ABHINAV
NATIONAL MONTHLY REFEREED JOURNAL OF RESEARCH IN SCIENCE & TECHNOLOGY
www.abhinavjournal.com

SECURE IDENTITY BASED AUTHENTICATED KEY AGREEMENT PROTOCOLS USING PAIRING

Shubha Katiyar

Associate Professor, Department of Mathematics, Pranveer Singh Institute of Technology,
Kanpur, India
Email: shubha.katiyar@gmail.com

ABSTRACT

Identity based cryptography was first introduced in 1984. Most identity-based key agreement protocols are based on a single PKG (Private Key Generator) environment. In 2002, Chen and Kudla proposed an identity based key agreement protocol for multiple PKG environments. In this paper, we present a new secure identity based authenticated key agreement protocol using pairing. We show that the proposed key agreement protocols satisfy every security requirements of key agreement protocols.

Keywords: Authenticated protocol, key agreement, identity-based protocol, bilinear pairing and Hash function

INTRODUCTION

In 1984, Shamir [12] introduced the concept of identity-based cryptography. In traditional public key cryptosystem, A (Alice) public key is a random string. When B (Bob) wishes to send a message to A, he must first obtain her authenticated public key in public directories. The main idea in ID-based cryptosystems is to eliminate the public key distribution problem by making A's public key derivable from some known aspect of her identity, such as her email address. When B wants to send a message to A, he merely derives A's public key directly from her identifying information. Public key directories are unnecessary. Such cryptosystems alleviate the Certificate overhead and solve the problems of PKG technology: certificate management including storage and distribution and the computational cost of certificate verification. Over the years a number of researchers tried to propose secure and efficient ID-based encryption schemes but with little success. Authenticated key establishment protocols are designed to provide two or more specified entities communicating over an open network with a shared secret key that may subsequently be used to achieve some cryptographic goal such as confidentiality or data integrity. There are two fundamental types of key establishment protocols [9]: key transport and key agreement. Key agreement protocols are more reliable because both entities contribute information that is used to derive the shared secret key. A key agreement protocol is desired to have these fundamental security goals: implicit key authentication and explicit key authentication [14, 17]. A key agreement protocol which provides implicit key authentication to both participating entities is called an authenticated key agreement (AK) protocol, while one providing explicit key authentication to both participating entities is called an authenticated key agreement with key conformation (AKC) protocol.

It is desirable for AK and AKC protocols to possess the following security attributes:

Known-key security: Each run of the protocol should result in a unique secret session key. The compromise of one session key should not compromise other session keys.

Forward secrecy: If long-term private keys of one or more of the entities are compromised, the secrecy of previously established session keys should not be affected. We say that a system has partial forward secrecy if the compromise some but not all of the entities' long-term keys can be corrupted without compromising previously established session keys, and we say that a system has perfect forward secrecy if the long-term keys of all the entities involved may be corrupted without compromising any session key previously established by these entities. There is a further (perhaps stronger) notion of forward secrecy in identity-based systems, which we call TA forward secrecy, which certainly implies perfect forward secrecy. This is the idea that the TA's long-term private key may be corrupted (and hence all users' long-term private keys) without compromising the security of session keys previously established by any user.

Key-compromise impersonation resilience: Compromising an entity A's long-term private key will allow an adversary to impersonate A, but it should not enable the adversary to impersonate other entities to A.

Unknown key-share resilience: An entity A should not be able to be coerced into sharing a key with any entity C when in fact A thinks that she is sharing the key with another entity B.

Key control: Neither entity should be able to force the session key to be a pre- selected value.

