Championnat de protocoles

Attaque sur le protocole de QGv2

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, $\{N_a\}_{pub(B)}$
2. B $\rightarrow$ A : $\{N_a\}_{pub(A)}$, $\{N_b\}_{pub(A)}$
3. A $\rightarrow$ B : $\{K\}_{\{N_b\}_{Na}}$
4. B $\rightarrow$ A : $\{K\}_{pub(A)}$

L'attaque se décrit de la façon suivante :

1. A $\rightarrow$ C(B) : A, $\{N_a\}_{pub_B}$
2. C $\rightarrow$ B : C, $\{N_a\}_{pub_B}$
3. B $\rightarrow$ C : $\{N_a\}_{pub(C)}$, $\{N_b\}_{pub_C}$
4. C(B) $\rightarrow$ A : $\{N_a\}_{pub(A)}$, $\{N_b\}_{pub_A}$
5. A $\rightarrow$ C(B) : $\{K\}_{\{N_b\}_{Na}}$
6. C $\rightarrow$ B : $\{K\}_{\{N_b\}_{Na}}$
7. B $\rightarrow$ C : $\{K\}_{pub(C)}$
8. C(B) $\rightarrow$ A : $\{K\}_{pub(A)}$

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 :
C se fait passer pour B à chaque communication avec A.

Propriété de sécurité : À la fin de l'échange, A croit dialoguer avec B alors qu'il dialogue avec C et C pourra lire les messages que A envoie à B.