Championnat de protocoles

Attaque sur le protocole de ATEAM

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

Pour rappel, le protocole se décrit de la façon suivante :

1. A $\rightarrow$ B : $\{A, Na\}_{pub(B)}$
2. B $\rightarrow$ A : $h(Na), \{Nb\}_{pub(A)}$
3. A $\rightarrow$ B : $h(Nb)$

L'attaque se décrit de la façon suivante :

1. A $\rightarrow$ C(B) : $\{A, Na\}_{pub(B)}$
2. C(A) $\rightarrow$ B : $\{A, Na\}_{pub(B)}$
3. B $\rightarrow$ C(A) : $h(Na), \{Nb\}_{pub(A)}$
4. C(B) $\rightarrow$ A : $h(Na), \{Kc\}_{pub(A)}$
5. A $\rightarrow$ C(B) : $h(Kc)$
6. C(A) $\rightarrow$ B : $h(Kc)$

Modèle : On suppose qu'un agent C peut intercepter et modifier les communications entre les agents A et B.

$$A \longleftrightarrow C \longleftrightarrow B$$

Description : L'attaque, de type « homme du milieu », consiste à modifier la donnée $\{Nb\}_{pub(A)}$ à l'étape 2. Le chiffrement à clef publique utilisé ne garantie pas l'authenticité du message. L'agent C génère un secret Kc et envoie à A la donnée $\{Kc\}_{pub(A)}$, car C a connaissance de la clef $pub(A)$.

Propriété de sécurité : À la fin de l'échange, l'agent B fini en rejetant l'échange car $h(Kc)$ est différent de $h(Nb)$. En revanche, A fini en pensant avoir reçu la clef Kc venant de B. En conséquence, **le protocole ne respecte pas la propriété de sécurité :** « si B (ici A) a fini pensant avoir reçu une clef K venant de A (ici B), alors A (ici B) a bien envoyé K à B (ici A) ».