Challenge Protocole : Attaque sur le protocole AZOTE v2

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 15, 2020

1 Principe

Le principe de l'attaque est l'attaque de la propriété suivante : Si A a finit en ayant envoyé une clé K à B, alors B a bien reçu K de la part de A.

2 Description de l'attaque :

L'attaque se décrit comme suit :

- A $\rightarrow C(B) : A, \{B,\mathrm{K}_{a_b}\}_{K a_s}$
  A initie le protocole mais C intercepte le premier message.
- C $\rightarrow B : A, \{C,\mathrm{K}\}_{K c_s}$
  C initie une communication en se faisant passer pour A.
- B $\rightarrow C(S) : A, \{C,\mathrm{K}\}_{K c_s}$,$\{\mathrm{A},N_b\}_{K b_s}$
  B envoie un message au serveur mais C l'intercepte.
- C $\rightarrow S : A, \{B,\mathrm{K}_{a_b}\}_{K a_s}$,$\{\mathrm{A},N_b\}_{K b_s}$
  C envoie le "bon message" au serveur.
- S $\rightarrow C(B) : \{\mathrm{K}_{ab}\}_{K b_s}$ Le serveur envoie un message qui est intercepté par C.
- S $\rightarrow A : \{\mathrm{N}_b\}_{K a_s}$
  Le serveur suit le protocole.
- A $\rightarrow B : \{\mathrm{N}_b\}_{K a_b}$
  C intercepte le message.

3 Conclusion :

A initie une communication avec B et A et S ont finit normalement. Toutefois, B n'a jamais été informé de cette communication donc la propriété décrite précédemment n'est pas respectée.