Championnat de protocoles

Attaque sur le protocole de Azote 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, $\{N_a\}_{pub_B}$
2. B $\rightarrow$ A : $hash(N_a)$, $\{N_b\}_{pub_A}$
3. A $\rightarrow$ B : $\{K\}_{\{N_b\}_{Na}}$
4. B $\rightarrow$ A : $h(K)$

L'attaque se décrit de la façon suivante :

1. A $\rightarrow$ B : A, $\{N_a\}_{pub_B}$
2. B $\rightarrow$ C(A) : hash($\{N_a\}$), $\{N_b\}_{pub_A}$ - Bloqué
3. C $\rightarrow$ B : C, $\{N_a\}_{pub_B}$
4. B $\rightarrow$ C : hash($\{N_a\}$), $\{N_{b1}\}_{pub_C}$
5. C(B) $\rightarrow$ A : hash($\{N_a\}$), $\{N_{b1}\}_{pub_A}$
6. A $\rightarrow$ C(B) : $\{\{K\}_{N_b1\}_{Na}}$
7. C $\rightarrow$ B : $\{\{K\}_{N_b1\}_{Na}}$
8. B $\rightarrow$ C : $hash(K)$
9. C(B) $\rightarrow$ A : $hash(K)$

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 hash($\{N_a\}$). 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.