Championnat de protocole - Équipe REX attaque l'équipe Azote

October 21, 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 va bloquer le premier message de A et envoyer le même message à B, mais avec son nom, C. B va répondre à C avec le message normal, chiffré avec la clé publique de C. C va déchiffrer, récupérer Nb, et transmettre avec cette fois la clé publique de A, se faisant passer pour B. A va répondre à B, message encore intercepté, puis transmettre le message à B en tant que lui même (C). B va répondre à C avec le secret chiffré par pub(C), que peut lire C, et donc récupérer le secret. C transmet alors ce secret chiffré avec pub(A).
Le protocole se termine normalement pour A et B, et C connaît la clé scrt. Cela ne respecte pas la propriété que la clé doit rester secrète entre A et B.

2 L'attaque

1 : $A \rightarrow B : A, \{Na\}_{pub(B)}$ (intercepté par C)
2 : $C \rightarrow B : C, \{Na\}_{pub(B)}$
3 : $B \rightarrow C : hash(Na), \{Nb\}_{pub(C)}$
4 : $C(B) \rightarrow A : hash(Na), \{Nb\}_{pub(A)}$
5 : $A \rightarrow B : \{scrt\}_{\{Nb\}_{Na}}$ (intercepté par C)
6 : $C \rightarrow B : \{scrt\}_{\{Nb\}_{Na}}$
7 : $B \rightarrow C : \{scrt\}_{pub(C)}$ (récupération du secret)
8 : $C(B) \rightarrow A : \{scrt\}_{pub(A)}$