TD5 – Modélisation des protocôles de sécurité

Exercice 1: En fonction de quelle connaissance initiale de chaque participant le protocôle suivant est correctement construit ? En particulier, peut K_{AB} être une clé de session ?

$$\begin{array}{ll} A \longrightarrow S: & A, B \\ S \longrightarrow A: & \{A, B, N\}_{K_{AB}} \\ A \longrightarrow B: & \{M\}_{K_{AB}} \end{array}$$

Exercice 2: Considérons le protocôle suivant :

$$\begin{array}{lll} 1. & A \longrightarrow S & : A, B, N_1 \\ 2. & S \longrightarrow A & : \{A, N_1, K_{AB}\}_{K_A}, \{B, N_1, K_{AB}\}_{K_B} \\ 3. & A \longrightarrow B & : \{N_2\}_{K_{AB}}, \{B, N_1, K_{AB}\}_{K_B} \\ 4. & B \longrightarrow A & : \{N_1, N_2\}_{K_{AB}} \\ 5. & A \longrightarrow B & : \{M\}_{K_{AB}} \end{array}$$

La connaissance initiale du serveur comprend la clé publique des autres.

- Est-ce que ce protocôle est correctement construit ?
- Décrire plusieurs assertions (confidentialité, authenticité) pour ce protocôle.
- Identifier, parmi ces assertions, une ou plusieurs qui n'est ou ne sont pas satisfaite(s), et donner une attaque qui montre le problème. Montrer aussi la correctitude de l'attaque ! (en construisant la connaissance de chaque participant, y compris l'intrus, après chaque pas de l'attaque)

Exercice 3: Ci-dessous on trouve une attaque contre un certain protocôle. Construire le protocôle complet, vérifier sa correctitude syntaxique en fonction des connaissances initiales de chaque participant, donner des assertions propres à ce protocôle, décrire une attaque contre une de ces assertions, montrer sa correctitude et donner une "parade" contre cette attaque :

$$\begin{array}{lll} M_1. & A \longrightarrow S: & A, B, N_A \\ M_2. & S \longrightarrow A: & S, \{S, A, N_A, K_B\}_{K_S^{-1}} \end{array}$$

$$\begin{array}{lll} M_1.1. & A \longrightarrow M_S: & A, B, N_A \\ M_2.1. & M_A \longrightarrow S: & ... \\ M_2.2. & S \longrightarrow M_A: & ... \\ M_1.2. & M_S \longrightarrow A: & ... \end{array}$$

Exercice 4: Mêmes questions pour le protocôle suivant :

$$\begin{array}{ll} M_1. & A \longrightarrow S: \quad A, B, N_1 \\ M_2. & S \longrightarrow A: \quad \{N_1, B, K_{AB}, \{K_{AB}\}_{K_{BS}}\}_{K_{AS}} \\ M_3. & A \longrightarrow B: \quad A, B, \{K_{AB}\}_{K_{BS}} \\ M_4. & B \longrightarrow A: \quad A, B, \{N_2\}_{K_{AB}} \\ M_5. & A \longrightarrow B: \quad \{N_2 - 1\}_{K_{AB}} \end{array}$$

Exercice 5: Décrire le protocôle suivant et donner une attaque contre lui :

$$\begin{array}{ll} M_1. & A \longrightarrow B: \quad A, \{N_A\}_{K_{AB}} \\ M_2. & B \longrightarrow A: \quad \{N_A + 1\}_{K_{AB}} \end{array}$$