Since the basic Diffie-Hellman key agreement scheme that provides the first practical solution to the key distribution problem, numerous protocols have been proposed. But many of these protocols were subsequently found to be flawed. For example, it is known that Unified Model, MTI/C0 and MQV protocol are vulnerable to key-compromise impersonation attack, small subgroup attack, and unknown key-share attack, respectively [1]. At Asiacrypt'96, Just and Vaudenay [5] proposed a 2-AK protocol whose elliptic curve version was subsequently proposed by Song and Kim [15] At Indocrypt'00. But in 2002, Kim [14] pointed that Just-Vaudenay protocol didn't provide protection against KCI attack, and finally present a modified version that can provide. Based on Weil and Tate pairing techniques, several practical ID-AK protocols, e.g., Smart [16], Chen-Kudla [8], Scott [11], Shim [13], and McCullagh - Barreto [8] etc., have been proposed. However, none of these protocols is secure, Xie [18] proposed an ID-AK protocol which is modified from McCullagh-Barreto [8] and asserted it can resistant KCI attack. Songping li, Quan Yuan and Jin li [7] also presented a new security 2-AK protocols that is secure.The paper is organized as follows. In Section 2, we introduce Technical Background (bilinear pairing and Diffie-Hellman assumption). In section 3, we briefly describe Chen and Kudla's key agreement and Li et al's protocol II. In section 4, we proposed our scheme, which is secure and efficient. We also prove security attributes of our scheme. At the end of the paper we give a conclusion of our scheme.

Technical Background

Bilinear Pairing: - In this section, we shall briefly describe the properties of the bilinear pairings. The bilinear parings include Weil pairing and Tate pairing in elliptic curve cryptography. The MOV attack using Weil pairing and the FR attack using Tate pairing reduce the discrete logarithm problem on some elliptic curves to the discrete logarithm problem in a finite field. Later, the bilinear pairings have been used in construction of the identity-based cryptography. We let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 are hard. We let e: $G_1 X G_1 \rightarrow G_2$ is a pairing which satisfies the following properties:

(Bilinear): If P, P_1, P_2, Q_1, Q_2 in G_1

$e(P_1 + P_2 ,Q) = e (P_1 ,Q) e (P_2,Q)$

$e (P, Q_1 + Q_2) = e (P,Q_1) e (P,Q_2)$

(Non-degenerate): If P is a generator of G_1 then $e(P, P) \neq 1$.

(Computability): There is an efficient algorithm to compute e(P, Q) for all P, Q in G_1 in polynomial - time.

The non - degeneracy does not hold for the standard Weil pairing e(P, Q), but it does hold for the modified Weil pairing e(P, Q). We note that the Weil and Tate pairings associated with super singular elliptic curves or abelian varieties can be modified to create such bilinear maps.

- **Diffie-Hellman Assumptions [3]:-** With the group G_1 described in Section 2.1, there are the following problems in elliptic curve cryptography which we use in our protocol frequently:
- **Discrete Logarithm (DL) Problem:** Given P, Q in G_1, find an integer n such that P = nQ whenever such integer exists.
- **Computational Diffie-Hellman (CDH) Problem:** Given a triple (P, aP, bP) in G_1 for a, b in Z_q, find the element abP
- **Decision Diffie-Hellman (DDH) Problem:** Given a quadruple (P, aP, bP, cP) in G_1 for a, b, c in Z_q, decide whether c = ab mod q or not.
- **Bilinear Diffie-Hellman (BDH) problem:** In (G_1, G_2, e) given a quadruple (P, aP, bP, cP) in G_1 for some a, b, c in Z_q. Find the $e (P, P)^{abc}$.

Helping Protocols

Chen and Kudla's Key Agreement [2]:- They presented an identity based authenticated key agreement protocol and analyzed the security using formal security model. Suppose (G_1, +) and (G_2, .) are group of large prime order q. G_1 is generated by, e is the bilinear mapping such that e : $G_1 X G_1 \rightarrow G_2$. Let h_1: 0, $1^* \rightarrow G_1^*$ be a map to point hash function. The PKG chooses a secret key s in Z_q and sets P pub = sP. Let two users A and B with public keys respective $Q_A = H_1 (ID_A)$ and $Q_B = H_1 (ID_B)$ decide to agree upon a common secret key.

