

F. Autreau
P. Lafourcade
JL. Roch

P. Lafourcade.

SET 6

Date: 13.11.2007

$$\begin{array}{llll}
 R_1 & C \cup \{T \Vdash u\} & \rightsquigarrow & C & \text{if } T \cup \{x \mid \\
 & & & & T' \Vdash x \in C, T' \subset T\} \vdash u \\
 R_2 & C \cup \{T \Vdash u\} & \rightsquigarrow_{\sigma} & C\sigma \cup \{T\sigma \Vdash u\sigma\} & \sigma = mgu(t, u), t \in st(T), \\
 & & & & t, u \text{ no variables} \\
 R_3 & C \cup \{T \Vdash u\} & \rightsquigarrow_{\sigma} & C\sigma \cup \{T\sigma \Vdash u\sigma\} & \sigma = mgu(t_1, t_2), t_1, t_2 \in st(T), \\
 & & & & t_1, t_2 \text{ no variables} \\
 R_4 & C \cup \{T \Vdash \{u\}_v\} & \rightsquigarrow & C \cup \{T \Vdash u, T \Vdash v\} & \\
 R_5 & C \cup \{T \Vdash \langle u, v \rangle\} & \rightsquigarrow & C \cup \{T \Vdash u, T \Vdash v\} & \\
 R_6 & C \cup \{T \Vdash u\} & \rightsquigarrow & \perp & \text{if } T = \emptyset \text{ or} \\
 & & & & var(T) = var(u) = \emptyset \text{ and } T \not\vdash u
 \end{array}$$

Exercise 1

Denning-Sacco Protocol

1. $A \rightarrow S : \langle A, B \rangle$
2. $S \rightarrow A : \{ \{ \langle B, N_{AB} \rangle, \langle N_s, \{ \langle N_{AB}, \langle A, N_s \rangle \} \}_{K_{BS}} \} \}_{K_{AS}}$
3. $A \rightarrow B : \{ \langle N_{AB}, \langle A, N_s \rangle \} \}_{K_{BS}}$
4. $B \rightarrow A : \{ s_{AB} \}_{N_{AB}}$

$P_{DS} = \{R_A, R_B, R_S\}$ models one session of A, B and S .

Exercise 2

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

Intruder knows only identities of A and B .

- Give role specification of this protocol of an instance of execution between A and B .
- Give a constraint system associated to this protocol between A and B .

Exercise 3

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

Intruder knows only identities of A and B .

- Use simplification rules to transform the system in solved form.
- There exists an easy attack, can you find it ?

Exercise 4

$$\begin{aligned}A &\rightarrow B : \{\langle A, K \rangle\}_{K_{ab}} \\B &\rightarrow A : \{s\}_{K_{ab}}\end{aligned}$$

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