Challenge Protocole : Attaque sur le protocole Protocool

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 22, 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 $\rightarrow C : \{\text{A,K}\}_{pub(C)}$
  A initie une communication avec C.
- C(A) $\rightarrow B : \{\text{A,K}\}_{pub(B)}$
  C se fait passer pour A auprès de B en réutilisant la même clé.
- B $\rightarrow A : \{\{N\}_{h(K_{pub(A)})}\}_{pub(A)}$
  B répond normalement à A.
- A $\rightarrow C : \{N\}_K$
- C(A) $\rightarrow B : \{N\}_K$ A envoie à C le nonce en suivant le protocole et C l'envoie à B.
- B $\rightarrow A : \{K\}_{pub(A)}$
  B répond à A.

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.