# Weaknesses of the Boyd-Mao Deniable Authenticated key Establishment for Internet Protocols

Jue-Sam Chou[1] , Yalin Chen [2] , Ming-De Yang [3]

[1]Department of Information Management, Nanhua University Chiayi 622 Taiwan, R.O.C

jschou@mail.nhu.edu.tw

Tel: 886+ (0)5+272-1001 ext.56226

[2] Institute of information systems and applications, National Tsing Hua University

d949702@oz.nthu.edu.tw

Tel: 886+(0)3-5738997

[3] Department of Information Management, Nanhua University Chiayi, 622, Taiwan

asurejoker@gmail.com

Tel: 886+(0)5-2721001 ext.2017

**Abstract**

In 2003, Boyd and Mao proposed two deniable authenticated key establishment protocols using elliptic curve pairings for Internet protocols, one is based on Diffie-Hellman key exchange and the other is based on Public-Key Encryption approach. For the use of elliptic curve pairings, they declared that their schemes could be more efficient than the existing Internet Key Exchange (IKE), nowadays. However in this paper, we will show that both of Boyd-Mao's protocols suffer from the key-Compromise Impersonation attack.

**Keywords:** deniable authenticated key establishment, Internet Key Exchange (IKE), key-Compromise Impersonation attack, elliptic curve cryptosystem

## 1. Introduction

Due to the use of Internet for trade and transmission in this era, the security services such as authentication, data integrity and confidentiality, etc have become more and more important. Therefore, secure communication in the open network environment seems to be an essential requirement for any Internet application [2, 6]. One of the basic secure communication technologies is the key establishment protocol that is known as Internet Key Exchange (IKE). It is the standard of Internet protocol Security (IPSec) proposed by the IETF in 1998 [3, 5, 6, 7, 10]. But, people have many criticisms for this protocol, especially for its complexity [5, 15].

In order to overcome such a problem, the elliptic curve cryptography that can reduce the computations and maintain the same security level becomes a better choice [1, 11, 14, 15, 16, 18]. So in recent years, several cryptography schemes [8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19] are designed based on the elliptic curve. One of these

schemes is the deniable authenticated key establishment for Internet protocols proposed by Boyd and Mao[15]. For the use of the elliptic curve cryptography, their schemes not only solute the complexity of computation but also become more efficient than others.

However, in this paper, we will point out that Boyd-Mao's deniable authenticated key establishment for Internet protocols can't resist against the key-Compromise Impersonation (KCI) attack defined by Wilson and Menezes [4]. The attack means that if A's long-term secret key is compromised and known by an adversary, the adversary can pretend others to communicate with A.

The structure of this paper is organized as follows. In Section 2, we will review Boyd-Mao's deniable authenticated key establishment protocols. In Section 3, we will describe our attacks on Boyd-Mao's key establishment protocols. Finally, a conclusion is given in Section 4.

## 2. Review Boyd-Mao's Deniable Authenticated key Establishment Protocols

In this section, we review Boyd-Mao's deniable authenticated key establishment protocols. First, we will introduce pairings on elliptic curves. Next we will introduce MAC based authenticator. At last, we present the Boyd-Mao's key establishment protocols.

### 2.1 Bilinear Weil Pairing:

Let $G_1$ be an additive group and $G_2$ be a multiplicative group and each of them have the same order. Then we assume that there exists an efficient computable bilinear map e, which is defined as $e: G_1 \times G_1 \to G_2$ and satisfies the following conditions:

1. Bilinear: For any $a, b \in Z$ and $P, Q, R \in G_1$, we have $e(aP, bQ) = e(P, Q)^{ab}$ and $e(P, Q+R) = e(P, Q) \cdot e(P, R)$ and $e(P+Q, R) = e(P, R) \cdot e(Q, R)$.
2. Non-degenerate: For any $P, Q \in G_1$, we have $e(P, Q) \neq 1$.
3. Computability: For any $P, Q \in G_1$, there is an efficient algorithm to compute $e(P, Q) \in G_2$

### 2.2 MAC based authenticator:

To construct the authenticator, user B first chooses a random number $N_B$ and sends it to user A. When A receives $N_B$, he chooses an intended message m and sends it together with $MAC_{F_{AB}}(B, N_B, m)$ to B, where B is user B's ID that is public and the MAC key $F_{AB}$ can be non-interactively computed as the session key shared by both A

and B. That is, A can compute $F_{AB}$ as $e(sQ_A, Q_B)$ and B can compute $F_{BA}(=F_{AB})$ as $e(Q_A, sQ_B)$. The figure of MAC based authenticator is shown in Fig.1.

