

# Models and Analysis for Security Protocols

1st Semester 2007/2008

*P. Lafourcade.*

## SET 2

Date: 11.10.2007

### Exercise 1

$S(t)$  is the smallest set such that:

- $t \in S(t)$
- $\langle u, v \rangle \in S(t) \Rightarrow u, v \in S(t)$
- $\{u\}_v \in S(t) \Rightarrow u, v \in S(t)$

$$(A) \frac{u \in T_0}{T_0 \vdash u}$$

$$(UL) \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u}$$

$$(P) \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle}$$

$$(UR) \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$$

$$(C) \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \{u\}_v}$$

$$(D) \frac{T_0 \vdash \{u\}_v \quad T_0 \vdash v}{T_0 \vdash u}$$

We denote  $S'(t) = \{t|_p \mid p \in Pos(t)\}$  the set of subterms of  $t$ .  
Prove that  $S'(t) = S(t)$

### Exercise 2

Let  $T$  be a set of terms. The mapping  $S : T \rightarrow T$ . Prove that

1.  $S(A \cup B) = S(A) \cup S(B)$
2.  $S$  is idempotent:  $S(S(A)) = S(A)$
3.  $S$  is monotonous: if  $A \subseteq B$  then  $S(A) \subseteq S(B)$
4.  $S$  is transitive: if for all  $X, Y, Z \subseteq T$ ,  $X \subseteq S(Y)$  and  $Y \subseteq S(Z)$  implies  $X \subseteq S(Z)$ .

### Exercise 3

If  $P$  is a minimal proof of  $T \vdash u$  then  $P$  is a simple proof of  $T \vdash u$ .

#### Exercise 4

We propose the following procedure to know if  $\{t_1, \dots, t_n\} \vdash_{\mathcal{I}_{DY}} t$ :

1. Apply first the rules decomposition  $(D)$ ,  $(UR)$ ,  $(UL)$ :

$$(UL) \quad \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u} \qquad (UR) \quad \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$$

$$(D) \quad \frac{T_0 \vdash \{u\}_v \quad T_0 \vdash v}{T_0 \vdash u}$$

until to reach a fix point.

2. Try to build  $t$  from this new set of terms using only composition rules  $(P)$ ,  $(C)$ :

$$(P) \quad \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle} \qquad (C) \quad \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \{u\}_v}$$

Why this procedure is false?

What is the restriction we have to add to get this result true?

#### Exercise 5

Consider the following protocol:

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

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.

#### Exercise 6

Give an exemple of inference system for which the locality property is false.

#### Exercise 7

Find an attack using a passive intruder aganst Shamir 3-Pass Protocol if we used Vernam encryption.

$$\begin{aligned} 1 \quad A \rightarrow B &: \{m\}_{K_A} \\ 2 \quad B \rightarrow A &: \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A} \\ 3 \quad A \rightarrow B &: \{m\}_{K_B} \end{aligned}$$