Secure Deniable Authenticated Key Establishment for Internet Protocols

Meng-Hui Lim[1], SangGon Lee[2], Youngho Park[3], Sangjae Moon[4]
[1] Department of Ubiquitous IT, Graduate school of Design & IT,
Dongseo University, Busan 617-716, Korea.
menghui.lim@gmail.com
[2] Division of Computer & Information Engineering,
Dongseo University, Busan 617-716, Korea.
nok60@dongseo.ac.kr
[3] School of Electronics and Electrical Engineering,
Sangju National University, Sangju-Si, Gyeongsangbuk-do 742-711, Korea
yhpark@sangju.ac.kr
[4] School of Electrical Engineering and Computer Science,
Kyungpook National University, Daegu 702-701, Korea.
sjmoon@ee.knu.ac.kr

Abstract

In 2003, Boyd et al. have proposed two deniable authenticated key establishment protocols for Internet Key Exchange (IKE). However, both schemes have been broken by Chou et al. in 2005 due to their susceptibility to key-compromise impersonation (KCI) attack. In this paper, we put forward the improved variants of both Boyd et al.'s schemes in order to defeat the KCI attack. On top of justifying our improvements, we further present a detailed security analysis to ensure that the desired security attributes: deniability and authenticity remain preserved.

1. Introduction

Privacy of secure communications over the internet has emerged to be much more essential nowadays. Electronic commerce applications such as electronic voting system, online shopping and online negotiation system may require a deniable authentication protocol to reveal the sender or customer's identity only to the intended receiver. This protocol should be able to allow the receiver to identify the source of a given message by the means of authentication and as long as both the sender and the receiver are not corrupted, no third party should be able to prove that either of them was involved in a specific protocol run. Even if the receiver cooperates with a third party by compromising his long term secret key, the receiver should not be able to convince him fully on the message sender's identity. Hence, the deniable protocol principals can then be capable of denying their involvement after they have taken part in a particular protocol run.

Over the years, many deniable authentication protocols have been proposed but most of them have been proven insecure due to various cryptographic attacks such as the KCI attack [3, 4, 5] and the MITM attack [9]. The KCI attack basically involves an adversary who has obtained the long term secret key of an honest party. Instead of impersonating the corrupted party directly, an adversary may want to exploit the long term key and impersonate another party in a communication run in order to capture valuable information about the corrupted party (e.g. credit card number). Whereas in the MITM attack, an adversary is able to read, insert and modify messages at will between two parties without either party knowing that the link between them has been compromised. This attack can usually be launched successfully when a protocol is employed without authentication.

In 2003, Boyd et al. [1] had proposed 2 deniable authenticated key establishment protocols by employing elliptic curve pairings. The first scheme is a key agreement protocol based on Diffie-Hellman key exchange whereas the second scheme is a key transport protocol based on Public-Key Encryption approach. It is analyzed that both schemes do not only appear to be more efficient than any existing IKE, but also provide absolute deniability and authentication. Hence, these schemes are able to withstand the MITM attack. However in 2005, these schemes are proven to be vulnerable to the KCI attack [4] since the adversary is able to impersonate another entity and establish a known session key with the target principal after the adversary has obtained his long term secret key.

Hence, in this paper, we propose 2 protocol variants based on Boyd et al.'s deniable schemes to conquer their defects, Subsequently, we demonstrate a detailed security scrutiny to prove that our scheme is more secure while preserving the other desired security attributes of a deniable authentication protocol.

2. Secure Deniable Authentication Schemes

2.1. Preliminaries

Let $\mathbf{G_1}$ be a cyclic additive group of a large prime order, q and $\mathbf{G_2}$ be a cyclic multiplicative group of the same order, q. Let e: $\mathbf{G_1}$ x $\mathbf{G_1} \rightarrow \mathbf{G_2}$ be a bilinear pairing with the following properties:

a) **Bilinearity**: $e(aP, bQ) = e(P, Q)^{ab} = e(abP, Q)$ for any $P, Q \in \mathbf{G_1}$, $a, b \in Z_q*$.
b) **Non-degeneracy**: There exists $P, Q \in \mathbf{G_1}$ such that $e(P, Q) \neq 1$.
c) **Computability**: There is an efficient algorithm to compute $e(P,Q)$ for any $P, Q \in \mathbf{G_1}$.

