Championnat de protocoles

Attaque sur le protocole de Azote

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, $\{B, K_{ab}\}_{k_{as}}$
2. B $\rightarrow$ S : A, $\{B, K_{ab}\}_{k_{as}}$, $\{N_b\}_{K_{bs}}$
3. S $\rightarrow$ B : $\{K_{ab}\}_{k_{bs}}$
4. S $\rightarrow$ A : $\{N_b\}_{K_{as}}$
5. A $\rightarrow$ B : $\{N_b\}_{K_{ab}}$

L'attaque se décrit de la façon suivante :

1. A $\rightarrow$ B : A, $\{B, K_{ab}\}_{k_{as}}$
2. B $\rightarrow$ C(S) : A, $\{B, K_{ab}\}_{k_{as}}$, $\{N_b\}_{K_{bs}}$
3. C(B) $\rightarrow$ S : C, $\{B, K_c\}_{k_{cs}}$, $\{N_b\}_{K_{bs}}$
4. S $\rightarrow$ B : $\{K_c\}_{K_{bs}}$
5. S $\rightarrow$ C : $\{N_b\}_{K_{cs}}$
6. C(B) $\rightarrow$ S : A, $\{B, K_{ab}\}_{k_{as}}$, $\{N_b\}_{K_{bs}}$
7. S $\rightarrow$ C(B) : $\{K_{ab}\}_{k_{bs}}$ - Bloqué
8. S $\rightarrow$ A : $\{N_b\}_{K_{as}}$
9. A $\rightarrow$ B : $\{N_b\}_{K_{ab}}$

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 : A l'étape 3, C remplace la clé K_{ab} par K_c. A l'étape 4, B pense recevoir la clé K_{ab} qui est la clé envoyée par A mais reçoit en fait K_c à la place. A l'étape 5, C connaît Nb qui devrait être caché.

Propriété de sécurité : À la fin de l'échange, C pourra lire pourra lire toutes les communications entre A et B tandis que ceux-ci ne pourront pas se lire entre eux car ils ont deux clés différentes.