Challenge Protocole : Attaque sur le protocole Proto-chorale

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 15, 2020

1 Principe

C peut usurper l'identité de B.

2 Description de l'attaque :

2.1 Première phase : communication entre A et C

La première phase se déroule normalement et à la fin de la communication, A et C partage une clé K'. Lors de ce premier échange C enregistre le message suivant $\{\mathrm{C}\}_{Ka_s}$.

2.2 Deuxième phase : communication entre A et B

- C(A) $\rightarrow S : A, \{C\}_{Ka_s}$
  A initie une communication mais C remplace le destinataire avec les données obtenues en première étape.
- S $\rightarrow A : \{A\}_{Ka_s}$
  S suit le protocole.
- A $\rightarrow S : A, \{K\}_{Ka_s}$
  A suit le protocole.
- S $\rightarrow C : \{K, A\}_{Kc_s}$
  S suit le protocole.
- A $\rightarrow C(B) : \{A\}_{pub(b)}$
  A suit le protocole mais C intercepte le message.
- C $\rightarrow B : \{B\}_{pub(a)}$
  C envoie l'acquittement.

- A $\rightarrow C(B) : \{h(K)\}_{pub(b)}$
  A suit le protocole mais C intercepte le message.
- C $\rightarrow A : \{B\}_K$
  C envoie l'identité de B.
- A $\rightarrow C(B) : \{A\}_K$
  A termine normalement le protocole.

3 Conclusion :

Le protocole se termine normalement du côté de A, S et C. Toutefois, A communique en réalité avec C.