Now, we describe some hard cryptographic problems:

Bilinear Diffie-Hellman Problem (BDHP): Let $\mathbf{G_1}$, $\mathbf{G_2}$, P and e be as above with order q being prime. Given (P, aP, bP, cP) with $a, b, c \in Z_q*$, compute $e(P, P)^{abc} \in \mathbf{G_2}$.

Discrete Logarithm Problem (DLP): Suppose that we are given two groups of elements P and Q, such that $Q = nP$. Find the integer n whenever such an integer exists.

Throughout this paper, we assume that BDHP and DLP are hard such that there is no polynomial time algorithm to solve these two cryptographic problems with non-negligible probability.

2.2. Key Agreement Based on Diffie-Hellman Key Exchange

Proposed Protocol 1. Suppose that two communication parties, A and B wish to communicate with each other. Assume that A and B's long term public/private key pairs are y_A/x_A and y_B/x_B respectively, where $y_A = g^{x_A}$ and $y_B = g^{x_B}$. A generates the static Diffie-Hellman key $F_{AB} = y_B{}^{x_A} = g^{x_A x_B}$, which is used as a message authentication code (MAC) key in this protocol. Similarly, B generates $F_{AB} = y_A{}^{x_B} = g^{x_A x_B}$. Before the communication begins, A and B each chooses an ephemeral private key r_A and r_B, and computes $t_A = g^{r_A}$ and $t_B = g^{r_B}$ respectively, where r_A, $r_B \in Z_q*$ and g is a primitive root. Then, the key exchange can be carried out as follows:

$A \rightarrow B$: t_A
$B \rightarrow A$: t_B , $MAC_{F_{AB}}(B, t_A{}^{x_B}, y_A{}^{r_B}, t_A, t_B)$
(*Event I*)
$A \rightarrow B$: t_B , $MAC_{F_{AB}}(A, t_B{}^{x_A}, y_B{}^{r_A}, t_A, t_B)$
(*Event II*)

Event I: A computes and verifies whether
$MAC_{F_{AB}}(B, y_B{}^{r_A}, t_B{}^{x_A}, t_A, t_B) = MAC_{F_{AB}}(B, t_A{}^{x_B}, y_A{}^{r_B}, t_A, t_B)$.
Event II: B computes and verifies whether
$MAC_{F_{AB}}(A, y_A{}^{r_B}, t_A{}^{x_B}, t_A, t_B) = MAC_{F_{AB}}(A, t_B{}^{x_A}, y_B{}^{r_A}, t_A, t_B)$.
If the verification at both events holds, the communicating parties then compute the session key:

$$A: K_{AB} = kdf(A, B, t_B{}^{r_A}, t_A, t_B),$$
$$B: K_{AB} = kdf(A, B, t_A{}^{r_B}, t_A, t_B),$$

where kdf denotes the one-way key derivation function.

2.3. Key Transport Based on Public Key Encryption

Proposed Protocol 2. Suppose that A and B register ahead of time with a Trusted Authority (TA). The TA picks a master key $s \in Z_q*$ and a collision-free one-way hash functions H: $\{0, 1\}* \rightarrow$ elements of $\mathbf{G_1}$. The TA then computes A's public key $Q_A = H(ID_A)$, and private key $S_A = sQ_A$, where ID_A is denoted as A's identity. Likewise, the TA computes B's public key $Q_B = H(ID_B)$, and private key as $S_B = sQ_B$, where ID_B is denoted as B's identity. Now, A and B can both compute the shared key used in the MAC

$$F_{AB} = e(sQ_A, Q_B) = e(Q_A, Q_B)^s = e(Q_A, sQ_B)$$

In this scheme, we denote the encryption by using A's public key as $E_A(\cdot)$. It is crucial to note that for both the encryption scheme and the non-interactive key agreement scheme, it is advisable that different identities should be used in deriving the relevant public and private keys. For example, one might use $H(A \parallel encrypt)$ and $H(A \parallel share)$ for A's two public keys [1]. With prior to the communication, A and B each chooses a random number N_A and N_B respectively, where N_A, $N_B \in [1..t]$ with a security parameter t. The key transport protocol can then be carried out as follows:

