, pp. 151-174.

[3] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer., “A secure routing protocol for ad hoc networks”, In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), 2002, pp. 78-89.

[4] Tingyao Jiang, Qinghua Li, Youlin Ruan, “Secure Dynamic Source Routing Protocol”, The Fourth International Conference on Computer and Information Technology (CIT'04), pp. 528-533.

[5] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng, “Anonymous Secure Routing in Mobile Ad-Hoc Networks”, Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) , pp. 102-108.

[6] Choie Young Ju, Jeong Eunkyung, Lee Eunjeong, “Efficient identity-based authenticated key agreement protocol from pairings”, Applied Mathematics and Computation Volume 162, Issue 1, March 4, 2005, pp. 179-188.

[7] Tseng Yuh-Min, “On the security of an efficient two-pass key agreement protocol”, Computer Standards and Interfaces Volume: 26, Issue: 4, August, 2004, pp. 371-374.

[8] Young Ju Choie, Eunkyung Jeong, Eunjeong Lee, “Efficient identity-based authenticated key agreement protocol from pairings”, Applied Mathematics and Computation 162, 2005, pp. 179–188.

[9] Songping Li, Quan Yuan, Jin Li, “Towards Security Two-part Authenticated Key Agreement Protocols”, Cryptology ePrint Archive, Report 2005/300, http://eprint.iacr.org, 2005.

[10] Boneh, M. Franklin,” Identity-based encryption from the Weil pairing”, Advances in Cryptology-CRYPTO 2001, LNCS 2139, 2001, pp. 213-229.

[11] Muhammad Bohio, Ali Miri, “Efficient identity-based security schemes for ad hoc network routing protocols”, Ad Hoc Networks 2 , 2004, pp. 309-317.

[12] Chu-Hsing Lin , and Hsiu-Hsia Lin, "Secure One-Round Tripartite Authenticated Key Agreement Protocol from Weil Pairing , " Proceedings of International Conference on Advanced Information Networking and Applications (AINA 2005) , Vol. 2, March 25-30, 2005 , pp. 135-138.

[13] Chu-Hsing Lin, K. J. Huang and H. H. Lin, “Improving Shim's tripartite authenticated key agreement protocol based on Weil pairing,” Proceedings of 14th Information Security Conference, Taipei, Taiwan, June 10-11, 2004, pp. 250-255.

[14] J. Broch, David B. Johnson, and David A. Maltz, “The dynamic source routing protocol for mobile ad hoc networks”, Internet-Draft Version 03, IETF, October 1999.

[15] Charles E. Perkins, Pravin Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing(DSDV) for Mobile Computers”, In

Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, 1994, pp. 234-244.

[16] S.B Wilson, and A.Meneges, "Authenticated Diffie-Hellman agreemenet protocols" proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC'98), Lecture Notes in Computer Science, 1999, pp. 339-361.