Security Models

2020/2021

P. Lafourcade and L. Robert

Session 3

Exercise 1

Prove or disprove that a passive Dolev Yao intruder can deduce the following messages with the initial knowledge T_1, where $\{\cdot\}_k$ represents a symmetric encryption scheme with key k.

- $T_1 = \{\langle m_1, m_2\rangle, \{\langle m_1, m_4\rangle\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{\langle m_4, m_7\rangle\}_{m_6}, m_7\}$ and $s = \{m_1\}_{m_1}$.
- $T_1 = \{\{a\}_k, \{c\}_a, \{k\}_{\{a\}_k}\}$ and $s = c$.
- $T_1 = \{\langle m_1, m_2\rangle, \{\langle m_1, m_4\rangle\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{\langle m_4, m_7\rangle\}_{m_6}, m_7\}$ and $s = m_3$.
- $T_1 = \{\{m_1\}_{m_2}, m_2, \{m_3\}_{\langle m_2, m_4\rangle}, \{\langle m_1, m_4\rangle\}_{\langle m_1, m_2\rangle}\}$ and $s = \langle m_3, m_4\rangle$.

Exercise 2

Give the mgu between t and s for the following terms, where x, y, z are variables and a, b constants:

- $t = \langle a, \{z\}_b\rangle$ and $s = \langle x, y\rangle$
- $t = \langle \{x\}_b, \{y\}_b\rangle$ and $s = \langle \{a\}_b, z\rangle$
- $t = \{\langle z, a\rangle\}_x$ and $s = \{\langle y, \{x\}_b\rangle\}_b$

Exercise 3

We define the notion of simple proof: A proof P is simple if each node appears at most once in each branch of P.

Prove that if P is a minimal proof of $T \vdash u$ then P is a simple proof of $T \vdash u$.

Exercise 4

Consider the following protocol:

$$\begin{aligned} A \to B &: \langle \{k_1\}_{k_2}, m\rangle \\ B \to A &: \{m\}_{\langle k_1, k_2\rangle} \end{aligned}$$

Assume that k_2 is a shared key between A and B. Show that k_1 is secret in presence of passive Dolev-Yao intruder.