Challenge Protocole : Attaque sur le protocole PROTOCOOL

Thomas FRAULOB
Alice MICARD
Zoé STAUDER

October 12, 2020

1 Principe

Si A effectue deux communication en parallèle, l'une avec B et l'autre avec un utilisateur C malveillant, alors C peut prendre la place de A du point de vu de B.

2 Description de l'attaque :

On considère que le protocole s'est déroulé normalement jusqu'à l'étape 2 incluse à partie de l'étape, l'attaque se décrit comme suit :

- A $\rightarrow S : A, B$
  A initie la communication avec B.
  $A \rightarrow S$:A,C
  A initie la communication avec C.

- S $\rightarrow A : \{\mathrm{N}_b\}_{Kas}$
  Le serveur envoie le nonce lié à la communication avec B à A

- S $\rightarrow A : \{\mathrm{N}_c\}_{Kas}$
  Le serveur envoie le nonce lié à la communication avec C à A

- C inverse les en-têtes si bien que A inverse N_c et N_b, à partir de ce moment C ne suit plus la protocole normale et ne va plus répondre à A.

- A $\rightarrow C : \{\mathrm{N}_b, K,\}pub(C)$
  A suit la procédure standard mais ce faisant il donne à C accès à la valeur N_b. C va à ce moment isoler A du réseau de manière à ce qu'il ne puisse pas avertir B si il détecte l'attaque.

- C(A) $\rightarrow B : \{\mathrm{N}_b, K', \}pub(B)$
  C envoie à B le nonce qui authentifie la communication entre A et B ainsi qu'une clé de son choix

- S $\rightarrow B : \{$A ,$\mathrm{N}_b, \}K_{sb}$
  Le serveur suit la procédure standard et transmet le nonce lié à la communication entre A et B

- B $\rightarrow C(A) : \{$K'$\}$pub(A)
  B suit la procédure standard mais C intercepte tous les messages à destination de A.

3 Conclusion :

Le protocole se termine normalement du côté de B qui pense que seul lui est A connaisse la clé. Malheureusement, seul C et B connaissent la clé.