Challenge Protocole : Attaque sur le protocole Proto-chorale

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 11, 2020

1 Principe

Si A commence par initier une communication avec un utilisateur malveillant C, C pourra se faire passer pour A lors d'une communication future entre A et 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 échanges les messages suivants vont être récupérés par C :

- $\{\text{A}\}_{Ka_s}$
- $\{\text{K'}\}_{Ka_s}$

2.2 Deuxième phase : communication entre A et B

- A $\rightarrow S : \{B\}_{Ka_s}$
  A envoie B au serveur via leur clé symétrique partagé.
- S $\rightarrow A : \{S\}_{Ka_s}$
  Le serveur envoie l'accusé de réception.
- C(A) $\rightarrow S : \{K'\}_{Ka_s}$
  A suit le protocole mais C remplace la clé K par l'ancienne clé K'.
- S $\rightarrow B : \{K', A\}_{Kb_s}$
  S suit le protocole.

- A $\rightarrow B : \{A\}_{pub(b)}$
  A suit le protocole.
- B $\rightarrow A : \{B\}_{pub(a)}$
  B suit le protocole.
- C(A) $\rightarrow B : \{hash(K')\}_{pub(b)}$
  C intercepte le message de A et envoie le hash de l'ancienne clé.
- B $\rightarrow A : \{B\}'_K$
  B suit le protocole.

3 Conclusion :

Le protocole se termine normalement du côté de S, B toutefois si B initie une communication avec A, C pourra la lire.