Challenge Protocole : Attaque sur le protocole AZOTE

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 21, 2020

1 Principe

Le principe de l'attaque est de ce faire passé pour A.

2 Description de l'attaque V4:

L'attaque se décrit comme suit :

- A $\rightarrow C : A, \{\text{Na}\}_{pub(C)}$
  A initie une communication avec C
- C(A) $\rightarrow B : A, \{\text{Na}\}_{pub(B)}$
  C se fait passer pour A auprès de B en réutilisant le Na de A.
- B $\rightarrow A : Hash(\text{Na}), \{\text{Nb}\}_{pub(A)}$
  B répond normalement à A en suivant le protocole.
- A $\rightarrow C : \{secret\}_{Nb_{Na}}$
- C(A) $\rightarrow B : \{secret\}_{Nb_{Na}}$
  A envoie à C le secret en suivant le protocole et C l'envoie à B.

- B $\rightarrow A : Hash(secret)$
  B suit le protocole et A pense que cette réponse vient de C.

3 Description de l'attaque V3:

L'attaque se décrit comme suit :

- A $\rightarrow C : A, \{\text{Na}\}_{pub(C)}$
  A initie une communication avec C

- C(A) $\rightarrow B : A, \{\text{Na}\}_{pub(B)}$
  C se fait passer pour A auprès de B en réutilisant le Na de A.
- B $\rightarrow A : Hash(\text{Na}), \{\text{Nb}\}_{pub(A)}$
  B répond normalement à A.
- A $\rightarrow C : \{secret\}_{Nb_{Na}}$
- C(A) $\rightarrow B : \{secret\}_{Nb_{Na}}$
  A envoie à C le secret en suivant le protocole et C l'envoie à B.
- B $\rightarrow A : \{secret\}_{pub(A)}$
  B renvoie normalement le secret à A.

4 Conclusion :

A initie une communication avec C et C commence une communication avec B en parallèle en se faisant passer pour A. A la fin A croit parler a C et B à A, ce qui est en contradiction avec les propriété de sécurité du championnat.