Cryptanalysis on Shim’s tripartite authenticated key agreement protocol from Weil pairing

Chu-Hsing Lin* and Hsiu-Hsia Lin
Department of Computer Sciences and Information Engineering, Tunghai University
E-mail: chlin@mail.thu.edu.tw

Abstract*- In 2003 (Electronics Letters, Vol. 39, No.2), Shim [1] proposed an efficient one-round tripartite authenticated key agreement protocol based on Weil pairing. In this letter, we show that Shim’s protocol cannot satisfy some basic security requirements.*

Keywords: Weil pairing, man-in-the-middle attack, tripartite authenticated key agreement protocol, insider attack, key-compromise impersonation attack.

1. Introduction

In 2000, Joux [2] first proposed a one-round tripartite Diffiee-Hellman key agreement protocol based on Weil pairing. However, the protocol cannot withstand the man-in-the-middle attack since it does not authenticate messages. To ensure authenticity, Shim [1] proposed an improved tripartite authenticated key agreement protocol. Shim introduced the certified public keys to overcome the security flaw in Joux’s protocol. In this article, we show that Shim’s protocol is still insecure against some attacks, such as the insider attack and the key-compromise impersonation attack.

2. Modified Weil pairing

The bilinear characteristic of Weil pairing can be applied to design tripartite key agreement protocols with less communication rounds than using Diffie-Hellman’s scheme (Joux’s protocol just needs one round).

Let p be a prime such that p = 2 (mod) 3 and p = 6q-1 for some prime q>3. Let $E[q]$ be a supersingular curve defined by $y^2 = x^3+1$ over F_p. Let $P\in E/F_p$ be a generator of the group of points with order q = (p+1)/6. Let μ_q be the subgroup of $F_{p^2}{}^*$ that contains all elements of order q. The Weil pairing on the curve $E/F_{p^2}{}^*$ is a mapping $e : G_q \times G_q \rightarrow m_q$. The modified Weil pairing is defined as $\hat{e} : G_q \times G_q \rightarrow m_q$, $\hat{e}(P,Q) = e(P, f(Q))$,where $f(x, y)=(\xi x, y)$, $1\neq\xi\in F_{p^2}{}^*$ is a solution of x^3-1 = 0 (mod$p$) and G_q is the group of points with order q. The modified Weil pairing satisfies the following properties:

(i) *Bilinear*: $\hat{e}(a\cdot P, b\cdot Q) = \hat{e}(P,Q)^{ab}$, for all P, $Q \in E[q]$ and $a, b \in Z$.

(ii) Alternative: $\hat{e}(P,Q) = \hat{e}(Q,P)^{-1}$.

(iii) Non-degenerate: there exists a point $P\in G_q$ such that $\hat{e}(P,P)\neq 1$.

(iv) Polynomial-time computable: $\hat{e}(P,Q)$ is computable in polynomial time.

3. Shim’s tripartite key agreement protocol

***Setup*:**

The public domain parameters (p, q, E, P, $\hat{e}$) are common to all entities. A certification authority (CA) is used to provide public-key certificates; $Cert_A$ denotes the certificate of user A, his public key is denoted as $Y_A = a\cdot P$, where a is A’s static private key. Similarly, $Cert_B$ and $Cert_C$ are the certificates for B and C, with $Y_B = b\cdot P$ and $Y_C = c\cdot P$ as their static public keys, and b and c as their static private keys of B and C, respectively.

***Shim’s protocol*:**

A (B and C) chooses a random number x (y and z) and computes $T_A = x\cdot Y_A$ ($T_B = y\cdot Y_B$ and $T_C = z\cdot Y_C$) and broadcasts the value with his certificate, where x, y and z are used as the ephemeral private keys, respectively.

$A \rightarrow B, C : \{T_A, Cert_A\}$
$B \rightarrow A, C : \{T_B, Cert_B\}$
$C \rightarrow A, B : \{T_C, Cert_C\}$

On receiving the broadcast message, the three entities can obtain the same keys K_A, K_B, and K_C, respectively, the result are as follows:

$$K_A = \hat{e}(T_B, T_C)^{a x \hat{e}(Y_B, Y_C)^a} = \hat{e}(P,P)^{abcxyz\hat{e}(P,P)^{abc}}$$

$$K_B = \hat{e}(T_A, T_C)^{b y \hat{e}(Y_A, Y_C)^b} = \hat{e}(P,P)^{abcxyz\hat{e}(P,P)^{abc}}$$

$$K_C = \hat{e}(T_A, T_B)^{c z \hat{e}(Y_A, Y_C)^c} = \hat{e}(P,P)^{abcxyz\hat{e}(P,P)^{abc}}$$

Then they can compute the shared session key: $K = kdf(K_A \| A \| B \| C) = kdf(K_B \| A \| B \| C) = kdf(K_C \| A \| B \| C)$ (where kdf is a key derivation function)

4. Cryptanalysis on Shim' s protocol

In this section, we present two kinds of attacks on Shim' s scheme including the insider attack and the key-compromise impersonation attack.

