Security Analysis of a Tripartite Authenticated Key Agreement Protocol Based on Weil Pairing

Gwoboa Horng*, Chao-Liang Liu**, Hsin-Yu Liu***
Institute of Computer Science, National Chung-Hsing University
{gbhorng, s9056001**, s9256050***}@cs.nchu.edu.tw*

Abstract*-In 2004, Lin et al. proposed an improved Shim's key agreement protocol to reduce one Weil pairing operation for efficiency. Unfortunately, their improvement is vulnerable to various attacks. In particular, an adversary can easily masquerade for any arbitrary entity.*

Keywords: Cryptanalysis, Key agreement, Weil pairing, Authentication.

1. Introduction

In 2000, Joux [3] proposed a one round tripartite key agreement protocol based on the Weil pairing. However, Joux's protocol suffers from the man-in-the-middle attack [8]. Latter, Al-Riyami and Paterson [6] proposed a enhancement to improve Joux's protocol. But it was shown that their protocol does not achieve some security in [7]. In 2003, Shim proposed a new ID-based authenticated key agreement protocol by including certified public keys [8]. But, this protocol can not withstand the key-compromise impersonation attack [2]. Recently, Lin et al. [4] argue that Shim's scheme was not efficiently enough. They proposed an improve protocol to reduce one Weil pairing operation by combining long-term keys and ephemeral keys. Their scheme is faster than Shim's, but it is not as secure. In this paper, we show that their improvement is vulnerable to key-compromise impersonation attack. Moreover, their scheme is insecure against impersonation attack since adversaries can easily masquerading for any arbitrary entity.

There are many security requirements have been identified for key agreement protocols [6][9]. We describe them as following. Here we assume A, B are two honest entities, and E is an intruder.

1. **Known session key security:** a protocol is *known session key secure* if, any session keys agreed by any three parties are compromised to E, there is no information for E to learn some other session keys.
2. **Perfect forward secrecy:** a protocol satisfied *perfect forward secrecy* if, the long-term private keys are all compromised the security, of previous session keys is not affected.
3. **Key-compromise impersonation resilience:** a protocol which is secure against the *key compromise impersonation attack* if, A's secret key is disclosed to E, E can not impersonate others to fool A.
4. **Impersonation resilience:** E can not impersonate any one in the group to execute the protocol and get the session keys with A and B.
5. **Unknown key-share resilience**: reference [1][5] for detail.
6. **No key control:** reference [5] for detail.

The remaining paper is organized as follows. In Section 2, we review the Lin et al.'s protocol. Section 3 we point out its weakness. We conclude this paper in Section 4.

2. Review of Lin et al.'s Protocol

In this section we will brief describe notations and protocol, presented in Lin et al.'s paper. It is a one round tripartite authenticated key agreement protocol, which enables three parties to get a common session key.

2.1. Notations

1. p, q: primes, $q > 3$ and $p = 6q - 1$.
2. *kdf*: key derivation function.
3. E : supersingular curve defined by $y^2 = x^3 + 1$ over F_p .
4. P: generator with order q.
5. μ_q : subgroup of $F_{p^2}^*$ that contains all elements of order q.
6. G_q : group of points with order q
7. $\hat{e}$: modified Weil pairing $\hat{e}: G_q \times G_q \to \mu_q$ 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.

8. *CA*: certification authority
9. *A*, *B*, *C*: A, B and C's identifier, respectively.
10. *a*, *b*, *c*: long-term private keys selected by A, B and C, respectively.
11. Y_α : α's public key and $Y_\alpha = \beta \cdot P$, where $(\alpha, \beta) \in \{(A,a),(B,b),(C,c)\}$.
12. $Cert_\alpha$: α's public key certificate issued by *CA*. $Cert_\alpha$ contains α's public key Y_α and unique identifier string of α, where $\alpha \in \{A,B,C\}$.

2.2. Protocol

At first, A, B, and C choose random numbers *x*, *y* and *z* as ephemeral private keys, respectively. Secondly, they compute and broadcast relative value to others. That is,

A broadcasts ($T_A = x \cdot (aP), Cert_A$),
B broadcasts ($T_B = y \cdot (bP), Cert_B$) and
C broadcasts ($T_C = z \cdot (cP), Cert_C$).

Finally, they compute common keys when the other's messages have been arrived.

A: $K_A = \hat{e}(Y_B + T_B, Y_C + T_C)^{a+ax} = \hat{e}(P,P)^{(a+ax)(b+by)(c+cz)}$,

B: $K_B = \hat{e}(Y_A + T_A, Y_C + T_C)^{b+by} = \hat{e}(P,P)^{(a+ax)(b+by)(c+cz)}$,

C: $K_C = \hat{e}(Y_A + T_A, Y_B + T_B)^{c+cz} = \hat{e}(P,P)^{(a+ax)(b+by)(c+cz)}$.

