Championnat de protocoles

Attaque sur le protocole de TAZ v2

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 $\rightarrow$ S : $\{Na\}_{pub(B)}$, $\{B\}_{k_{AS}}$
2. S $\rightarrow$ B : $\{Na\}_{pub(B)}$, $\{A\}_{k_{BS}}$
3. B $\rightarrow$ S : $\{Nb\}_{pub(A)}$, $\{A\}_{k_{BS}}$
4. S $\rightarrow$ A : $\{Nb\}_{pub(A)}$, $\{B\}_{k_{AS}}$
5. A $\rightarrow$ B : $\{S\}_{\{N_b\}_{Na}}$
6. B $\rightarrow$ A : $\{S\}_{pub(A)}$

L'attaque se décrit de la façon suivante :

1. A $\rightarrow$ C(S) : A, $\{Na\}_{pub(B)}$, $\{B\}_{k_{AS}}$ (Donc C connaît $\{B\}_{k_{AS}}$)
2. C $\rightarrow$ S : $\{Na\}_{pub(B)}$, $\{B\}_{k_{CS}}$
3. S $\rightarrow$ B : $\{Na\}_{pub(B)}$, $\{C\}_{k_{BS}}$
4. B $\rightarrow$ S : $\{Nb\}_{pub(C)}$, $\{C\}_{k_{BS}}$
5. S $\rightarrow$ C : $\{Nb\}_{pub(C)}$, $\{B\}_{k_{CS}}$
6. C(S) $\rightarrow$ A : $\{Nb\}_{pub(A)}$, $\{B\}_{k_{AS}}$ (On a eu Kas à l'item 1)
7. A $\rightarrow$ C(B) : $\{S\}_{\{N_b\}_{Na}}$
8. C(A) $\rightarrow$ B : $\{S\}_{\{N_b\}_{Na}}$
9. B $\rightarrow$ C : $\{S\}_{pub(C)}$ (la clé n'est plus secrète)
10. C(B) $\rightarrow$ A : $\{S\}_{pub(A)}$

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 : L'attaque, de type « homme du milieu mais pas trop quand même », consiste à faire croire à A qu'il dialogue avec B. B sait qu'il parle avec C mais il recevra les messages des A qu'on va pouvoir lire en clair grâce à lui. Et A va nous envoyer ses messages pour B :evilface:

Propriété de sécurité : À la fin de l'échange, l'agent C connaît la clé K partagée entre A et B et donc peut écouter les conversations.