Challenge Protocole : Attaque sur le protocole A-Team v3

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 21, 2020

1 Principe

Le principe de l'attaque est de faire passer pour A auprès de B en jouant sur la confusion entre Nonce et Identité.

2 Description de l'attaque :

- C(A) $\rightarrow B : \{A,\text{A}\}_{pub(B)}$
  C envoie à B une initiation de communication en se faisant passé pour A.
- B $\rightarrow C(A) : \{B\}_{N_b},\{\text{A}\}_{N_b}, \{\text{Nb}\}_{pub(A)}$
  B suit le protocole mais ce faisant il permet à l'attaquant de faire l'acquittement en dernière étape.
- C(A) $\rightarrow B : \{A\}_{N_b}$
  C envoie l'acquittement à B.

3 Conclusion :

B finit le protocole en ayant pensé avoir parlé à A alors que ce n'est pas le cas.