2001 Paper 9 Question 15

Topics in Concurrency

This question assumes familiarity with the process language **SPL** and its event-based semantics. In the following **SPL** process, *Auth*, agents can behave as initiator or responder in parallel with an attacker *Spy*. Letting A and B range over agent names, define

$$Init(A,B) \equiv out\ new\ x\ \{x, A\}_{Pub(B)}.\,in\{x\}_{Pub(A)}.\ nil$$
$$Resp(B) \equiv in\{x, X\}_{Pub(B)}.\,out\ \{x\}_{Pub(X)}.\ nil$$

$$Auth \equiv \|_{i\in\{init,resp,spy\}}\ P_i \quad \text{where}$$
$$P_{init} \equiv \|_{A,B}\ Init(A,B), \quad P_{resp} \equiv \|_{A}!Resp(A), \text{ and } P_{spy} \equiv !Spy$$

(*a*) Explain briefly and informally the behaviour of $Init(A,B)$ and $Resp(B)$, for agent names A and B. Describe diagrammatically the reachable events of $Init(A,B)$ and $Resp(B)$, taking care to specify the pre- and postconditions, and actions of the events. [5 marks]

(*b*) Write down an **SPL** process for the attacker *Spy*; the process should be able to compose, decompose, encrypt under public keys, and decrypt with leaked private keys. Draw the reachable events of *Spy*. [5 marks]

Assume a sequence of event-transitions

$$\langle Auth, s_0, t_0\rangle \xrightarrow{e_1} \cdots \langle p_{r-1}, s_{r-1}, t_{r-1}\rangle \xrightarrow{e_r} \langle p_r, s_r, t_r\rangle \cdots$$

from the configuration $\langle Auth, s_0, t_0\rangle$, of which it is assumed that the names in *Auth* and the output messages t_0 are included in the name-set s_0. Suppose that the event e_r is the input of a message $\{m\}_{Pub(A)}$ by agent A as initiator. Define a property of subsets of messages t by

$$Q(t) \text{ iff } \forall M \in t.\ m \sqsubset M \Rightarrow \{m, A\}_{Pub(B)} \sqsubset M\ ,$$

where, for instance, $m \sqsubset M$ means m is a submessage of M.

(*c*) Explain briefly why $Q(t_0)$ is true and $Q(t_{r-1})$ is false. [6 marks]

(*d*) Describe, without proof, the possible form(s) of the earliest event e_i for which $Q(t_{i-1})$ is true while $Q(t_i)$ is false. [4 marks]