Championnat de protocoles

Attaque sur le protocole de ATEAM v4

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

L'attaque se décrit de la façon suivante :

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

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 :
B n'a aucune confirmation que c'est A qui lui envoie les messages.

Propriété de sécurité : À la fin de l'échange, l'agent B fini en pensant parler à A alors qu'il parle à C.