Championnat de protocoles

Attaque sur le protocole de Protocool 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 : A,B
2. S $\rightarrow$ A : $\{N\}_{Ksa}$
3. S $\rightarrow$ B : $\{N, A\}_{Ksb}$
4. A $\rightarrow$ B : $\{N, K\}_{Ksb}$
5. B $\rightarrow$ A : $\{N\}_{pub(A)}$

L'attaque se décrit de la façon suivante :

Étape 1 :

1. A $\rightarrow$ C(S) : A,B
2. C(A) $\rightarrow$ S : A,C
3. C $\rightarrow$ S : C,B

Étape 2 :

1. S $\rightarrow$ A : $\{N\}_{Ksa}$
2. S $\rightarrow$ C : $\{Nc\}_{Ksc}$

Étape 3 :

1. S $\rightarrow$ C : $\{N, A\}_{Ksc}$
2. S $\rightarrow$ B : $\{Nc, C\}_{Ksb}$

Étape 4 :

1. A $\rightarrow$ B : $\{N, K\}_{Ksb}$

Étape 5 :

1. C(B) $\rightarrow$ A : $\{N\}_{pub(A)}$

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 consiste à se faire passer pour B pour A et pour A à B. Comme A pense pense que N est le nonce de B et que C y a accès C peut faire croire à A que le protocole c'est bien déroulé. Mais en réalité B va refuser la clé K, car pour lui le nonce est Nc et pas N !

Propriété de sécurité : À la fin de l'échange, A pense que la clé a été envoyé à B et valide cette clé, alors que B ne la valide pas. C'est à dire la propriété : Si A a fini en ayant envoyé une clé K à B alors B a bien reçu K de la part de A