Security analysis on Nalla-Reddy's ID-based tripartite authenticated key agreement protocols

Zhongliang Chen
Department of Information Science & Electronic Engineering,
Zhejiang University, Hangzhou, 310027,
Email:chenzl@mail.hz.zj.cn

May 25, 2003

Abstract

In this paper we propose security analysis on passive attack for Nalla-Reddy's ID-AK-2 and ID-AK-3 protocols.

Keywors: Passive attack,Tripartite key agreement,Bilinear pairings

1 Introduction

Recently, several ID-based tripartite authenticated key agreement protocols were proposed [1, 4, 2]. In [2], Nalla and Reddy proposed Three ID-based tripartite authenticated key agreement protocols and provided informal proofs on active attacks for their three protocols, but no security analysis on passive attack for their protocols. In this paper, we propose security analysis on passive attack for Nalla-Reddy's ID-AK-2 and ID-AK-3 protocols.

2 Nalla-Reddy's ID-AK-2 and ID-AK-3 protocols

First, we introduce Nalla-Reddy's ID-based tripartite authenticated key agreement protocols: ID-AK-2 protocol and ID-AK-3 protocol.

Suppose we have a subgroup G of an Elliptic curve for which the modified Weil Pairing $\hat{e}$ maps into the finite field F_{q^k}. i.e., $\hat{e}$ is a modified Weil pairing from $G \times G$ to F_{q^k}.

Let $V : F_{q^k}^* \rightarrow \{0,1\}^*$ be the key derivation function [3] and let $H : \{0,1\}^* \rightarrow G$ denote a cryptographic hash function.

The KGC chooses a secret key $s \in \{1, ..., l-1\}$. The KGC produces a random $P \in G$ and computes $P_{KGC} = [s]P$. Then the KGC publishes (P, P_{KGC}).

Let A, B and C be the three parties wishing to compute a common shared key. A sends its identity ID_A to the KGC and gets its private key from the KGC. A's Public key: $W_A = H(ID_A)$; A's Private key: $w_A = [s]W_A$(computed by the KGC). B's public and private keys are given by $W_B = H(ID_B), w_B = [s]W_B$ and C's public and private keys are given by $W_C = H(ID_C), w_C = [s]W_C$. respectively. The pairs (W_{ID}, w_{ID}) for A, B, and C are their static (or long term) public/private key pairs.

2.1 ID-AK-2 protocol

Each user generates a random number, say $a, b, c \in Z_q^*$. The ephemeral (or short term) public keys would be $[a]P_{KGC}$, $[b]P_{KGC}$, and $[c]P_{KGC}$, and the ephemeral or short term private keys would be a, b and c.

ID-AK-2 protocol is the following:

$$\begin{array}{l} A \rightarrow B, C : [a]P_{KGC}; \\ B \rightarrow C, A : [b]P_{KGC}; \\ C \rightarrow A, B : [c]P_{KGC}; \end{array}$$

Hence the shared secret key is the output of the key derivation function V with k_{ABC} as input where

$$k_{ABC} = k_A = k_B = k_C = \hat{e}([a]W_A + [b]W_B + [c]W_C, [s]P)$$

The secret key is $V(k_{ABC})$.

2.2 ID-AK-3 protocol

Each user generates a random number, say $a, b, c \in Z_q^*$. which are the ephemeral private keys of A, B, and C respectively.

ID-AK-3 protocol is the following:

$$\begin{array}{l} A \to B : [a]P, [a]W_C, A \to C : [a]P, [a]W_B; \\ B \to C : [b]P, [b]W_A, B \to A : [b]P, [b]W_C; \\ C \to A : [c]P, [c]W_B, C \to B : [c]P, [c]W_A; \end{array}$$

Hence the shared secret key is the output of the key derivation function V with k_{ABC} as input where

$$k_{ABC} = k_A = k_B = k_C = \hat{e}([a](W_B+W_C)+[b](W_C+W_A)+[c](W_A+W_B), [s]P)$$

The secret key is $V(k_{ABC})$.

3 Passive attack for Nalla-Reddy's ID-AK-2 and ID-AK-3 protocols

In passive attack, what attacker does is just eavesdropping.

3.1 Passive attack for ID-AK-2 protocol

In ID-AK-2 protocol,

$$\begin{aligned} K_{ABC} &= \hat{e}([a]W_A + [b]W_B + [c]W_C, [s]P) \\ &= \hat{e}(W_A, [a]P_{KGC})\hat{e}(W_B, [b]P_{KGC})\hat{e}(W_C, [c]P_{KGC}) \end{aligned}$$

$W_A, W_B, W_C \in G$ are the public keys of A, B, and C respectively, passive attacker can know them; and when ID-AK-2 protocol is run, passive attacker can eavesdrop $[a]P_{KGC}, [b]P_{KGC}, [c]P_{KGC}$, so passive attacker can compute k_{ABC}.

3.2 Passive attack for ID-AK-3 protocol

In ID-AK-3 protocol,

$$\begin{aligned} K_{ABC} &= \hat{e}([a](W_B + W_C) + [b](W_C + W_A) + [c](W_A + W_B), [s]P) \\ &= \hat{e}([a](W_B + W_C) + [b](W_C + W_A) + [c](W_A + W_B), P_{KGC}) \end{aligned}$$

$P_{KGC} \in G$ are the public keys of KGC, passive attacker can know it; and when ID-AK-3 protocol is run, passive attacker can eavesdrop

$$[a]W_B, [a]W_C, [b]W_C, [b]W_A, [c]W_A, [c]W_B,$$

so passive attacker can compute k_{ABC}.

4 conclusion

Nalla-Reddy's ID-AK-2 and ID-AK-3 protocols are not secure for passive attack.

References

[1] Al-Riyami S. and Paterson K. G.. Authenticated Three Party Key Agreement Protocols from Pairings. Cryptology ePrint Archive, Report 2002/035, available at http://eprint.iacr.org/2002/035/.

[2] Nalla D. and Reddy K.C.. ID-based tripartite Authenticated Key Agreement Protocols from pairings. Cryptology ePrint Archive, Report 2003/004, available at http://eprint.iacr.org/2003/004/.

[3] Smart N.P.. An Identity based authenticated Key Agreement protocol based on the Weil Pairing. Cryptology ePrint Archive, Report 2001/111, available at http://eprint.iacr.org/2001/111/.

[4] Zhang F., Liu S. and Kim K.. ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings. Cryptology ePrint Archive, Report 2002/122, available at http://eprint.iacr.org/2002/122/.