Security Models

2020/2021

P. Lafourcade and L.Robert

Session 4

Exercise 1
We consider the following protocol:

1. $A \to B$: $\{\langle A, N_A \rangle\}_{pk(B)}$
2. $B \to A$: $\{\langle N_A, N_B \rangle\}_{pk(A)}$
3. $A \to B$: $\{N_B\}_{pk(B)}$

Give the role description of the protocol.

Exercise 2
We consider the following protocol called FFFGGG:
1 $A \to B$: A
2 $B \to A$: B, N, M, O
3 $A \to B$: $A, \{N, M, O, S\}_{pk(B)}$
4 $B \to A$: $N, X, \{X, Y, S, N\}_{pk(B)}$

We omit to write pairing, you can do the same in your solution. In step 3, if B receives the message $A, \{N, X, Y, S\}_{pk(B)}$ then he only checks the correspondance of N and sees the other data as variables.

- Give the role description of the protocol.
- Give an attack on this protocol showing that S is not secret

Exercise 3

$$\begin{array}{ll} A \to B: & \langle A, N_A \rangle \\ B \to A: & \{\langle N_A, N_B \rangle\}_{K_{ab}} \\ A \to B: & N_B \\ B \to A: & \{\langle K, N_B \rangle\}_{K_{ab}} \\ A \to B: & \{s\}_K \end{array}$$

Intruder knows only identities of A and B.

- There exists an attack allowing the intruder to know the secret s, can you find it?
- Give the associated interleaving for this attack and write the constraints system associated.
- Use simplification rules to transform the system in solved form.

Exercise 4

$$\begin{array}{ll} A \to B: & \{\langle A, K \rangle\}_{K_{ab}} \\ B \to A: & \{s\}_{K_{ab}} \end{array}$$

Intruder knows only identities of A and B. Show that the secret data s is preserved by one single session between A and B.