

Championnat de protocole - Équipe REX attaque l'équipe QG

October 19, 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 Na et Nb, et transmettre avec cette fois la clé publique de A, se faisant passer pour B. A va répondre à B, message encore intercepté, avec le secret chiffré par Na et Nb, que connaît C. C va donc récupérer le secret, puis transmettre le message à B. La suite se passe normalement, mis à part le fait que C doit rechiffrer le secret avec la clé publique de A.

Le protocole se termine normalement pour A et B, et C connaît la clé scrt. A pense parler à B, ce qui n'est pas le cas. 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 : $B \rightarrow C : \{Na\}_{pub(C)}, \{Nb\}_{pub(C)}$
- 4 : $C(B) \rightarrow A : \{Na\}_{pub(A)}, \{Nb\}_{pub(A)}$
- 5 : $A \rightarrow B : \{scrt\}_{\{Nb\}_{Na}}$ (intercepté par C et déchiffré)
- 6 : $C \rightarrow B : \{scrt\}_{\{Nb\}_{Na}}$
- 7 : $B \rightarrow C : \{scrt\}_{pub(C)}$
- 8 : $C(B) \rightarrow A : \{scrt\}_{pub(A)}$