

Etude de protocoles d'authentification

Protocole 1

Dans le protocole suivant, on dénote par K_A et K_B les clés de session symétriques générées respectivement par Alice et Bob et par PK_S la clé publique de chiffrement du serveur d'authentification. De plus l'opérateur \oplus dénote le ou-exclusif bit à bit entre deux chaînes de bits. On suppose qu'Alice est celle qui initie le protocole.

1. $A \rightarrow S : B, \{K_A\}_{PK_S}$
2. $S \rightarrow B : A$
3. $B \rightarrow S : A, \{K_B\}_{PK_S}$
4. $S \rightarrow A : B, K_A \oplus K_B$

Questions :

- Traduisez le protocole tel qu'il est écrit en notation de protocole de sécurité dans des phrases en langue naturelle expliquant son déroulement.
- Est ce que ce protocole permet une authentification mutuelle entre A et B ? Quelque soit votre réponse prenez le temps de l'argumenter.
- Décrivez une attaque permettant à un adversaire de réussir à se faire passer pour A auprès de B (ou vice-versa). Comment qualifierait vous le degré de difficulté de cette attaque?
- Comment peut-on modifier le protocole pour se prémunir contre cette attaque?

Protocole 2

Ce protocole se déroule uniquement entre Alice et Bob. Il suppose que ces deux participants partagent déjà une clé secrète K_{AB} et qu'ils souhaitent l'utiliser pour s'authentifier ainsi que pour générer une nouvelle clé K'_{AB} .

1. $A \rightarrow B : \{N_A\}_{K_{AB}}$
2. $B \rightarrow A : \{N_A+1, N_B\}_{K_{AB}}$
3. $A \rightarrow B : \{N_B+1\}_{K_{AB}}$
4. $B \rightarrow A : \{K'_{AB}, N'_B\}_{K_{AB}}$

Questions :

- Traduisez le protocole tel qu'il est écrit en notation de protocole de sécurité dans des phrases en langue naturelle expliquant son déroulement.
- Une fois que l'étape 3 est terminée peut-on considérer qu'Alice et Bob sont mutuellement authentifiés?
- Décrivez une attaque par rejeu contre le protocole. Pourquoi est ce que cette attaque est possible ?
- Comment peut-on modifier le protocole pour se prémunir contre cette attaque?