Challenge Protocole : Protocole TAZ V2

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 20, 2020

1 Principe

Connaissances initiales : Au début du protocole, on suppose que les agents A et B partagent chacun une clé symétrique avec le serveur (k_{AS} et k_{BS}), que l'on suppose complètement sûr. De plus, on suppose qu'ils connaissent leur clés publiques respectives.

Valeur générée au cours du protocole : Na est un nonce secret généré aléatoirement par A à chaque nouvelle communication qui permet de garantir l'authentification.
Nb est un nonce secret généré aléatoirement par B à chaque nouvelle communication qui permet de garantir l'authentification.

Hypothèse : On suppose que A,B sont capable de générer des nonces sûres (différents et impossibles à deviner) à chaque nouvelle communication.
On suppose également que les nonces ne sont valables que durant un temps limité si bien que tester de décrypté un message avec toutes les nonces disponibles à un instant T est réaliste pour B.

Description du protocole :

- A $\rightarrow B : \{\mathrm{N}_a\}_{pub(B)}$
  A envoie un nonce avec la clé publique de B.
- B $\rightarrow A : \{\{\mathrm{N}_b\}_{N_a}\}_{pub(A)}$, hash($N_a$)
  B renvoie un autre nonce chiffré symétriquement avec le nonce de A et chiffré avec la clé publique de A, le tout accompagné par le hash de A.
- A $\rightarrow B : hash(\mathrm{N}_b)$
  A revoit le hash du nonce de B.

Propriétés de sécurité :

- *Authentification* Lorsque Bob reçoit le message hash(N_b), il est sûr que celui-ci vient d'Alice si le hash est bon.

- *Authentification* Lorsque Alice reçoit le message $\{\{N_b\}_{N_a}\}_{pub(A)}$, hash$(N_a)$, elle est sûr que le nonce N_b vient de Bob si le hash est bon.
- *Confidentialité* Les deux agents Alice et Bob sont les seuls à partager le couple N_a/N_b.

2 Poids du protocole :

Le poids total du protocole est de 29 . Voici le détail :

- Règle 1 : 3
- Règle 2 : $14 + 6 = 20$
- Règle 3 : 6