Security Protocols: Answers to Exercises 2

Security Principles
Gavin Lowe

Answer to Exercise 2.1

In the public key delivery part of the protocol:

Msg 1. $a \rightarrow s : a, b, n_1$
Msg 2. $s \rightarrow a : \{s, a, n_1, PK(b)\}_{SSK(s)}$

there is no guarantee that a receives the key he requests.

The intruder could replace B's name in message 1 with his own, so that A receives the intruder's key instead of B's:

Msg 1. $A \rightarrow I_S : A, B, N_1$
Msg 1'. $I_A \rightarrow S : A, I, N_1$
Msg 2. $S \rightarrow A : \{S, A, N_1, PK(I)\}_{SSK(S)}$

The intruder will then be able to decrypt the resulting message 3, leading to a failure of authentication and secrecy.

Attacking the responder

Similarly, the intruder can arrange for B to receive his key in message 5 instead of A's, so that the intruder can imitate A:

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

Fixing the protocol

The problem is that both key delivery messages do not include the identity of the agent whose key is being delivered—a violation of Principle 3.

This can be fixed by changing the protocol to:

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