Challenge Protocole : Protocole TAZ

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 7, 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 la clé publique pub (C) de tout agent C.

Valeur générée au cours du protocole : K est une clé symétrique secrète générée par le serveur et partagée entre A et B.
N est un nonce secret généré par A à chaque nouvelle communication qui permet de garantir l'authentification.

Hypothèse : On suppose que le serveur est capable de générer une clé symétrique d'une manière qui soit cryptographiquement sécurisée.
On suppose que A est capable de généré des nonce sûre (différent et impossible à deviner) à chaque nouvelle communication.

Description du protocole :

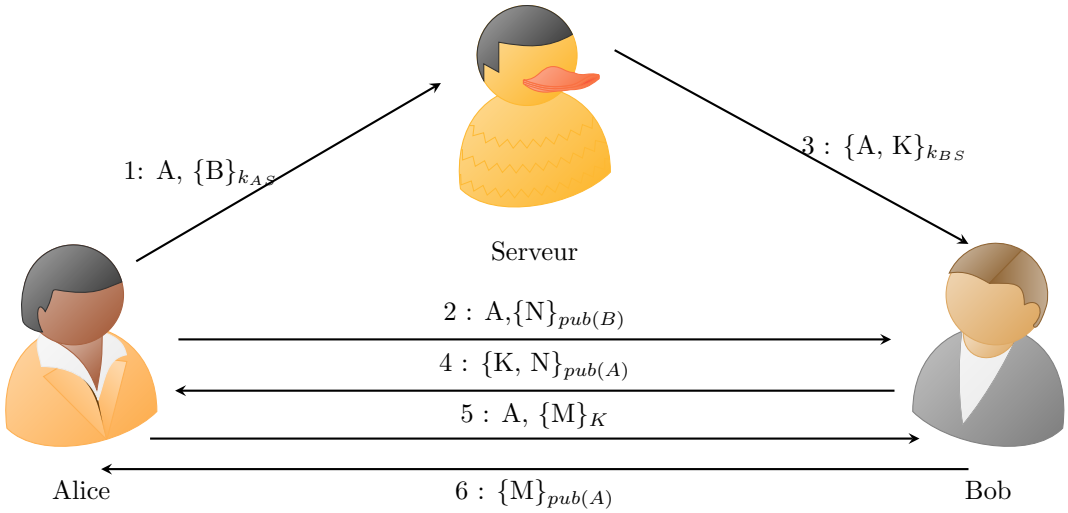
- A $\rightarrow S : A, \{B\}_{k_{AS}}$
  A envoie le destinataire B au serveur chiffré grâce à leur clé partagée k_{AS} ainsi que son identité.
  Le serveur génère aléatoirement la clé secrète symétrique K.
- A $\rightarrow B : A, \{N\}_{pub(B)}$
  A envoie son identité ainsi qu'un Nonce N généré aléatoirement et lié à cette communication à B. N est codé à l'aide de la clé publique de B.
- S $\rightarrow B : \{A, K\}_{k_{BS}}$
  Le serveur envoie la paire {K,A} à B
- B $\rightarrow A : \{K, N\}_{pub(A)}$
  B envoie la paire {K,N} à A crypté avec la clé publique de A
- A $\rightarrow B : A, \{M\}_K$
  A envoie M à B chiffré par K ainsi que son identité

- B $\rightarrow A : \{M\}_{pub(A)}$
  B renvoie M crypté avec la clé publique de A

Propriétés de sécurité :

- *Authentification* Lorsque Bob reçoit le message M (A, $\{M\}_K$), il est sûr que celui-ci vient d'Alice.
- *Confidentialité* Les deux agents Alice et Bob sont les seuls à partager la clé symétrique K (car le serveur est supposé sûr). Les deux agents Alice et Bob sont les seuls à partager le connaissance de N (car il est supposé être généré de manière sécurisé)

2 Schéma



3 Poids du protocole :

Le poids total du protocole est de 150. Voici le détail :

- Règle 1 : $1 + 10 + 1 + 1 = 13$
- Règle 2 : $1 + 1 + 1 + 1 = 4$
- Règle 3 : $10 + 50 + 1 + 1 + 1 = 63$
- Règle 4 : $1 + 50 + 1 + 1 + 1 = 54$
- Règle 5 : $1 + 10 + 1 + 1 = 13$
- Règle 6 : $1 + 1 + 1 = 3$