Description du protocole du groupe *Protocool*

Lucas THOMAS, Matthieu PHAM et Emmanuel PERRIN

7 Octobre 2020

Notre protocole d'échange de clé secrète se décrit de la façon suivante :

$$\begin{array}{ll} A \longrightarrow S : & A, B \\ S \longrightarrow A : & \{N\}^s_{ksa} \\ A \longrightarrow B : & \{N,\, K\}^a_{\mathrm{pub}(B)} \\ S \longrightarrow B : & \{A,\, N\}^s_{ksb} \\ B \longrightarrow A : & \{K\}^a_{\mathrm{pub}(A)} \end{array}$$

Connaissances initiales : Au début du protocole, on suppose que les agents A et B partagent deux clés : la clé publique $\mathrm{pub}(A)$ associée à A et $\mathrm{pub}(B)$ associée à B. Les agents A et B ont donc chacun également une clé privée associée : $\mathrm{prv}(A)$ et $\mathrm{prv}(B)$.
On suppose aussi que A et B partagent chacun une clé symétrique avec le serveur S respectivement ksa et ksb.
K est le message à envoyer (la clé secrète à échanger avec B).

Valeurs générées au cours du protocole : N est un nonce généré par S pour A.

Description du protocole : À la première étape du protocole, l'agent Alice envoie son nom A et le nom de l'agent Bob B au serveur S.
Le serveur envoie à A un nonce N chiffré par la clé symétrique ksa, c'est à dire que seul A peut déchiffrer N.
Alice envoie alors N et K à Bob en les chiffrant avec la clé publique de Bob : $\mathrm{pub}(B)$. Bob pourra déchiffrer avec sa clé privée $\mathrm{prv}(B)$.
Le serveur envoie à Bob A et N chiffrés avec la clé symétrique qu'ils partagent : ksb. Ainsi Bob, sait qu'il doit bien recevoir N de la part de A et peut vérifier que tout est conforme. Les deux étapes où B reçoit des informations peuvent être interchangées car B attend de recevoir les deux messages avant de vérifier.
Enfin, Bob, ayant reconnu N, répond à Alice K chiffré par $\mathrm{pub}(A)$. Cet échange remplit la fonction d'un acquittement.

Propriétés de sécurité :

- Si B a fini pensant avoir reçu une clé K venant de A, alors A a bien envoyé K à B
- Si A a fini en ayant envoyé une clé K à B, alors B a bien reçu K de la part de A.
- La clé K est secrète entre A et B.

Poids du protocole : 134

- Règle 1 : $1 + 1 = 2$
- Règle 2 : $10 + 1 + 1 = 12$
- Règle 3 : $50 + 1 + 1 + 1 + 1 = 54$
- Règle 4 : $50 + 10 + 1 + 1 + 1 = 63$
- Règle 5 : $1 + 1 + 1 = 3$