

# Models and Analysis for Security Protocols

1st Semester 2007/2008

P. Lafourcade.

## SET 3

Date: 25.10.2007

### 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.  $A \rightarrow B : \{ \{ N_{AB}, \langle A, N_s \rangle \} \}_{K_{BS}}$
4.  $B \rightarrow A : \{ s_{AB} \}_{N_{AB}}$

Write down each agent's role description.

**Solution :**

$$R_A = (init \rightarrow \langle A, B \rangle, \\ \{ \{ \langle B, x_A \rangle, \langle y_A, z_A \rangle \} \}_{K_{AS}} \rightarrow z_A, \\ \{ w_A \}_{x_A} \rightarrow stop)$$

$$R_B = (\{ x_B, \langle a, y_B \rangle \}_{K_{BS}} \rightarrow \{ s_{AB} \}_{x_B})$$

$$R_S = (\langle A, B \rangle \rightarrow \{ \langle B, N_{AB}, \langle N_S, \langle A, N_S \rangle \} \}_{K_{BS}} \}_{K_{AS}})$$

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

### Exercise 2

Consider the following protocol:

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

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

**Solution :**

- Give role specification of this protocol of an instance of execution between  $A$  and  $B$ .

$$T_1 = \{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K\}$$

$$R_A = \begin{aligned} & (init \rightarrow \langle A, N_A \rangle), \\ & (\{\langle N_A, X_{N_B} \rangle\}_{K_{ab}} \rightarrow X_{N_B}), \\ & (\{\langle X_K, X_{N_B} \rangle\}_{K_{ab}} \rightarrow \{s\}_{X_K}) \end{aligned}$$

$$R_B = \begin{aligned} & (\langle X_A, X_{N_A} \rangle \rightarrow \{\langle X_{N_A}, N_B \rangle\}_{K_{ab}}) \\ & (N_B \rightarrow \{\langle K, N_B \rangle\}_{K_{ab}}), \\ & (\{X_s\}_K \rightarrow stop) \end{aligned}$$

- Give a constraint system associated to this protocol between  $A$  and  $B$ .  $T_1 = \{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K\}$

Constraints System

$$\begin{array}{ll} T_1 & \Vdash \langle A, X_{N_A} \rangle \\ T_2 = T_1 \cup \{\langle A, X_{N_A} \rangle\} & \Vdash \{\langle X_{N_A}, X_{N_B} \rangle\}_{X_{K_{AB}}} \\ T_3 = T_2 \cup \{\{\langle X_{N_A}, X_{N_B} \rangle\}_{X_{K_{AB}}}\} & \Vdash X_{N_B} \\ T_4 = T_3 \cup \{X_{N_B}\} & \Vdash \{\langle X_K, X_B \rangle\}_{X_{K_{AB}}} \\ T_5 = T_4 \cup \{\{\langle X_K, X_B \rangle\}_{X_{K_{AB}}}\} & \Vdash \{s\}_{X_K} \\ T_6 = T_5 \cup \{\{s\}_{X_K}\} & \Vdash s \end{array}$$

- Use simplification rules to transform the system in solved form.

$$T_1 = \{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K\}$$

$$\begin{array}{ll} C_1 \quad T_1 & \Vdash \langle A, X_{N_A} \rangle \\ C_2 \quad T_2 = T_1 \cup \{\langle A, X_{N_A} \rangle\} & \Vdash \{\langle X_{N_A}, X_{N_B} \rangle\}_{X_{K_{AB}}} \\ C_3 \quad T_3 = T_2 \cup \{\{\langle X_{N_A}, X_{N_B} \rangle\}_{X_{K_{AB}}}\} & \Vdash X_{N_B} \\ C_4 \quad T_4 = T_3 \cup \{X_{N_B}\} & \Vdash \{\langle X_K, X_B \rangle\}_{X_{K_{AB}}} \\ C_5 \quad T_5 = T_4 \cup \{\{\langle X_K, X_B \rangle\}_{X_{K_{AB}}}\} & \Vdash \{s\}_{X_K} \\ C_6 \quad T_6 = T_5 \cup \{\{s\}_{X_K}\} & \Vdash s \end{array}$$

Road book

- Apply  $R_4, R_1$  and  $R_2$  on  $C_1$  give  $\sigma = \{X_{N_B} \rightarrow N_A\}$

- Apply  $R_4, R_5, R_2$ , on  $\sigma_0 C_2$  give  $\sigma_1 = \{X_{N_B} \rightarrow N_B\}$  (or  $N_A$ )
  - Apply  $R_1$  on  $\sigma_1 C_3$
  - Apply  $R_4, R_5, R_2$  on  $\sigma_1 \sigma_0 C_4$  give  $\sigma_2 = \{X_K \rightarrow N_A\}$
  - Apply  $R_4$ , on  $\sigma_2 \sigma_1 \sigma_0 C_5$
- There exists an easy attack, can you find it ?

- 1  $A \rightarrow B : \langle A, N_A \rangle$
- 2  $B \rightarrow A : \{\langle N_A, N_B \rangle\}_{K_{ab}}$
- 3  $A \rightarrow B : N_B$
- 4  $B \rightarrow A : \{\langle K, N_B \rangle\}_{K_{ab}}$
- 5  $A \rightarrow B : \{s\}_K$

Yes, the resolution of constraints system gives to use the following attack: send 2st message  $\{\langle N_A, N_B \rangle\}_{K_{ab}}$  instead of the 4th  $\{\langle K, N_B \rangle\}_{K_{ab}}$  message. Hence  $A$  will replay  $\{s\}_{N_A}$  because intruder knows  $N_A$ .

### Exercise 3

Consider the following protocol:

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

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

**Solution :** All attempts for resolution give a constraint system in solved form with bottom.

### 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  $B$ .

Give a modeling of this Protocol in Horn clauses, with capabilities of the intruder.

**Solution :**

$$\begin{aligned} & \frac{I(pk(sk(Y)))}{I(enc((pk(sk(A)), K[pk(sk(Y))]), sk(AB)))} \\ & \frac{I(enc((X, Z), sk(AB)))}{I(enc(s, sk(AB)))} \\ & \frac{I(m), I(n)}{I(pair(m, n))} (pair) \quad \frac{I(pair(m, n))}{I(m)} (UL) \quad \frac{I(pair(m, n))}{I(n)} (UR) \\ & \frac{I(m), I(pubk)}{I(enc(m, pubk))} (encrypt) \quad \frac{I(enc(m, pk(x))), I(x)}{I(m)} (decrypt) \end{aligned}$$