

Championnat de protocoles

Description du protocole

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

Le protocole se décrit de la façon suivante :

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

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 B connaît la clef publique $pub(A)$.

Valeurs générées au cours du protocole : K est un secret généré par S .

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 une clef secrète K et l'envoie à A en utilisant un chiffrement symétrique. Ainsi, ce message est confidentiel et authentique car Kas est connu par A et S uniquement.

À la troisième étape, le serveur S envoie l'identité du demandeur A et la clef K , à l'agent à contacter B , en utilisant un chiffrement symétrique. Ce message est confidentiel et authentique car Kbs est connu par B et S uniquement.

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 : 90

1. $10 + 1 + 1 = 12$
2. $10 + 1 + 1 = 12$
3. $50 + 10 + 1 + 1 + 1 = 63$
4. $1 + 1 + 1 = 3$