$B \rightarrow A$: $E_A(N_B)$
$A \rightarrow B$: $E_B(K)$, A, N_A, $MAC_{F_{AB}}(B, N_B, E_B(K))$

(***Event III***)
$B \rightarrow A$: $Z_{AB} = MAC_K(A, B, N_A, N_B)$
(***Event IV***)

Event III: B decrypts $E_B(K)$ to obtain K and verifies MAC.
Event IV: A verifies MAC.

If both MAC verifications are successful, K will then be accepted as the session key.

3. Security Analysis

3.1. Security of the Proposed Key Agreement Protocol

In protocol 1, F_{AB} is computed by using both communicating parties' static keys non-interactively. Usually, each communicating party's static public key is supported by a certificate. It is important to note that the use of certificates in this protocol may testify that the owner has registered for participation in the scheme and this may cause the scheme to provide a slightly weaker sense of deniability. However, if B exposes A's identity to a third party, A may still repudiate and argue that B is also able to generate the same messages as A and those messages do not necessarily come from A. Hence, despite the minor disadvantage, A can still deny his participation after he has taken part in the protocol. Likewise, the same situation applies to B whenever A is corrupted.

Note that A achieves full deniability, but B only possesses completed-session deniability. This means that B's deniability can only be guaranteed if A completes the session. In other words, if A aborts during ***Event I***, then B's deniability cannot be proved. Consider the scenario where A is malicious and he attempts to prove the authenticity of the transcript from B to a third party (let's say C). Initially, C provides A with $t_A^* = g^{r_A^*}$ and keeps r_A^* secret. A then carry out the key exchange as follows:
$A \rightarrow B$: t_A^*
$B \rightarrow A$: t_B, $MAC_{F_{AB}}(B, t_A^{*x_B}, y_A^{r_B}, t_A^*, t_B)$
A aborts and hands t_B and $MAC_{F_{AB}}(B, t_A^{*x_B}, y_A^{r_B}, t_A^*, t_B)$ to C. Since only C has the knowledge of r_A^*, he can be sure that $t_A^{*x_B}$ $(= y_B^{r_A^*})$ in the MAC must be computed by B with his long term private key. In this sense, B's deniability is breached. Note that this completed session deniability for the responder B may still be useful in the case where A (client) needs more privacy and full deniability than B (bank or shop).

In terms of authenticity, note that the MAC employed in protocol 1 comprises of the sender's identity and static private key, and it can only be computed by using the secret static key, F_{AB} since the receiver would verify the received MAC by computing it with his secret ephemeral private key and F_{AB} in the next step. Hence, the receiver can always be assured that the message is originated from the intended sender through the MAC verification.

In order to analyze the resistance of protocol 1 against the KCI attack, 2 scenarios are scrutinized here:
a) Suppose that an adversary, E_B has compromised x_A and computed $F_{AB} = y_A^{x_B}$. In this case, he can then attempt fooling A by masquerading as B in a communication run. However, E_B does not know how to calculate $t_A^{x_B}$ $(= y_B^{r_A})$ in the first MAC since he has no knowledge about x_B or r_A. Hence, E_B's attempt will eventually be impeded when A performs the verification in ***Event I***.
b) In contrast, if an adversary, E_A has compromised x_B, obtained $F_{AB} = y_B^{x_A}$ and he wants to fool B by impersonating A in a communication run, E_A would be unable to calculate $t_B^{x_A}$ $(= y_A^{r_B})$ in the second MAC since he has no knowledge about x_A or r_B. Thus, E_A's attempt will finally be obstructed when B performs the verification in ***Event II***.
As a result, we conclude that protocol 1 is completely immune to the KCI attack.

