Protocole NOMITM

Description et schéma

JEKKAM Issame, GURTNER Leo, GEORGEON Gautier

Protocole

Le protocole est décrit comme suit :

$$
\begin{aligned}
&(1) \quad A \to B : A, N_a \\
&(2) \quad B \to A : \{B, N_b, N_a\}_{\text{pub}(A)} \\
&(3) \quad A \to B : \{K_{AB}, N_b, N_a\}_{\text{pub}(B)} \\
&(4) \quad B \to A : H(K_{AB}, N_a)
\end{aligned}
$$

Connaissances initiales On suppose qu'au début du protocole les agents A et B connaissent la clé publique $\text{pub}(C)$ de tout agent C.

Valeurs générées Les nonces N_a et N_b sont générés à la première exécution. La clé de session K_{AB} est choisie par A.

Description pas à pas

1. A envoie son identité et un nonce N_a à B.
2. B génère N_b et renvoie (B, N_b, N_a) chiffré avec $\text{pub}(A)$. B répond à l'identité qui a été donnée dans le message à l'étape 1, c'est-à-dire A.
3. A vérifie N_a, puis envoie (K_{AB}, N_b, N_a) chiffré avec $\text{pub}(B)$. A répond à l'identité envoyée dans le chiffré, c'est-à-dire B.
4. B vérifie les nonces et renvoie une preuve de possession $H(K_{AB}, N_a)$.

Propriétés de sécurité (intuitives)

— **Authentification :** les nonces assurent la fraîcheur ; le message (4) confirme que B connaît K_{AB}.
— **Confidentialité et intégrité :** K_{AB} n'est connu que de A et B (clés privées gardées secrètes).

Calcul du coût

Règles utilisées.

(1) $A \to B : A, N_a$ Message en clair à deux atomes :

$$c_1 = f(A) + f(N_a) = 1 + 1 = \boxed{2}.$$

(2) $B \to A : \{B, N_b, N_a\}_{\mathrm{pub}(()A)}$ On modélise la triple concaténation par des paires imbriquées :

$$\begin{aligned} f\big(\langle B, N_b\rangle\big) &= 50 + 1 + 1 = 52, \\ f\big(\langle\langle B, N_b\rangle, N_a\rangle\big) &= 50 + 52 + 1 = 103, \\ c_2 &= 1 + 103 + f\big(\mathrm{pub}(()A)\big) = 1 + 103 + 1 = \boxed{105}. \end{aligned}$$

(3) $A \to B : \{K_{AB}, N_b, N_a\}_{\mathrm{pub}(()B)}$

$$\begin{aligned} f\big(\langle K_{AB}, N_b\rangle\big) &= 50 + 1 + 1 = 52, \\ f\big(\langle\langle K_{AB}, N_b\rangle, N_a\rangle\big) &= 50 + 52 + 1 = 103, \\ c_3 &= 1 + 103 + f\big(\mathrm{pub}(()B)\big) = 1 + 103 + 1 = \boxed{105}. \end{aligned}$$

(4) $B \to A : H(K_{AB}, N_a)$

$$\begin{aligned} f\big(\langle K_{AB}, N_a\rangle\big) &= 50 + 1 + 1 = 52, \\ c_4 &= 20 + 0.5 \times 52 = \boxed{46}. \end{aligned}$$

Coût total du protocole

$$\boxed{c(P) = c_1 + c_2 + c_3 + c_4 = 2 + 105 + 105 + 46 = \mathbf{258}}.$$