Challenge Protocole : Protocole TAZ V2

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 14, 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 : K est une clé symétrique secrète générée par A et partagée entre A et B.
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 que S ne communique jamais avec seulement A et B mais qu'il y a beaucoup de communication passant par S et pouvant utiliser ce protocole.
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.
Le serveur dispose d'une clé publique, clé privé S.

Description du protocole :

- A $\rightarrow S : \{Na\}_{pub(B)}$, $\{\text{B}\}_{k_{AS}}$
- S $\rightarrow B : \{Na\}_{pub(B)}$, $\{\text{A}\}_{k_{BS}}$
- B $\rightarrow S : \{Nb\}_{pub(A)}$, $\{\text{A}\}_{k_{BS}}$

- S $\rightarrow A : \{Nb\}_{pub(A)}$, $\{\mathrm{B}\}_{k_{AS}}$
- A $\rightarrow B : \{\{scrt\}_{Nb}\}_{Na}$,
- B $\rightarrow A : \{scrt\}_{pub(A)}$,

Propriétés de sécurité :

- *Authentification* Lorsque Bob reçoit le message scrt, il est sûr que celui-ci vient d'Alice.
- *Authentification* Lorsque Alice reçoit le message $\mathrm{scrt}_{pub(A)}$, il est sûr que celui-ci vient de Bob si c'est le bon "scrt".
- *Confidentialité* Les deux agents Alice et Bob sont les seuls à partager scrt.

2 Poids du protocole :

Le poids total du protocole est de 86 . Voici le détail :

- Règle 1 : $3 + 12 = 15$
- Règle 2 : 15
- Règle 3 : 15
- Règle 4 : 15
- Règle 5 : $10 + (10 + 1 + 1) + 1 = 23$
- Règle 7 : 3