Challenge Protocole : Protocole TAZ V4

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

November 2, 2020

1 Principe

Connaissances initiales : Au debut du protocole, on suppose que A et B connaissent leurs 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. De plus, les nonce et les agents étant de types différents, ils ne peuvent pas être confondus. Donc Na ne peut jamais être égal à A par exemple.

Description du protocole :

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

Propriétés de sécurité :

- *Authentification* Lorsque Bob reçoit le message $\{N_b\}_{pub(B)}$, il est sûr que celui-ci vient d'Alice si c'est bon.
- *Authentification* Lorsque Alice reçoit le message de B elle est sûr que le nonce N_b vient de Bob si c'est bien son identité qui est transmise.
- *Confidentialité* Les deux agents Alice et Bob sont les seuls à partager le nonce N_a si le protocole finit correctement.

2 Poids du protocole :

Le poids total du protocole est de 33. Voici le détail :

- Règle 1 : 4
- Règle 2 : $14 + 12 = 26$
- Règle 3 : 3