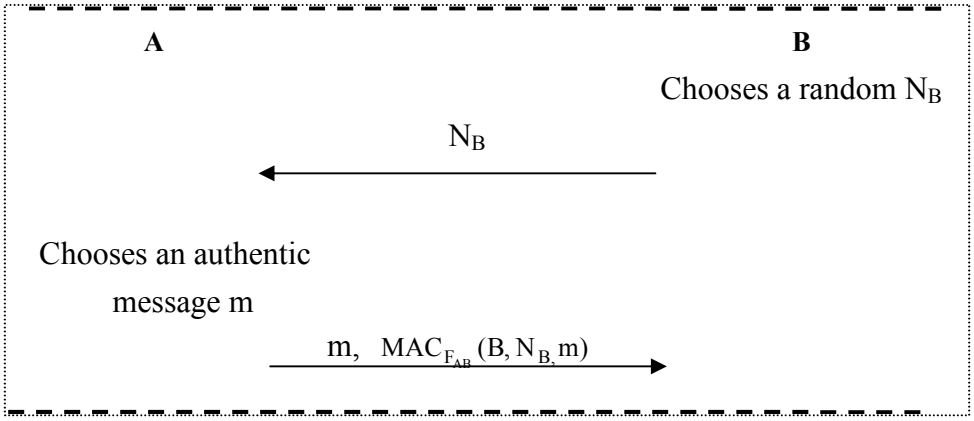


**Fig.1. MAC based authenticator**

### 2.3 Boyd-Mao's key establishment protocols

The Boyd-Mao's key establishment protocols can be divided into two portions, one is the key establishment protocol established using Diffie-Hellman key exchange, and the other key is established from public key encryption approach. Each of them can be stated as follows:

#### 2.3.1 Key Establishment Using Diffie-Hellman Key Exchange

In this scheme, a key exchange between users A and B can be accomplished as follow:

Users A and B each chooses a random number $R_a$ and $R_b$ respectively, then they compute $g^{Ra}$ and $g^{Rb}$ individually, where $R_a$, $R_b$ belongs to $Z_q$ and g is a primitive root. In the protocol, users A's and B's IDs are $ID_A$ and $ID_B$ respectively, and $F_{AB}$ denotes the non-interactively computed MAC key shared by both A and B derived from the bilinear pairing computation. That is, A can compute $F_{AB}$ as $e(sQ_A, Q_B)$ and B can compute $F_{BA}$ ( = $F_{AB}$) as $e(Q_A, sQ_B)$. After that, A and B can begin to exchange information. The steps are as follows:

Step1. User A sends $t_A = g^{Ra}$ to user B. After accepting $t_A$, B will send $t_B = g^{Rb}$ and $MAC_{F_{AB}}(ID_B, t_A, t_B)$ to user A.

Step2. When user A receives $t_B$ and $MAC_{F_{AB}}(ID_B, t_A, t_B)$, he can verify whether the MAC is authentic. If it is authentic, he will send $MAC_{F_{AB}}(ID_A, t_B, t_A)$ to user B. Then A can compute the final session key $Z_{AB} = t_B^{Ra}$ shared with B.

Step3 After accepting the $MAC_{F_{AB}}(ID_A, t_B, t_A)$, B will verify whether the MAC is

authentic. If it is authentic, B then computes the session key $Z_{BA}\ (= Z_{AB} = t_A^{Rb})$.

