Description du protocole Azote de l'équipe Protoxyde

Chlebus, Flory, Heinfling

October 21, 2020

Le protocole Azote se décrit de la façon suivante:

$$A \rightarrow B : A, \{Na\}_{PubB}$$

$$B \rightarrow A : Hash(Na), \{Nb\}_{PubA}$$

$$A \rightarrow B : \{\{Secret\}_{Nb}\}_{Na}$$

$$B \rightarrow A : Hash\{Secret\}$$

Connaissances initiales:
A et B connaissent la clef publique de A et de B.

Valeurs générées au cours du protocole:
N_b est un nonce généré par B.
N_a est un nonce généré par A.

Description du protocole:

1. Dans un premier temps, A envoie à B "$A, \{Na\}_{PubB}$" qui contient son identité "A", puis un nonce chiffrée par la clef publique de B.

2. Ensuite, B envoie à A le hash qu'il a généré à partir du nonce qu'il a reçu ainsi qu'un nouveau nonce chiffrée par la clef publique de A.

3. A envoie alors son secret à B. Le secret est chiffré une première fois en utilisant le nonce généré par puis le tout est chiffré une seconde fois en utilisant le nonce généré par B.
   Avant de passer à l'étape suivant, B vérifie que le message qu'il a reçu de A fait du sens (après un premier déchiffrage puis un second).

4. Finalement, B renvoie le hash du secret à A. C'est à ce moment là que A peut savoir si il a bel et bien parlé avec B, et ce en comparant le hash reçu avec le hash du secret envoyé.

Propriétés de sécurité:
Ce protocole permet à deux utilisateurs de s'échanger une clé symétrique tout en s'assurant de l'identité des deux acteurs.

- *Confidentialité* Les deux agents Alice et Bob sont seuls à connaître le secret.

- *Authentification* La dernière ligne permet à A d'être sûr qu'il a parlé avec B.

- *Authentification* L'avant dernier ligne permet à B de savoir si le message qu'il reçoit fut bel et bien créé par A.

Poids du protocole: 42

- 1+(1+1+1)

- (5+1)+(1+1+1)

- (((1)+10+1)+10+1)

- 5+1