Description du protocole Azote de l'équipe Protoxyde

Chlebus, Flory, Heinfling

October 7, 2020

Le protocole Azote se décrit de la façon suivante:

$$A \rightarrow B : A, \{B, K_{ab}\}_{Kas}$$

$$B \rightarrow S : A, \{B, K_{ab}\}_{Kas}, \{N_b\}_{Kbs}$$

$$S \rightarrow B : \{K_{ab}\}_{Kbs}$$

$$S \rightarrow A : \{N_b\}_{Kas}$$

$$A \rightarrow B : \{N_b\}_{Kab}$$

Connaissances initiales:
Le serveur S détient au préalable une clef symétrique partagée avec A et une clef symétrique partagée avec B.

Valeurs générées au cours du protocole:
K_{ab} est une clef symétrique générée par A. N_b est un nonce généré par B.

Description du protocole:

1. Dans un premier temps, A envoie à B "$A, \{B, K_{ab}\}_{Kas}$" qui contient son identité "A", puis la paire constituée du destinataire "B" et de la clé symétrique K_{ab} générée par A, paire étant chiffrée par sa clé symétrique K_{as} connue du serveur et de A uniquement.

2. Ensuite, B envoie au serveur S le message reçu précédemment ("A,{B,$K_{ab}\}_{Kas}$"), ainsi qu'un nonce N_b chiffré avec sa propre clé symétrique K_{bs}. Le système peut donc déchiffrer le message grâce à la connaissance de K_{as} et de l'identité "A". Il récupère alors K_{ab} et l'identité "B" qui lui permet de déchiffrer le nonce N_b grâce à la connaissance de K_{bs}.

3. Le Serveur renvoie à B la clé "$\{K_{ab}\}$" chiffrée avec K_{bs}. Ainsi B peut déchiffrer le message et récupérer la clé K_{ab}.

4. Le Serveur envoie également à A le nonce N_b chiffré avec la clé symétrique de A K_{as}.

5. Enfin, A déchiffre le message, récupère le nonce N_b, et l'envoie à B en le chiffrant avec K_{ab}. B ayant connaissance de cette dernière clé depuis l'étape 3, il peut vérifier la valeur du nonce N_b.

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 la clé K_{ab}

- *Authentification* Lorsque Bob reçoit N_b, il est sûr que celui-ci vient d'alice.

Poids du protocole: 177

- 10+50+1+1+1+1

- 1+10+50+1+1+1+10+1+1

- 10+1+1

- 10+1+1

- 10+1+1