### 2.3.2 Key Established from Public Key Encryption Approach

In this scheme, users A and B each chooses a random number $N_A$ and $N_B$ respectively, where $N_A, N_B \in [1 \ldots t]$. $F_{AB}$ denotes the same value defined in section 2.3.1. Then, A and B can begin to exchange information. The steps are as follows:

Step1. User B sends $N_B$ to user A. After receiving $N_B$, A chooses a session key K and encrypts it using B's public key denoted as $E_B(K)$. Then A sends $E_B(K)$, $ID_A$, $N_A$, and $MAC_{F_{AB}}(ID_B, N_B, E_B(K))$ to B.

Step2. When B receives $E_B(K)$, $ID_A$, $N_a$, and $MAC_{F_{AB}}(ID_B, N_B, E_B(K))$, he decrypts $E_B(K)$ with his private key to get K and using the MAC key $F_{AB}$ to verify whether the MAC holds. If it holds, B can confirm he is communicating with A and sends $MAC_K(ID_A, ID_B, N_A, N_B)$ to user A.

Step3. After receiving $MAC_K(ID_A, ID_B, N_A, N_B)$, user A verifies whether the MAC holds. If it holds, the MAC is authentic and A can confirm he is communicating with the intended person B. Therefore, user A and B can begin to communicate with each other.

## 3. Our attacks

In this section, we use the four security attributes defined by Wilson and Menezes [4] to analyze Boyd-Mao's key establishment protocols. After that, we can find that Boyd-Mao's key establishment protocols can't resist against the KCI attack. An adversary can pretend others to communicate with A when he obtains A's long-term secret key. Now, we show our KCI attacks on the Boyd-Mao's key establishment protocols as follows:

### 3.1 Attack on the Key Establishment Using Diffie-Hellman Key Exchange

We assume an adversary X who knows user A's long-term secret key $sQ_A$ and wants to launch the KCI attack to pretend user B to communicate with A. He can act as follows:

Step1. When X intercepts $t_A$ sent from A intended to B, X can compute the MAC key $F_{AB}$ in the same manner specified in Section 2.3.1 and choose a random number $R_b'$ to compute $t_B' = g^{R_b'}$. Then he can send $t_B'$ and $MAC_{F_{AB}}(ID_B, t_A, t_B')$ to user A.

Step2. After receiving $t_B'$ and $MAC_{F_{AB}}(ID_B, t_A, t_B')$ from X, user A can verify it as

authentic for he also has the MAC key $F_{AB}$. And because he knows $t_B'$, he can compute the session key $Z_{AB} = ((t_B')^{R_a})$ by Diffie-Hellman key exchange protocol, where $R_a \in_R Z_q$ is selected by A. After that, user A sends $MAC_{F_{AB}}(ID_A, t_B', t_A)$ back to X.

Step3. When X receives $MAC_{F_{AB}}(ID_A, t_B', t_A)$, he can also verify it successfully, because $t_B'$ is computed by himself. So he can take $t_A$ and his secret random $R_b'$ to compute the session key $Z_{AB} = t_A^{Rb'}$. Accordingly, user A and X have the same session key and thus can communicate with each other. Because adversary X can send his message using B's ID, A will believe that he is communicating with B. So, adversary X can pretend to be user B to communicate with A successfully. Therefore, we have a successful KCI attack. The figure of KCI attack on this scheme is shown in Fig.2

