Challenge Protocole : Attaque sur le protocole QG V2

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 19, 2020

1 Principe

Le principe de l'attaque est celui du Man In The Middle : C peut se faire passer pour B.

2 Description de l'attaque :

L'attaque se décrit comme suit :

- C(A) $\rightarrow B : C, \{\mathrm{N}_a\}_{pub(B)}$
  A initie une communication avec B mais C change l'identité de A par la sienne.
- B $\rightarrow C : \{\mathrm{N}_a\}_{pub(C)}, \{N_b\}_{pub(C)}$
  C récupère donc le nonce de A par B.
- C(B) $\rightarrow A : \{\mathrm{N}_a\}_{pub(A)}, \{N_b\}_{pub(A)}$
  C usurpe l'identité de B.
- A $\rightarrow C(B) : \{scrt\}_{\{Nb\}_{\{Na\}}}$
  A suit le protocole et C intercepte le message qu'il peut décrypter.
- C(B) $\rightarrow A : \{\mathrm{scrt}\}_{pub(A)}$
  C finit la communication en usurpant le rôle de B.

3 Conclusion :

La communication se termine normalement du côté de A. Toutefois, A communique en réalité avec C et non avec B. C peut même finir la communication avec B en lui donnant ce qu'il veut comme clé comme ça B finit normalement aussi.