

# Championnat de protocoles

---

## Attaque sur le protocole de TAZ v3

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

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

1.  $A \rightarrow B : \{N_a\}_{pub_B}$
2.  $B \rightarrow A : \{\{N_b\}_{N_a}\}_{pub_A}, h(N_a)$
3.  $B \rightarrow A : h(N_b)$

L'attaque se décrit de la façon suivante :

1.  $A \rightarrow B : \{N_a\}_{pub_B}$
2.  $B \rightarrow C(A) : \{\{N_b\}_{N_a}\}_{pub_A}, h(N_a)$  - Bloqué
3.  $C \rightarrow B : \{N_a\}_{pub_B}$
4.  $B \rightarrow C : \{\{N_{b1}\}_{N_a}\}_{pub_C}, h(N_a)$
5.  $C(B) \rightarrow A : \{\{N_{b1}\}_{N_a}\}_{pub_A}, h(N_a)$
6.  $A \rightarrow C(B) : hash(N_{b1})$
7.  $C \rightarrow B : hash(N_{b1})$

**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 :**

On commence d'abord une connexion entre  $A$  et  $B$  pour sauvegarder les messages intéressants  $\{N_a\}_{pub_B}$  et  $h(\{N_a\})$ . A l'étape 3,  $C$  initie une connexion avec  $B$  avec le nonce donné par  $A$ .

A l'étape 4,  $B$  envoie un nouveau nonce à  $C$ , ce qui est la suite logique du protocole.

A l'étape 5,  $C$  utilise les informations envoyées par  $B$  pour faire croire à  $A$  que la 1ere connexion continue normalement.

**Propriété de sécurité** : À la fin de l'échange,  $A$  pense parler à  $B$  alors qu'il parle à  $C$ .