They execute the following steps:

- A chooses a random ephemeral key a in Z_q^* computes T_A = aQ_A and sends T_A to B.
- B chooses a random ephemeral key b in Z_q^*, computes T_B = bQ_B and sends T_B to A.
- A computes, K_A =$e(S_A, T_B + aQ_B)$,where S_A = sQ_A is the long term secret key of A sent by the PKG on submitting A's public identity.
- B computes, K_B =$e(S_B, T_A + bQ_A)$,where S_B = sQ_B is the long term secret key of B sent by the PKG on submitting B's public identity.
- After an honest execution of the above steps both A and B will share the common secret key $K_{AB} = K_A = K_B = e(Q_A,Q_B)^{(a+b)s}$

Li Et Al's Protocol Ii [3]:- With the help of the addition operation in the finite field, he will give another modified version. The algorithms of Setup and Extract are similar to Mc-Cullagh, Barreto and Xie's, except the + operation and a system public parameter e(P,P). Let p is an 1024 bits prime, q is an 160 bits prime divisor of p -1, G_1 is a q order subgroup of Z_p^* and G_2 is a q order subgroup of the multiplicative group F_p^* of finite field F_p. The + operation is the addition operation in finite field F_p. The PKG generates $P_A = (Q_A + s)P$ and $P_B = (Q_B + s)P$ as their public keys and $S_A = (Q_A + s)^{-1}$ P and $S_B = (Q_B + s)^{-1}$ P as their private keys. The final shared secret is $K_{AB} = e(P, P)^{ab} + e(P, P)^a . e(P,P)^b$. As the calculations are in finite field, so we know entity A and entity B share the same value above. We also know the value of the shared secret is in finite field Fp but not only in G_2.

Let two users A (Alice) and B (Bob) with public keys respective $Q_A = H_1 (ID_A)$ and $Q_B = H_1 (ID_B)$ decide to agree upon a common secret key. They execute the following steps:

- A chooses a random ephemeral key a in Z_q^*, computes T_A = aP_B and sends T_A to B.
- B chooses a random ephemeral key b in Z_q^*, computes T_B = bP_A and sends T_B to A.
- A computes $K_A = e(T_B, S_A)^a + e(T_B, S_A) . e(P, P)^a$.
- B computes $K_B = e(T_A, S_B)^b + e(T_A, S_B) . e(P ,P)^b$.
- After an honest execution of the above steps both A and B will share the common secret key $K_{AB} = K_A = K_B = e(P, P)^{ab} + e(P, P)^a . e(P, P)^b$.

Proposed Scheme

Initial Set Up: Let p is an 1024 bits prime, q is an 160 bits prime divisor of p-1 , G_1 is a q order subgroup of Z_p^*. Suppose (G_1, +) and (G_2, .) are group of large prime order q, G_1 is generated by P, e is the bilinear mapping such that e : $G_1 X G_1 \rightarrow G_2$. Let the h_1: 0, $1^* \rightarrow G_1^*$ be a map to point hash function. The PKG chooses a secret key s in Z_q^* and sets P_{pub} = s P

Extract: Given a public identity ID in 0, 1^*, the PKG computes the public key $Q_ID = H_1$ (ID) in G_1 and generates the associated private key S_ID = s Q_ID**.**

Key Agreement: Let two users A (Alice) and B (bob) with public keys respective $Q_A = H_1 (ID_A)$ and $Q_B = H_1 (ID_B)$ decide to agree upon a common secret key.

They execute the following steps:

- A chooses a random ephemeral key a in Z_q^*, computes $T_A = aQ_A$ and sends T_A to B.
- B chooses a random ephemeral key b in Z_q^*, computes $T_B = bQ_B$ and sends T_B to A.
- A computes $K_A = e(aT_B ,S_A + Q_A) + e(T_B + aQ_B ,Q_A)$,where $S_A = sQ_A$ is the long term secret key of A sent by the PKG on submitting A's public identity.
- B computes $K_B = e(bT_A ,S_B + Q_B) + e(T_A + bQ_A,Q_B)$,where $S_B = sQ_B$ is the long term secret key of B sent by the PKG on submitting B's public identity.
- After an honest execution of the above steps both A and B will share the common secret key $K_{AB} = K_A = K_B = e(Q_A,Q_B)^{ab\,(s + 1)} + e(Q_A,Q_B)^{(a + b)}$.

