Example of Principle 6

The Otway-Rees Protocol is as follows:

Msg 1. $a \to b : a, b, n_a, \{n_a, a, b\}_{shared(a,s)}$

Msg 2. $b \to s : a, b, n_a, \{n_a, a, b\}_{shared(a,s)}, \{n_b, n_a, a, b\}_{shared(b,s)}$

Msg 3. $s \to b : \{n_b, k_{ab}\}_{shared(b,s)}, \{n_a, k_{ab}\}_{shared(a,s)}$

Msg 4. $b \to a : \{n_a, k_{ab}\}_{shared(a,s)}$.

The following variant was proposed:

Msg 1. $a \to b : a, b, n_a, \{n_a, a, b\}_{shared(a,s)}$

Msg 2. $b \to s : a, b, n_a, n_b, \{n_a, a, b\}_{shared(a,s)}, \{n_a, a, b\}_{shared(b,s)}$

Msg 3. $s \to b : \{n_b, k_{ab}\}_{shared(b,s)}, \{n_a, k_{ab}\}_{shared(a,s)}$

Msg 4. $b \to a : \{n_a, k_{ab}\}_{shared(a,s)}$.

An attack

Assume the intruder has previously run the protocol with B, and stored the component $\{N_i, I, B\}_{shared(B,S)}$ from message 2, and the corresponding N_i. Then the following attack is possible.

Msg 1. $I_A \to B : A, B, N_i', \{N_i, I, B\}_{shared(I,S)}$

Msg 2. $B \to I_S : A, B, N_i', N_b, \{N_i, I, B\}_{shared(I,S)},$
$\{N_i', A, B\}_{shared(B,S)}$

Msg 2′. $I_B \to S : I, B, N_i, N_b, \{N_i, I, B\}_{shared(I,S)},$
$\{N_i, I, B\}_{shared(B,S)}$

Msg 3. $S \to B : \{N_b, K_{ab}\}_{shared(B,S)}, \{N_i, K_{ab}\}_{shared(I,S)}$

Msg 4. $B \to I_A : \{N_i, K_{ab}\}_{shared(I,S)}$

Analysis of the attack

In the original protocol, n_b was being used as a substitute for a's identity in message 3:

Msg 3. $s \to b : \{n_b, k_{ab}\}_{shared(b,s)}, \ldots$

so that b could be sure the key was for use with a.

n_b was bound to a's identity by the encryption in message 2:

Msg 2. $b \to s : \ldots, \{n_b, n_a, a, b\}_{shared(b,s)}$

Removing n_b from the encryption (in the adapted version) broke the link between n_b and a, and so allowed the attack.

A better protocol

Rather than using n_b as a substitute for a's identity, it is better to use a's identity explicitly (and similarly for b). This leads to a much simpler protocol:

Msg 1. $a \to b : a, b, n_a$

Msg 2. $b \to s : a, b, n_b, \{n_a, a\}_{shared(b,s)}$

Msg 3. $s \to b : \{a, n_b, k_{ab}\}_{shared(b,s)}, \{b, n_a, k_{ab}\}_{shared(a,s)}$

Msg 4. $b \to a : \{b, n_a, k_{ab}\}_{shared(a,s)}$.