Les protocoles Cryptographiques

Mounira Msahli

February 9, 2024

Exercice 1:

On considère le protocole suivant:

1. $A \rightarrow B : \{<A, N_A>\}_{pk(B)}$
2. $B \rightarrow A : \{<N_A, N_B>\}_{pk(A)}$
3. $A \rightarrow B : \{N_B\}_{pk(B)}$

1. Donner la description des roles du protocole

Solution :

Il y a deux roles: R_1 (the initiator) et R_2 (the responder).

$R_1(A, B, N_A) = (init \rightarrow \{< A, N_A >\}_{pk(B)}$

$(\{< N_A, N_B >\}_{pk(A)} \rightarrow \{N_B\}_{pk(B)})$

$R_2(B, N_B) = (\{< A, N_A >\}_{pk(B)} \rightarrow \{< N_A, N_B >\}_{pk(X_A)})$

$(\{N_B\}_{pk(B)} \rightarrow stop)$

Exercice 2:

On considere le protocole suivant appelé FFFGGG:

1. $A \rightarrow B : A$
2. $B \rightarrow A : B, N, M, O$
3. $A \rightarrow B : A, \{N, M, O, S\}_{pk(B)}$

4. $B \rightarrow A : N, M, \{M, O, S, N\}_{pk(B)}$

1. Donner la description des roles du protocole
2. Donner l'attaque possible (en se basant sur le 3 parallel sessions) permettant de montrer que S n'est pas sécurisé

Solution :

1. Role description

$RA = ((init, B \rightarrow A),$

$(A, N, M, O \rightarrow A, \{N, M, O, S\}_{pk_B}),$

$(N, M, \{M, O, S, N\}_{pk_B} \rightarrow stop))$

$RB = ((A \rightarrow B, N, M, O),$

$(A, \{N, X, Y, S\}_{pk_B} \rightarrow \{X, Y, S, N\}_{pk_B}))$

2. Parallel Attack

1.1 $A \rightarrow B : A$

2.1 $A \rightarrow B : A$

3.1 $A \rightarrow B : A$

1.2 $B \rightarrow I(A) : B, N_1, M_1, O_1$

2.2 $B \rightarrow I(A) : B, N_2, M_2, O_2$

3.2 $B \rightarrow I(A) : B, N_3, M_3, O_3$

1.2 $I(B) \rightarrow A : B, N_1, N_2, N_3$

1.3 $A \rightarrow B : A, \{N_1, N_2, N_3, S\}_{Pk_B}$

1.4 $B \rightarrow A : N_1, N_2, \{N_2, N_3, S, N_1\}_{Pk_B}$

2.3 $I(A) \rightarrow B : A, \{N2, N3, S, N1\}_{Pk_B}$

2.4 , $B \rightarrow A : N_2, N_3, \{N_3, S, N_1, N_2\}_{Pk_B}$

3.3 $I(A) \rightarrow B : A, \{N_3, S, N_1, N_2\}_{Pk_B}$

3.4$B \rightarrow A : N_3, S, \{S, N_1, N_2, N_3\}_{Pk_B}$

Exercice 3:

On considère le protocole suivant:

1. $A \rightarrow B : <A, N_A>$
2. $B \rightarrow A : \{<N_A, N_B>\}_{K_{ab}}$
3. $A \rightarrow B : N_B$
4. $B \rightarrow A : \{<K, N_B>\}_{K_{ab}}$
5. $A \rightarrow B : \{s\}_K$

Pour cette partie, on suppose que l'attaquant connait les identités de A et B.

1. Donner la description des roles du protocole
2. Décrire les actions des participants dans ce protocole: comment chaque participant verifie les messages reçus et comment il construit les messages émis.
3. Il y a une attaque permettant de connaitre s, pouvez vous la décrire ?
4. Donner plus de détails sur cette attaque et comment on peut la corriger.

Solution :

3. L'attaque consiste à envoyer le 2 eme message $\{<NA, NB>\}_{K_{ab}}$ à la place du 4 eme message $\{<K, NB>\}_{K_{ab}}$. Donc A répondra avec $\{s\}_{N_A}$ puisque l'attaquant connait N_A donc peut lire s. Le dernier message n'est pas re-envoyé à B.

4. On peut ajouter l'identité de de B dans le message 2