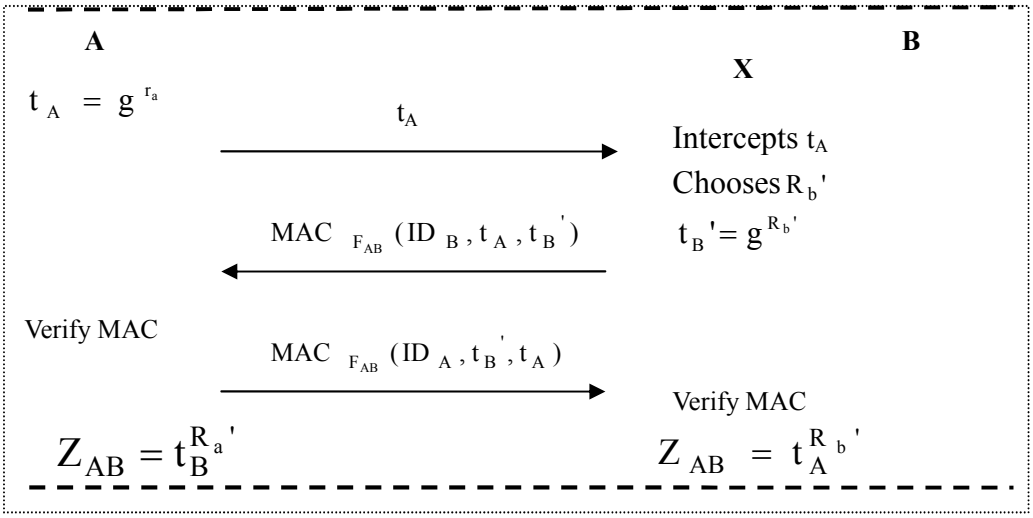


**Fig2. KCI attack on the Key Establishment Using Diffie-Hellman key exchange**

### 3.2 Attack on the Key Establishment based on Public Key Encryption Approach

Here, we assume that an adversary X knows user B's long-term secret key $sQ_B$. Under this assumption, when he wants to launch a KCI attack, he can compute the MAC key $F_{AB}$ to pretend user A to communicate with B. We delineate it as follows:

Step1. After intercepting $N_B$ sent by B, X will choose a random key $K'$ as the shared session key and encrypts it using B's public key denoted as $E_B(K')$. He also chooses a random number $N_A'$. After that, he sends $ID_A, N_A'$, $E_B(K')$ and the computed $MAC_{F_{AB}}(ID_B, N_B, E_B(K'))$ to B.

Step2. After receiving the $E_B(K')$, $ID_{A,}$ $N_A'$, and $MAC_{F_{AB}}(ID_B, N_B, E_B(K'))$, B will decrypt $E_B(K')$ to get $K'$ using his private key and verify to see if $MAC_{F_{AB}}(ID_B, N_B, E_B(K'))$ is authentic. Obviously, B will verify it successfully for he also has the same MAC key $F_{AB}$ as X does. After that B will send the authenticator encrypted with the session key K' selected by X and send $MAC_{K'}(ID_A, ID_B, N_A', N_B)$ to user X. Then X can also verify it successfully for $K'$ is selected by himself.

Step3. Then users B and X will have the same session key $K'$, and thus can communicate with each other. Because X sends his information using A's ID, B will believe that he is communicating with A. So X can pretend user A to communicate with B successfully. Therefore, we also have a successful KCI attack. The figure of KCI attack on this scheme is shown in Fig.3

