Championnat de protocole - Équipe REX attaque l'équipe Protocool

October 22, 2020

1 Principe de l'attaque

Dans un premier temps l'attaquant C va intercepter tous les messages provenant de A. Au début de l'étape 2, C se fait passer pour A aux yeux de B. Il possède déjà la clé secrète entre A et B. Ensuite, B répond à A, C intercepte et renvoie juste le message en tant que C. A répond à C, ce dernier peut lire le nonce s'il veut, et renvoyer ce message en tant que A à B. B répondra à A normalement, encore une fois intercepté par C pour qu'il le renvoie en tant que lui même.
Le protocole se termine normalement pour A et B, et C connaît la clé K. B pense parler à A mais il parle à C. Cela ne respecte pas la propriété que la clé doit rester secrète entre A et B.

2 L'attaque

1 : $A \rightarrow C : \{A, K\}_{pub(C)}$
2 : $C(A) \rightarrow B : \{A, K\}_{pub(B)}$
3 : $B \rightarrow A : \{\{N\}_h(\{K\}_p ub(A))\}_p ub(A)(intercepté par C)$
4 : $C \rightarrow A : \{\{N\}_h(\{K\}_p ub(A))\}_p ub(A)$
5 : $A \rightarrow C : \{N\}_K$ (intercepté par C)
6 : $C(A) \rightarrow B : \{N\}_K$
7 : $B \rightarrow A : \{K\}_p ub(A)$ (intercepté par C)
8 : $C \rightarrow A : \{K\}_p ub(A)$