Protocoles de Sécurité et Vérification
Description du Protocole

1 Description du protocole

Notre protocole à clé publique est décrit comme suit :

$$A \to B : \{N_a\}_{pub(B)}, \{K\}_{pub(B)}, A$$
$$B \to A : \{|\{|N_a|\}_{N_a}|\}_K, \{N_b\}_{pub(A)}, B$$
$$A \to B : H(N_b)$$

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. H est une fonction de hachage.

Valeurs générées

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

Description des étapes

1. L'agent A envoie un nombre aléatoire N_a chiffré avec la clé publique de B,la clé K chiffré avec la clé publique de B et son nom A.
2. B déchiffre l'entièreté du message de A. B communique avec A qui l'agent indiqué en 3e place dans le premier message. Il lui envoie le nonce N_a chiffré avec le nonce N_a et chiffré une deuxième fois avec la clé privée K qu'il possède entre lui et A, N_b chiffré avec la clé publique de A et son nom B.
3. A déchiffre les élements reçus par B. Il retient le nonce N_b et vérifie qu'il reçoit le bon nonce N_a si ce n'est pas le cas, il abandonne le protocole. Il envoie à B le N_b haché avec la fonction H.
4. B reçoit le message envoyé par A et vérifie qu'il reçoit le bon nonce N_b si ce n'est pas le cas, il abandonne le protocole.

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,
— Si N_a a une longueur de C, alors N_b à une longeur de 2C et K à une longeur de 3C. Si un agent reçoit un message avec un élément d'une longueur anormale, il abandonne le protocole,
— Les nonces et clés sont des valeurs aléatoires qui s'étendent sur plusieurs octets et donc qui ne peuvent pas être obtenues par force brute.

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 4. Il n'y a que A qui peut 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 2.
— Le secret K n'est connu que de A et B. En effet, tous les échanges impliquant la communication de K sont chiffrés par des des éléments qui sont à la connaissance de A ou B.

Coût du protocole

— Étape 1 : $1 + 1 + 1 + 1 + 1 + 1 + 1 = 7$
— Étape 2 : $10 + 10 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 17$
— Étape 3 : $20 + 0.5 * 1 = 20.5$
— Total : $7 + 16 + 12 = 54.5$