And the shared secret key $K = kdf(K_A \| A \| B \| C) =$ $kdf(K_B \| A \| B \| C) =$ $kdf(K_C \| A \| B \| C)$.

3. Cryptanalysis of Lin et al.'s Protocol

In this section, we present Lin et al.'s scheme does not satisfy two security attributes, which described in section 1. We will show that, an adversary E can impersonate anyone to fool others; even E has no information about the *long-term private keys*. In the same way, their scheme can not resist *key-compromise impersonate attack*.

3.1. Impersonate attack

Suppose E wants to impersonate C and agrees a session key with A and B on Lin et al.'s scheme. Then, E can execute the following steps:

Step1. E eavesdrops to get the certificate of C, chooses random numbers *u* and computes $T'_C = -Y_C + u \cdot P$ to masquerading C. That is,

A broadcasts ($T_A = x \cdot (aP), Cert_A$),
B broadcasts ($T_B = y \cdot (bP), Cert_B$) and
E broadcasts ($T'_C = -Y_C + u \cdot P, Cert_C$).

Step2. The keys computed by A, B, and E are:

$K_A = \hat{e}(Y_B + T_B, Y_C + T'_C)^{a+ax} = \hat{e}(P,P)^{(a+ax)(b+by)u}$

$K_B = \hat{e}(Y_A + T_A, Y_C + T'_C)^{b+by} = \hat{e}(P,P)^{(a+ax)(b+by)u}$

$K_E = \hat{e}(Y_A + T_A, Y_B + T_B)^{u} = \hat{e}(P,P)^{(a+ax)(b+by)u}$

Then the shared secret key $K = kdf(K_A \| A \| B \| C)$ $= kdf(K_B \| A \| B \| C) =$ $kdf(K_E \| A \| B \| C)$.

Thus, E succeeds to impersonate C and agreed a session key with A, B.

3.2. Key-compromise impersonate attack

As in session 1, *key-compromise impersonate attack* is a special case of *impersonation attack*. That is, if E can impersonate any entity without *long-term private key* then *key-compromised impersonate attack* is automatically established. Thus, Lin et al.'s protocol is insecure under *key-compromise impersonate attack*.

4. Conclusions

In this paper, we show that Lin et al.'s protocol is vulnerable to *impersonate attack*. Moreover, either their protocol cannot resist *key-compromised impersonate attack*. Since certificates can't be used to authenticate users under our attacks. We can say that our attack is stronger than *man-in-middle attack*. Finally, to find an efficient and secure tripartite authenticated key agreement protocol deserves future work.

5. Acknowledgement

This research was supported by the National Science Council, Taiwan, R.O.C., under contract number: NSC93-2213-E-005-021.

References

[1] Liqun Chen, Caroline Kudla, "Identity based authenticated key agreement protocols from pairings," *in Proceedings of the 16th IEEE Computer Security Foundations Workshop(CSFW)*, pp. 219-233, 30 June-2 July 2003.

[2] Bin-Tsan Hsieh, Hung-Min Sun, "Key Compromise Impersonation Attack on Shim's Key Agreement Protocol from Weil Pairing," *Symposium on Digital Life and Internet Technologies*, 2003.

[3] A. Joux, "A one round protocol for tripartite Diffie-Hellman," In W. Bosma, editor, *Proceedings of Algorithmic Number Theory Symposium*. ANTS IV, volume 1838 of Lecture notes in Computer Science , pages 385-394, Springer-Verlag, 2000.

[4] Chu-Hsing Lin, Kuo-Jung Huang, Shiu-Shia Lin, "Improving Shim's tripartite authenticated key agreement protocol based on Weil pairing," *Proceedings of 2004 Information Security Conference (ISC'04)*, , pp.250-255, June 10-11, 2004.

[5] C. Mitchell, M. Ward, and P. Wilson, "Key control in key agreement protocols," *Electronics Letters*, 34:980-981, 1998.

[6] Sattam S. Al-Riyami, Kenneth G. Paterson, "Tripartite Authenticated Key Agreement Protocols from Pairings," *IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science Vol. 2898, pp.332-359, Springer-Verlag, Berlin, 2003.* See also Cryptology ePrint Archive, Report 2002/035.

[7] Kyungah Shim, ”Cryptanalysis of Al-Riyami-Paterson's Authenticated Three Party Key Agreement Protocols,” *Cryptology ePrint Archive*, Report 2003/122.

[8] Kyungah Shim, ”Efficient one round tripartite authenticated key agreement protocol from Weil pairing,” *Electronics Letters*, Vol. 39, No. 2, pp. 208-209, 2003.

[9] 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, 199.