Challenge Protocole : Attaque sur le protocole NSA v2

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 15, 2020

1 Principe

Le principe de l'attaque est que si A communique avec deux personnes dont un utilisateur malveillant, le protocole n'est alors plus sûr car C peut se faire passer pour A.

2 Description de l'attaque :

- A $\rightarrow S : A, \{C\}_{Ka_s}$
  A envoie C au serveur via leur clé symétrique partagé.
- S $\rightarrow C : S, \{A, N\}_{Kc_s}$
  S suit le protocole.
- C $\rightarrow S : A, \{B\}_{Ka_s}$
  C envoie au serveur une initialisation de communication récupérée d'un échange précédent entre A et B.
- S $\rightarrow B : S, \{A, N'\}_{Kb_s}$
  Le serveur suit la procédure.
- S $\rightarrow A : S, \{N'\}_{Ka_s}$
  Le serveur suit le protocole mais C modifie les entêtes pour que A pense qu'il s'agit du message relié à sa communication avec C, l'autre message ayant été bloqué par C.
- A $\rightarrow C : \{N', K\}_{pub(c)}$
  A suit la procédure et C apprend ainsi N'.
- C $\rightarrow B : \{N', K'\}_{pub(b)}$
  C envoie l'acquittement de "A".

3 Conclusion :

Le protocole se termine normalement du côté de A, B et S toutefois C partage une clé avec B qui pense la partager avec A.