Challenge Protocole : Attaque sur le protocole AZOTE

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 11, 2020

1 Principe

Le principe de l'attaque est que C peut se faire passer pour A.

2 Description de l'attaque :

- C $\rightarrow B : A, \{B,\mathrm{K}\}_{Kcs}$
  C initie une communication avec B en se faisant passer pour A.
- C(B) $\rightarrow S : C, \{B,\mathrm{K}\}_{Kc_s}, \{N_b\}_{Kbs}$
  B suit le protocole et C modifie l'identité de A par la sienne avant l'arrivée au serveur.
- S $\rightarrow B : \{\mathrm{K}\}_{Kbs}$
  Le serveur envoie la clé à B.
- S $\rightarrow C : \{\mathrm{N}_b\}_{Kcs}$
  Le serveur envoie le nonce de B à C.
- C $\rightarrow B : \{\mathrm{N}_b\}_K$
  C envoie à B son nonce codé avec K.

3 Conclusion :

Le protocole se termine normalement du côté de C, B et S toutefois B pense communiquer avec A alors qu'il communique en réalité avec C.