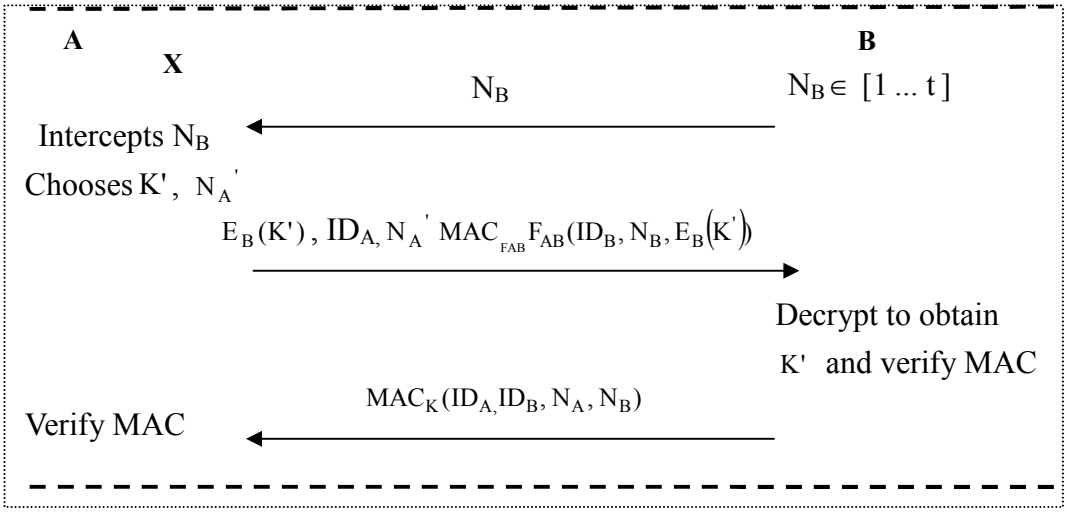


**Fig3. KCI attack on the Key Establishment based on Public Key Encryption**

## 4. Conclusion

In this paper, we have pointed out the weaknesses existed in Boyd-Mao's Deniable Authenticated key Establishment Protocols that it can't resist the KCI attack. Therefore, Boyd-Mao's Deniable Authenticated key Establishment Protocols are not secure enough and need our further work to improve the security of the Internet Key Exchange (IKE) protocol. How to design a more secure and efficient IKE still remains an open problem.

## Reference

[1] A.J. Menezes and T. Okamoto, " Reducing elliptic curve logarithms to a Finite

Field, ” IEEE Transaction on Information Theory, 39(5)(1993)1639-1646.

[2] M. Bellare and P. Rogaway, “ Provably secure session key distribution -the three party case, ” In Proceedings of the 27th ACM Symposium on the Theory of Computing, (1995).

[3] D. Harkins and D. Carrel, “ The Internet Key Exchange (IKE), ” Internet RFC 2409, (1998).

[4] 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, (1999) (339-361)

[5] M.S. Borella, “ Methods and protocols for secure key negotiation using IKE, ” IEEE Network, (2000), 18-29.

[6] J. Zhou, “ Further analysis of the Internet key exchange protocol, ” Computer Communications, (23)(2000)1606-1612.

[7] R. Perlman and C. Kaufman, “ Key exchange in IPSec: Analysis of IKE, ” IEEE Internet Computing, (2000)50-56.

[8] R. Sakai and K. Ohgishiand, “ Cryptosystems based on pairing, ” In The 2000 Sympoium on Cryptography and Information Security, Okinawa, Japan,(2000).

[9] D. Boneh and M. Franklin, “ Identity-based encryption from the Weil pairing,” In Cryptology-CRYPTO 2001, 21st Annual International Cryptology Conference, volume 2139 of LNCS,(2001) 213-229.

[10] R. Canetti and H. Krawczy, “ Security analysis of IKE's signature-based key exchange protocol, ” In Advances in Cryptology ,(2002).

[11] Z.F. Zhang and J. XU, “Attack on an Identification Scheme Based on Gap Diffie-Hellman Problem, ” Cryptology ePrint Archive: Report,(153)(2003).

[12] Z. Chen, “Security analysis on Nalla-Reddy’s ID-based tripartite authenticate key agreement protocols, ” Cryptology ePrint Archive: Listing,(2003).

[13] F. Zhang and. S.N. Reihaneh, “ ID-Based Chameleon Hashes from Biliner Pairings, ” Cryptology ePrint Archive: Report,(128)(2003).

[14] H.M. Sun and B.T. Hsieh, “ Security Analysis of Shim’s Authenticated Key Agreement Protocols from Pairings, ” Cryptology ePrint Archive: Report, (113)(2003)

[15] G. Boyd and W. Mao, “ Deniable Authenticated Key Establishment for Internet Protocols, ” Security Protocols workshop of Cambridge, UK,(2003) 255-271.

[16] H.S. Lee, “ A self-pairing map and its applications to cryptography, ” Applied Mathematics and Computation, (151)(2004) 671-678.

[17] R. Lu and Z. Cao, “ A new deniable authentication protocol from bilinear pairings, ” Applied Mathematics and Computation, (2004).

[18] I. Duursma and H.S. Lee, “ A group key agreement protocol from pairings,”

Applied Mathematics and Computation, (2004).
[19] Y.J. Choie and E.J. Jeong, “Efficient identity-based authenticated key agreement protocol from pairings, ” Applied Mathematics and Computation, (162)(2005) 179-188