Championnat de protocoles

Description du protocole (1re correction)

NoSafetyAssociation (NSA)

Encadrante :
Véronique Cortier
veronique.cortier@loria.fr

Bastien Del-Valle
bastien.del-valle@telecomnancy.eu

Louis Jacotot
louis.jacotot@telecomnancy.eu

Bruno Gomes Dos Santos
bruno.gomes-dos-santos@telecomnancy.eu

2020 – 2021

Le protocole se décrit de la façon suivante :

1. A → S : A, $\{B\}_{Kas}$
2. S → B : S, $\{A, N\}_{Kbs}$
3. S → A : S, $\{N\}_{Kas}$
4. A → B : $\{N, K\}_{pub(B)}$
5. B → A : $\{K\}_{pub(A)}$

Connaissances initiales : Au début du protocole, on suppose que :
- L'agent A connaît la clef symétrique Kas ;
- L'agent B connaît la clef symétrique Kbs ;
- L'agent S connaît la clef symétrique Kas ;
- L'agent S connaît la clef symétrique Kbs ;
- L'agent A connaît la clef publique $pub(B)$;
- L'agent B connaît la clef publique $pub(A)$.

Valeurs générées au cours du protocole :
- N est un nonce généré par S ;
- K est un secret généré par A.

Description du protocole : À la première étape, A envoie au serveur S l'identité B de l'agent à contacter, en utilisant un chiffrement symétrique. Ce message est authentifié par le serveur S car A est le seul autre connaisseur de la clef Kas.

À la deuxième étape, le serveur S génère un nonce N et l'envoie à B avec l'identité A en utilisant un chiffrement symétrique. Ainsi, ce message est confidentiel et authentique car Kbs est connu par B et S uniquement.

À la troisième étape, le serveur S envoie le nonce N, à l'agent demandeur A, en utilisant un chiffrement symétrique. Ce message est confidentiel et authentique car Kas est connu par A et S uniquement.

À la quatrième étape, l'agent A génère et envoie à l'agent B un secret, en utilisant un chiffrement asymétrique. Ce message est donc confidentiel. L'agent B vérifie que le nonce envoyé par A correspond au nonce reçu par le serveur S.

À la dernière étape, B envoie la clef reçue à A en utilisant un chiffrement asymétrique. Ce message est donc confidentiel car seul A connaît $prv(A)$. L'agent A vérifie que la clef reçue correspond bien à la clef envoyée par S. Un acquittement valide ne peut pas être envoyé par un autre agent que B (également A ou S) car la clef K est uniquement connue par A, B et S.

Propriétés de sécurité : À la fin de l'échange :
- Si B a fini pensant avoir reçu une clef 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, B et S.

Poids du protocole : 147

1. $10 + 1 + 1 + 1 = 13$
2. $50 + 10 + 1 + 1 + 1 + 1 = 64$
3. $10 + 1 + 1 + 1 = 13$
4. $50 + 1 + 1 + 1 + 1 = 54$
5. $1 + 1 + 1 = 3$