Security Attributes. Now we explain our protocol providing the desirable security attributes:

- **Known-key security:** Each run of the key agreement between A and B produces a unique session key due to the random numbers a and b, and there are no ways to get some session key from other session keys.
- **Forward secrecy:** Even if all the long-term private keys of A and B are compromised, it is hard to get $e(Q_A,Q_B)^{ab\,(s + 1)} + e(Q_A,Q_B)^{(a + b)}$, for the adversary that is indispensable in the calculation of KA and KB. So the previous session keys are not affected.
- **Key-compromise impersonation resilience:** Suppose A's long-term private key is disclosed, the adversary C couldn't construct message because C have no knowledge of either a or b and he couldn't calculate K_{AB}.
- **Unknown key-share resilience:** As we usually utilizes the method of tampering the public-key certificates and ID-based key agreement ,since the public-keys are the identities and the public-key certificates are discarded, so unknown key-share attack is hard to be carried into execution and the security attribute of Unknown Key-Share resistant is naturally owned by all ID-based protocols.
- **Key Control:** Neither entity should be able to force the session key to be a pre-selected value for they offer the random number a and b each other.

CONCLUSION

We have investigated some secure issues related to identity based authenticated key agreement and proposed a few new protocols modified from a previous protocol to efficiently achieve certain security properties. We have then used techniques from provable security to analyze the security properties of our new protocols.

REFERENCES

1. C. Boyd and A. Mathuria, "Protocols for Authentication and Key Establishment", Springer-Verlag Press, 2003.

2. L. Chen and C. Kudla, “Identity based authenticated key agreement protocols from pairing” In: Proc. 16th IEEE Security Foundations Workshop, pages 219- 233. IEEE Computer Society Press, 2003.

3. Ratna Dutta,Rana Barua and Palash Sarkar, “ pairing-based cryptographic protocols: a survey”, http://eprint.iacr.org/2004/064.pdf

4. M. C. Gorantla, R. Gangishetti and A. Saxena, “A Survey on ID-Based Cryptographic Primitives” Cryptology ePrint Archive, Report2005/094, 2005, http://eprint.iacr.org/2005/094.

5. M. Just and S. Vaudenay, “Authenticated multi-party key agreement” Advances in Cryptology, Asiacrypt’96, LNCS 537, pp., 19.

6. Law, A. Menezes, M. Qu, J. Solinas, S. Vanstone, “An efficient protocol for authenticated key agreement” Designs, Codes and Cryptography. Marc 2003.

7. Songping li, Quan Yuan and Jin li, “Towards security two-part authenticated key agreement protocols” http://eprint.iacr.org/2005/300.pdf.

8. N. McCullagh and P. S. L. M. Barreto, “A New Two-Party Identity-Based Authenticated Key Agreement” Cryptology ePrint Archive, Report 2004/122, 2004. In Proceeding of CT-RSA 2005. http://eprint.iacr.org/2004/122.

9. Menezes, P. vanOorschot and S. Vanstone, “Handbook of Applied Cryptography” CRC Press. 1997.

10. Menezes, M. Qu and S. A. Vanstone, “Some new key agreement protocols providing implicit authentication” In Workshop on Selected Areas in Cryptography (SAC’95), pp. 22 - 32,1995.

11. M. Scott, “Authenticated ID-based key exchange and remote log-in with insecure token and PIN number” http://eprint.iacr.org/2002/164.pdf.

12. Shamir, “Identity-based cryptosystems and signature schemes”, Advances in cryptology; Crypto’84, LNCS 196, Springer-Verlag, pp. 47-53, 1884.

13. Shim, “Efficient ID-based authenticated key agreement protocol based on the Weil pairing” Electronics Letters 39(8):653-654, 2003.

14. K.Shim, “The Risks of Compromising Secret Information” ICICS 2002, LNCS 2513, pp. 122-133, 2002.

15. Song and K. Kim, “Two-pass authenticated key agreement protocol with key confirmation” Progress in Cryptology, Indocrypto’00, LNCS 1977, pp. 237- 249, 2000.

16. P. Smart, “Identity-based authenticated key agreement protocol based on Weil pairing” Electronics Letters 38(13):630-632, 2002

17. S. B. Wilson and A. Menezes, “Authenticated Diffie-Hellman key agreement protocols” Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC ’98), Lecture Notes in Computer Science, pp. 339-361, 1999.

18. Guohong Xie, “An ID-Based Key Agreement Scheme from pairing” Cryptology ePrint Archive, Report2005/093, 2005.