4.1. The insider attack

In a tripartite key agreement protocol, the insider attack [3] means that some one of the entities tries to impersonate any other entity. For instance, B is an insider attacker who might try to impersonate C (to fool A) that he and C have participated in a key agreement protocol at the same time, while in fact C does not. If the insider attack is successfully launched in Shim' s protocol, it could have damaging consequences: for example, if C acts as an on-line escrow agent or a referee.

Assumptions

(i) A, B and C: Legal entities appear in a tripartite key agreement protocol.

(ii) $Cert_A$, $Cert_B$ and $Cert_C$: The certificates of A, B and C, respectively, have been certified by a trusted CA.

(iii) B: The insider attacker wants to impersonate C to A and has the $Cert_C$ beforehand.

(iv) C: The insider entity is unknown to the communication round.

Based on the above assumptions the insider attacker B, then, initiates a key agreement protocol, and also plays another role C'(masquerades as C to fool A). Therefore, A mistakenly accepts C' as the real C.

Insider attack algorithm

(I1) B: $T_C' = z' \cdot Y_C = z' \cdot (cP)$.

(I2) $B \rightarrow A, C'$: $\{T_B, Cert_B\}$

(I3) $C' \rightarrow A, B : \{T_C', Cert_C\}$

(I4) $A \rightarrow B, C'$: $\{T_A, Cert_A\}$

(I5) Computes $K_A = K_B = K_C' = \hat{e}(P,P)^{abcxyz'\hat{e}(P,P)^{abc}}$

(I6) $K = kdf\left(K_A \| A \| B \| C'\right) = kdf\left(K_B \| A \| B \| C'\right) = kdf\left(K_C' \| A \| B \| C'\right)$

4.2. Key-compromise impersonation attack

An outsider attacker E, who has compromised B' s static private key b, can also impersonate the other entities to B. The details are illustrated as below.

Assumptions

(i) A, B and C: Legal entities appear n a tripartite key agreement protocol.

(ii) $Cert_A$, $Cert_B$ and $Cert_C$: The certificates of A, B and C, respectively, have been certified by a trusted CA.

(iii) E: The outsider attacker wants to impersonate both of A and C and communicate with B. Note that E now owns the messages $\{b, T_B, Cert_B\}$ and has got the $Cert_A$ and $Cert_C$ beforehand.

(iv) A, C: The insider entities are unknown to this communication round.

The outsider attacker E pretends to be A and C, indicated as A' and C', respectively. E can initiate a key agreement protocol among the three entities A', B and C' and impersonate both the roles of A and C to cheat B. Therefore, B mistakenly believes that A' is the real A and C' is the real C.

Key-compromise impersonation algorithm

(K1) E: $T_A' = u \cdot P$ and $T_C' = w \cdot P$

(K2) $E \rightarrow B$: $\{T_A', Cert_A\}$,$\{T_C', Cert_C\}$

(K3) $B \rightarrow A', C'$: $\{T_B, Cert_B\}$

(K4) Computes $K_A' = K_B = K_C' = \hat{e}(P,P)^{byu\hat{w}(eP,P)^{abc}}$

(K5) $K = kdf\left(K_A' \| A' \| B \| C'\right) = kdf\left(K_B \| A' \| B \| C'\right) = kdf\left(K_C' \| A' \| B \| C'\right)$

5. Conclusion

Shim [1] proposed an improved tripartite authenticated key agreement protocol based on Weil pairing to resist the man-in-the-middle attack. This letter shows that Shim' s tripartite authenticated key agreement protocol is still insecure against some attacks including the insider attack and the key-compromise impersonation. These attacks are due to that the partial messages (such as the public ephemeral key T_A, T_B and T_C) are not authenticated. From the proposed cryptanalysis, Shim' s protocol seems not satisfying some basic security requirements.

References

[1] K. Shim, "Efficient one-round tripartite authenticated key agreement protocol from Weil pairing," Electronics Letters, Vol. 39, no. 2, pp.208-209, January, 2003.

[2] A. Joux, "A one-round protocol for tripartite Diffie-Hellman," Proceedings of the 4th International Algorithmic Number Theory Symposium (ANTS-IV), LNCS 1838, pp.385-394, July, 2000.

[3] S.S. Al-Riyami, and K.G. Paterson, "Tripartite authenticated key agreement protocol from pairings," IMA Conference on Cryptography and Coding 2003, LNCS 2898, pp.332-359, December, 2003.