Another attack

The initiator's identity is not included within the nested encryption of message 3. This allows the following attack:

Msg α.1. $A \to S : A, B, N_1$
Msg α.2. $S \to A : \{S, A, B, N_1, PK(B)\}_{SSK(S)}$
Msg α.3. $A \to I_B : A, \{A, Ts, \{N_2\}_{PK(B)}\}_{SK(A)}$
Msg β.3. $I \to B : \{I, Ts, \{N_2\}_{PK(B)}\}_{SK(I)}$
Msg β.4. $B \to S : I, N_3$
Msg β.5. $S \to B : \{S, B, I, N_3, PK(I)\}_{SSK(S)}$
Msg β.6. $B \to I : \{B, N_2\}_{PK(I)}$
Msg α.6. $I_B \to A : \{B, N_2\}_{PK(A)}$.

Fixing the protocol, again

The flaw that allows this can be seen as a violation of both Principle 3 and Principle 5.

It is best fixed by including *a*'s identity inside the nested encryption:

Msg 1. $a \to s : a, b, n_1$
Msg 2. $s \to a : \{s, a, b, n_1, PK(b)\}_{SSK(s)}$
Msg 3. $a \to b : a, \{ts, \{a, n_2\}_{PK(b)}\}_{SK(a)}$
Msg 4. $b \to s : a, n_3$
Msg 5. $s \to b : \{s, b, a, n_3, PK(a)\}_{SSK(s)}$
Msg 6. $b \to a : \{b, n_2\}_{PK(a)}$.

A multiplicity attack

The intruder can replay message 3 (within the lifetime of the timestamp) so as to achieve a repeat authentication:

Msg α.1. $A \to S : A, B, N_1$
Msg α.2. $S \to A : \{S, A, B, N_1, PK(B)\}_{SSK(S)}$
Msg α.3. $A \to B : A, \{Ts, \{A, N_2\}_{PK(B)}\}_{SK(A)}$
Msg α.4. $B \to S : A, N_3$
Msg α.5. $S \to B : \{S, B, A, N_3, PK(A)\}_{SSK(S)}$
Msg α.6. $B \to A : \{B, N_2\}_{PK(A)}$
Msg β.3. $I_A \to B : A, \{Ts, \{A, N_2\}_{PK(B)}\}_{SK(A)}$
Msg β.4. $B \to S : A, N_3'$
Msg β.5. $S \to B : \{S, B, A, N_3', PK(A)\}_{SSK(S)}$
Msg β.6. $B \to I_A : \{B, N_2\}_{PK(A)}$.

About multiplicity attacks

B thinks he has completed two runs of the protocol, but *A* was only willing to run the protocol once.

Does this matter?

It might do, for example if the protocol is used for a financial transaction.

Multiplicity attacks can be prevented by comparing each message received with previous ones (expensive) or via a nonce challenge.