Protocoles de Sécurité et Vérification
Description du Protocole

1 Description du protocole

Notre protocole à clé publique est décrit comme suit :

$$
\begin{aligned}
&B \to S : \{N_b\}_{pub(S)}\{B\}_{N_b}\{B\}_{N_b} \\
&S \to A : \{N_b\}_{K_{as}}\{B\}_{N_b}\{K\}_{K_{as}} \\
&A \to B : \{N_b\}_{pub(B)}\{K\}_{pub(B)} \\
&B \to A : \{N_b\}_K
\end{aligned}
$$

Connaissances initiales

On suppose qu'au début du protocole, les agents A et B connaissent la clé publique $pub(C)$ de tout agent C. S est un serveur honnête.

Valeurs générées

— N_b est un nonce généré par B.
— K est une clé générée par S à chaque communication.

Description des étapes

1. L'agent B envoie un nombre aléatoire N_b chiffré avec la clé publique de S, son nom B chiffré avec N_b et le nom de B chiffré avec N_b à S.
2. S déchiffre l'entièreté du message de B. S communique avec A qui est le destinataire du message 1. Il lui envoie le nonce N_b chiffré avec la clé privée qu'il possède entre S et A : K_{as}, B chiffré avec N_b et K chiffré avec la clé privée entre S et A.
3. A déchiffre les élements reçus par S. Il retient la clé K et le nonce N_b. Il envoie à B le N_b chiffré avec la clé publique de B, et il envoie aussi la clé privé K chiffré avec la clé publique de B

4. B déchiffre les élements reçus par A et vérifie que le nonce reçu est bien le nonce généré. Ensuite il envoie au même A le nonce de B N_b chiffré avec la clé privée K. Donc B sait qu'il communique bien avec A
5. A déchiffre les élements envoyés par B, il vérifie que c'est bien le même N_b afin de confirmer la communiquation avec A.

Règles de sécurité

— Si un agent ne reçoit pas de message alors qu'il devrait pendant une durée anormalement longue, il abandonne le protocole et oublie les étapes précédentes.

Propriétés de sécurité

— Lorsque B pense avoir reçu un secret provenant de A et qu'il a fini une exécution du protocole, il est certain que c'est A qui lui a envoyé le secret grâce à l'étape 3. Il n'y a que A et S qui peuvent avoir la connaissance de Nb dans les étapes précédentes.
— Lorsque A a envoyé un secret K à B et qu'il a terminé une exécution du protocole, il est certain que B a bien reçu K car A est le seul à pouvoir déchiffrer le message de l'étape 2 et B est le seul a pouvoir déchiffrer le message de l'étape 3. De plus, B prouve a A qu'il a bien connaissance du secret K en l'utilisant pour chiffrer ses messages dans l'étape 4.
— Le secret K n'est connu que de A, B et S. En effet, tous les échanges impliquant la communication de K sont chiffrés par des des éléments qui sont à la connaissance de A, B ou S.

Coût du protocole

— Étape 1 : $10 + 1 + 1 + 1 + 1 + 1 + 10 + 1 + 1 = 27$
— Étape 2 : $10 + 1 + 1 + 10 + 1 + 1 + 10 + 1 + 1 = 36$
— Étape 3 : $1 + 1 + 1 + 1 + 1 + 1 = 6$
— Étape 3 : $10 + 1 + 1 = 12$
— Total : $27 + 36 + 6 + 12 = 81$