Championnat de protocole - Équipe REX attaque l'équipe TAZ

October 10, 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 1, C va bloquer le premier message de A et envoyer sa propre demande de connexion avec B au serveur S. Durant l'étape 3 et 4, C intercepte le message de A et modifie le premier élément en C et ne modifie pas le deuxième, le nonce chiffré avec la clé publique de B. Pendant l'étape 5, le serveur envoie la demande de connexion à B. B pensant dialoguer avec C renvoie donc à C la clé K et le nonce de A chiffré cette fois-ci avec la clé publique de C. C envoie ensuite le même message à A. Celui-ci reconnaît son nonce et envoie donc son message codé à B. C l'intercepte et peut le déchiffrer car il connaît aussi la clé K.
Le protocole se termine normalement pour A et C connaît la clé K ainsi que le message M. Cela ne respecte pas la propriété que la clé doit rester secret entre A et B.

2 L'attaque

1 : $A \rightarrow C(S) : A, \{B\}_{K_{as}}$
2 : $C \rightarrow S : C, \{B\}_{K_{cs}}$
3 : $A \rightarrow C(B) : A, \{N\}_{pub(B)}$
4 : $C \rightarrow B : C, \{N\}_{pub(B)}$
5 : $S \rightarrow B : \{C, K\}_{K_{bs}}$
6 : $B \rightarrow C : \{K, N\}_{pub(C)}$
7 : $C(B) \rightarrow A : \{K, N\}_{pub(A)}$
8 : $A \rightarrow C(B) : A, \{M\}_{K}$
9 : $C \rightarrow B : C, \{M\}_{K}$
10 : $B \rightarrow C : \{M\}_{pub(C)}$
11 : $C(B) \rightarrow A : \{M\}_{pub(A)}$