Challenge Protocole : Attaque sur le protocole REX

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 9, 2020

1 Principe

Le principe de l'attaque est celui du Man In The Middle. Dans cette attaque A pense communiquer avec C tandis que B pense communiquer avec A.

2 Description de l'attaque :

- A $\rightarrow C : \{A,\mathrm{K}_{a_b}\}_{pub(c)}$
  Initialisation normale entre A et C.
- C $\rightarrow B : \{A,\mathrm{K}_{a_b}\}_{pub(b)}$
  C envoie le même message codé avec la clé publique de B.
- B $\rightarrow A : B, \{h(K_{a_b}), \mathrm{N}_b\}_{pub(A)}$
  B tente d'envoyer le message prévu pour A mais celui-ci est intercepté par C.
- C $\rightarrow A : C, \{h(K_{a_b}), \mathrm{N}_b\}_{pub(A)}$
  C envoie une copie du message précédent en remplaçant l'identité de B par la sienne.
- A $\rightarrow C : \{N_b,\mathrm{K}\}_{K a_b}$
  A suit la procédure normal en envoyant son message à C.
- C $\rightarrow B : \{N_b,\mathrm{K'}\}_{K a_b}$
  C finit la procédure avec B.

3 Conclusion :

Le protocole se termine normalement. Cependant, C connaît le secret K et B ne le connaît pas.