Challenge Protocole : Attaque sur le protocole ~~REX~~ NSA

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 10, 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 rien n'indique l'identité des expéditeurs dans le protocole à part les entêtes.

2 Description de l'attaque :

- A $\rightarrow S : \{B\}_{K a_s}$
  A envoie B au serveur via leur clé symétrique partagé.
- A $\rightarrow S : \{C\}_{K a_s}$
  A envoie C au serveur via leur clé symétrique partagé.
- S $\rightarrow A : \{\mathrm{K}_{a_b}\}_{K a_s}$
  Le serveur renvoie la clé partagé avec B à A mais C modifie les entêtes pour que A croit qu'il s'agit de K_{a_c}.
- S $\rightarrow A : \{\mathrm{K}_{a_c}\}_{K a_s}$
  Le serveur renvoie la clé partagé avec C à A mais C modifie les entêtes pour que A croit qu'il s'agit de K_{a_b}.
- S $\rightarrow B : \{A,\mathrm{K}_{a_b}\}_{K b_s}$
  Le troisième étape se déroule normalement pour B et le serveur.
- S $\rightarrow C : \{C,\mathrm{K}_{a_c}\}_{K c_s}$
  Le troisième étape se déroule normalement pour C et le serveur.
- B $\rightarrow A : \{\mathrm{K}_{a_b}\}_p ub(A)$ B termine le protocole normalement mais C modifie les entêtes pour que A croit qu'il s'agit de K_{a_c}.
- C $\rightarrow A : \{\mathrm{K}_{a_c}\}_p ub(A)$ C termine le protocole normalement mais il modifie les entêtes pour que A croit qu'il s'agit de K_{a_b}.

3 Conclusion :

Le protocole se termine normalement du côté de A, C, B et S toutefois C pourra lire toutes les communications entre A et B tandis que B en sera incapable.