Protune Negotiation Model

J. L. De Coi, D. Ghita, D. Olmedilla

August 4, 2006

Definition 1 (List) A list of elements is

- either the empty list
- or an element followed by a list

Let l be a non-empty list, therefore it is composed of an element e and a (sub)list l'. e (resp. l') is called *head* (resp. *tail*) of l.

We will write the empty list as [] and a non-empty list as $[head, tail]$.

Definition 2 (Length of a list) The length of a list is a function

$$length : L \rightarrow \mathcal{N}$$

where

- L is the set of all lists
- $\mathcal{N}$ is the set of all natural numbers

such that

- $length([]) = 0$
- $length([head, tail]) = 1 + length(tail)$

Definition 3 (i-th element of a list) The i-th element of a list is a function

$$elementAt : A \rightarrow E$$

where

- $A = \{(n, l) \in \mathcal{N}^* \times L : n \leq length(l)\}$
- $\mathcal{N}^*$ is $\mathcal{N} \setminus \{0\}$
- E is the set of all elements

such that

- $elementAt(1, [head, tail]) = head$
- $elementAt(i, [head, tail]) = elementAt(i - 1, tail)$

Definition 4 (Containment relationship) Let e be an element and l be a list. l *contains* e iff $e = elementAt(i, l)$ for some i.

If e is contained in l we will write (with abuse of notation) $e \in l$.

Definition 5 (Negotiation Message) A negotiation message is an ordered pair

$$(fp, C)$$

where

- $fp \equiv$ a filtered policy
- $C \equiv$ a set of credentials

Definition 6 (Negotation State) A negotiation state is an ordered pair

$$(M_{snd}, M_{rcv})$$

where both M_{snd} and M_{rcv} are lists of messages.

M_{snd} (resp. M_{rcv}) is intended to represent the list of sent (resp. received) messages.

Notice that for each state $s = (M_{snd}, M_{rcv})$ the following expressions represent the sets of credentials globally sent or received so far

$$\bigcup \{C_i : \exists fp_i \ (fp_i, C_i) \in M_{snd}\}$$

$$\bigcup \{C_i : \exists fp_i \ (fp_i, C_i) \in M_{rcv}\}$$

Definition 7 (Peer) A Peer is composed of the following elements

- A policy p
- A set of credentials C
- A set of filtered policies FP
- A set of states S
- A state s_0 (called *initial state*)
- Two sets of messages M_{snd} and M_{rcv}
- A function $tf_{snd} : S \times M_{snd} \to S$ (called *transition function*)
- A function $tf_{rcv} : S \times M_{rcv} \to S$ (called *transition function*)
- A function $f : S \to FP$ (called *filter*)
- A function $csf : S \to \mathcal{P}(C)$ (called *credential selection function*)
- A function $ta : S \to \{true, false\}$ (called *termination algorithm*)

The tuple $(S, s_0, M_{snd}, M_{rcv}, tf_{snd}, tf_{rcv})$ is also called *transition system*, the ordered pair (csf, ta) is also called *negotiation strategy.*

The intended meaning is as follows

- p represents the Peer's policy protecting the local credentials and allowing access to the local resources
- C represents the set of the credentials local to the Peer
- FP represents the set of filtered policies the Peer can send to the other Peer
- S represents the set of states in which the Peer can be
- s_0 represents the initial state, i.e. the state in which the Peer is at the beginning of the negotiation
- M_{snd} (resp. M_{rcv}) represents the set of messages the Peer can send (resp. receive)
- tf_{snd} (resp. tf_{rcv}) represents the Peer's state transition following the sending (resp. reception) of a message
- f represents the process of filtering the Peer's policy according to the current state
- cfs represents the process of selecting the Peer's credentials to send to the other Peer
- ta represent the Peer's decision about whether going on or terminating the current negotiation

Hereafter we will consider Peers with the following characteristics

- s_0 is empty (i.e. it is the ordered pair $([], [])$)
- $f_{snd} : (s_{snd}, m) \rightarrow s'_{snd}$ where
  - $s_{snd} = (M_{snd}, M_{rcv})$
  - $s'_{snd} = ([m, M_{snd}], M_{rcv})$
- $f_{rcv} : (s_{rcv}, m) \rightarrow s'_{rcv}$ where
  - $s_{rcv} = (M_{snd}, M_{rcv})$
  - $s'_{rcv} = (M_{snd}, [m, M_{rcv}])$

Definition 8 (Negotiation) A Negotiation is an ordered pair

$$(P^1, P^2)$$

where P^1 (resp. P^2) is a Peer.

P^1 (resp. P^2) is called *requester Peer* (resp. *provider Peer*).
Hereafter we will consider Negotiations with the following characteristics

- $M^1_{snd} = M^2_{rcv}$
- $M^2_{snd} = M^1_{rcv}$