Challenge Protocole : Attaque sur le protocole A-TEAM V4

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

November 3, 2020

1 Principe

Le principe de l'attaque est que si A initie une communication avec C alors C peut se faire passer pour A auprès de B.

2 Description de l'attaque :

L'attaque se décrit comme suit :

- A $\rightarrow C$: $\{\text{A,N}_a\}_{pub(C)}$
  A initie une communication avec C.
- C(A) $\rightarrow B$: $\{\text{A,N}_a\}_{pub(B)}$
  C se fait passer pour A auprès de B en réutilisant le même nonce.
- B $\rightarrow A$: $\{\{\text{N}_b\}_{N_a}\}_{pub(A)}$
  B répond normalement à A.
- A $\rightarrow C$: $hash(\text{N}_b)$
- C(A) $\rightarrow B$: $hash(\text{N}_b)$
  A envoie à C le nonce en suivant le protocole et C l'envoie à B.

3 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.