Protocoles de sécurité
Description du protocole des cotesdeporc
Moser Meven - Thébault Adrien - Trebon Landry

Description du protocole de l'équipe cotesdeporc

Le protocole de l'équipe cotesdeporc à clef publique se décrit de la façon suivante :

$$A \rightarrow B : \quad < A , \{ N_1 \}_{pub(B)} , \{ K \}_{pub(B)} , h(< A , K >) >$$
$$B \rightarrow A : \quad < \{ N_2 \}_{pub(A)} , h(< K, N_1 , N_2 >) >$$
$$A \rightarrow B : \quad N_2$$

Connaissances initiales : au début du protocole, on suppose que les agents *A* et *B* connaissent la clef publique pub(*C*) associée à l'agent *C*, pour tout agent *C*.

Valeurs générées au cours du protocole :
- N_1 est un nonce généré par *A*
- N_2 est un nonce généré par B

Description du protocole :

Au début du protocole, A envoie à B le quadruplet contenant son identité, un nonce N1 chiffré avec la clef publique de B, le secret K chiffré avec la clef publique de B et un hash de la paire contenant l'émetteur (A) et le secret K.

Lorsque B reçoit ce message, il déchiffre N1 et K et calcule le hash de la paire <A,K> puis le compare avec celui qu'il a reçu. Si cela correspond, il répond avec une paire contenant un nonce N2 chiffré avec la clef publique de A et le hash du triplet contenant le secret K, le nonce N1 reçu précédemment et le nonce N2 qu'il a généré.

A déchiffre ensuite N2, calcule le hash du triplet K, N1 (qu'il a conservé en mémoire), N2 et le compare avec celui reçu. Si les hash sont égaux, il renvoie le nonce N2 à B.

Lorsque B reçoit N2, il le compare avec celui qu'il a généré, s'ils sont égaux alors le protocole est terminé correctement.

Propriétés de sécurité :
- *Confidentialité* : la donnée *K* reste secrète entre *A* et *B*
- *Authentification* : à la fin du protocole, *B* est sûr que le secret *K* vient de *A*
- A la fin du protocole, *A* est sûr que *B* a bien reçu le secret *K*

Poids du protocole : 23
- Message 1 : 1 + (1 + 1) + (1 + 1) + (5 + 1 + 1) = 12
- Message 2 : (1 + 1) + (5 + 1 + 1 + 1) = 10
- Message 3 : 1