3.2. Security of the Proposed Key Transport Protocol

In protocol 2, F_{AB} is derived from the identity information and no certificate is used. In this case, no third party can actually show that either of them was involved in a protocol run as long as both A and B cooperates. Since the encryption is performed by using the respective public key, protocol 2 can be perfectly simulated by either A or B alone. Hence, absolute deniability is achieved apparently.

Since the previously encrypted contents (N_B and K) are always included in the MACs by the sender, the message receiver could authenticate implicitly whether the previously encrypted contents have been decrypted properly and known by the sender (since only the intended sender can decrypt the prior encryption by using his private key). Based on MAC verification, the message sender can always be authenticated.

Suppose that A's private keys for both the MAC key computation and the encryption scheme have been compromised. An adversary, E_B can therefore compute $F_{AB} = e(sQ_A, Q_B)$. Then E_B impersonates B and establishes a communication round with A. However, he has no idea in decrypting $E_B(K)$ received from A since he does not know B's private key and hence, he would not be able to compute the second MAC. Similarly if an adversary, E_A who wants to fool B, impersonates A in a communication run after he has compromised B's private keys for the MAC key computation and the encryption scheme, he can only obtain $F_{AB} = e(Q_A, sQ_B)$ but not N_B since he does not know A's private key to decrypt $E_A(N_B)$. Therefore, E_A would not be able to compute the first MAC. We again conclude that protocol 2 is able to guard against the KCI attack.

4. Conclusion

In a nutshell, privacy of electronic communications can be secured by employing deniable authenticated key establishment schemes. However, many deniable schemes have been proven insecure due to the KCI attack as well as the MITM attack. In this paper, we have proposed 2 secure protocol variants for the IKE based on Boyd et al.'s deniable schemes. In addition, we have performed a thorough security analysis on both of our protocols and subsequently proved that our protocols are able to withstand the malicious cryptographic attacks while preserving deniability as well as authenticity.

Acknowledgement

This research was supported by MIC of Korea, under ITRC support program supervised by IITA (IITA-2007-C1090- 0701-0026).

References

[1] Boyd C., Mao, W., Paterson, K.G., "Deniable Authenticated Key Establishment for Internet Protocols, 11th International Workshop on Security Protocols", LNCS, vol. 3364, pp. 255-271 (2003)

[2] Cao, T.J., Lin, D.D., Xue, R., "An Efficient ID-based Deniable Authentication Protocol from Pairings", Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05), pp. 388-391 (2005)

[3] Chou, J.S., Chen, Y.L., Huang, J.C., "A ID-Based Deniable Authentication Protocol on Pairings", Cryptology ePrint Archive: Report, (335) (2006)

[4] Chou, J.S., Chen, Y.L., Yang, M.D., "Weaknesses of the Boyd-Mao Deniable Authenticated Key Establishment for Internet Protocols", Cryptology ePrint Archive: Report, (451) (2005)

[5] Lim, M.H., Lee, S.G., Park, Y.H., Lee, H.J., "An Enhanced ID-based Deniable Authentication Protocol on Pairings", Cryptology ePrint Archive: Report, (113) (2007)

[6] Paterson, K.G., "Cryptography from Pairings: A Snapshot of Current Research", Information Security Technical Report, vol. 7(3), pp. 41-54 (2002)

[7] Sakai, R., Ohgishiand, K., "Cryptosystems based on Pairing", Proceedings of 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, (2000)

[8] Blake-Wilson, S., Menezes, A., "Authenticated Diffie-Hellman Key Agreement Protocols", Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98), LNCS, vol. 1556, pp. 339-361 (1999)

[9] Zhu, R.W., Wong, D.S., Lee, C.H., "Cryptanalysis of a Suite of Deniable Authentication Protocols", IEEE Communications Letters, vol. 10, no. 6, pp. 504-506 (2006)