Département d'informatique
Faculté des sciences exactes et des sciences de la nature et de la vie
Université Mohamed Khider, Biskra

Année universitaire 2019/2020.

Sécurité Informatique — Série d'exercices N 3 (L3)

Exercice 1

[Challal 2016]

1. Objectif de sécurité. Soit le protocole cryptographique suivant :
   `M1 : B ==> A : B.PKb`
   `M2 : A ==> B : {m}PKb`
   L'objectif de ce protocole est :
   ◯ Authentification de A auprès de B
   √ **Confidentialité de m**
   ◯ Authentification de B auprès de A

2. Certification. Soit le protocole cryptographique suivant :
   `M1 : B ==> A : B.PKb`
   `M2 : A ==> B : {m}PKb`
   En supposant que S est une autorité de certification, ce protocole peut atteindre son objectif de sécurité en remplaçant M1 par :
   ◯ `B==>A : {B.PKb}PKs`
   ◯ `B==>A : {B.SKb}SKs`
   ◯ `B==>A : {B.SKb}PKs`
   √ `B==>A : {B.PKb}SKs`

3. Objectif de sécurité. Supposons que Kab est un secret partagé entre A et B. Soit le protocole suivant :
   `M1 : A==> B : Hello.A`
   `M2 : B==> A : Nb`
   `M3 : A==> B : {Nb}Kab`
   Quel est l'objectif de sécurité de ce protocole ?
   ◯ confidentialité de Nb
   ◯ confidentialité de Kab
   ◯ authentification mutuelle
   √ **authentification de A auprès de B**
   ◯ authentification de B auprès de A

4. Equivalence. Supposons que Kab est un secret partagé entre A et B. Soit le protocole suivant :
   `M1 : A==> B : Hello.A`
   `M2 : B==> A : Nb`
   `M3 : A==> B : {Nb}Kab`
   Quels sont les protocoles équivalents, au protocole précédent, dans l'objectif de sécurité ?
   √
   ```
   M1 : A==> B : Hello.A
   M2 : B==> A : {Nb}Kab
   M3 : A==> B : Nb
   ```
   ◯
   ```
   M1 : A==> B : Hello.A
   M2 : B==> A : {Nb}PKb
   M3 : A==> B : Nb
   ```
   √
   ```
   M1 : A==> B : Hello.A
   M2 : B==> A : Nb
   M3 : A==> B : {Nb}SKa
   ```

5. Kerberos. Le protocole Kerberos :
   √ **a pour objectif d'assurer une authentification mutuelle**
   √ **est basé sur une tierce partie de confiance**

√ **nécessite une synchronisation des horloges du client et serveur.**

6. Fonctionnement de Kerberos. Soit le schéma simplifié de Kerberos de la figure suivante :

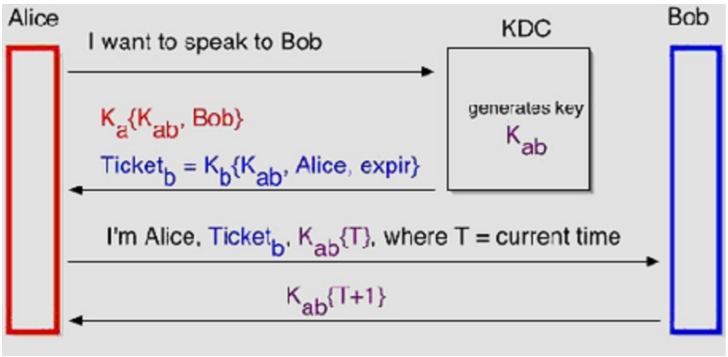

FIGURE 1 – Kerberos simplifié

◯ `Kb` est connue par Alice
√ `Kb` **est une clé symétrique partagée entre le KDC est Bob uniquement**
◯ `Kb` est égale à `Kab-Ka`
◯ `Kb` est utilisée par Alice pour déchiffrer Kab à partir du `Ticket_b`
◯ le message qui permet d'authentifier Alice auprès de Bob est `M1`
√ **le message qui permet d'authentifier Alice auprès de Bob est** `M3`

Exercice 2

[Avoine *et al.* 2010] Protocole d'authentification reposant sur une tierce partie. La figure suivante représente un protocole d'authentification utilisant un centre de distribution de clefs (KDC). A l'issu de l'échange de la clef `Kab`, `A` peut envoyer des messages chiffrés avec `Kab` à `B`.

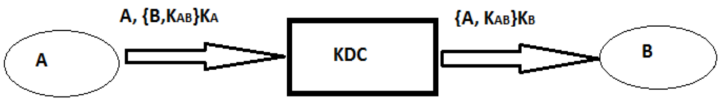

FIGURE 2 – Protocole d'authentification via KDC

1. Expliquer pourquoi un pirate ne peut pas se faire passer pour A auprès de KDC.
   Un pirate ne peut pas se faire passer pour A auprès du KDC parce que A partage une clé secrète Ka avec le KDC.
2. Expliquer pourquoi B est certain que le message provient du KDC.
   Parce que le message est chiffré en utilisant la clé secrète Kb partagée entre B et le KDC seulement.
3. A quelle attaque ce protocole ne résiste-t-il pas ?
   Réponse : l'attaque par rejeu des messages "Replay attack" *Indice* : Imaginer qu'un pirate `I` ait effectué un travail pour `A`. Après avoir échangé une clef de session via le KDC, `A` envoie un message à son banquier `B` pour lui demander de verser la rétribution sur le compte de `I`. Que faire à la place de `I` pour augmenter ses gains ?
4. Comment améliorer le protocole sans augmenter le nombre d'échanges pour déjouer ce type d'attaque ?
   Il suffit d'introduire le timestamp dans les messages envoyés.

Exercice 3

[Avoine *et al.* 2010] Analyse d'un système d'authentification chez la Sarl. Amane. La Sarl. Amane possède un réseau informatique interne qui permet de gérer la ligne de production. L'accès depuis les stations de travail aux serveurs intégrés sur les machines de la ligne de production nécessite une authentification sur un serveur centralisé.
Quand un employé, appelé dans la suite Client et noté `C`, veut accéder au serveur (noté `S`) contrôlant une machine, il doit passer le contrôle d'authentification exigé par le serveur centralisé (`AS`). Si cette authentification réussit, `AS` envoie des données à `C`, en particulier la liste des serveurs auxquels il est autorisé à se connecter. La figure suivante représente les échanges entre `AS`, `C` et `S`. On suppose qu'un pirate est capable d'écouter la communication.

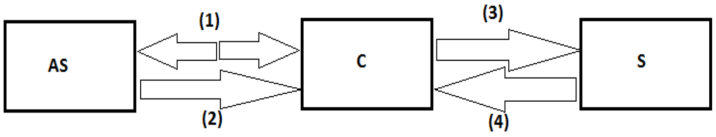

FIGURE 3 – Système d'authentification de Amane

(a) `C` et `AS` effectuant un protocole d'authentification (que vous devrez concevoir dans la suite). A l'issu de ce protocole, on suppose qu'il se sont mis d'accord sur une clef de session `Kc,as`.

(b) Quand `C` est authentifié, AS choisit une clef aléatoire KC,S et envoie :
`{V,L}Ks,as||{C,Kc,s,V}Ks,as||{Kc,s}Kc,as` à `C`, où `V` est une période de validité (suffisamment longue pour que le client ne doive effectuer l'authentification qu'une seule fois par jour) et `L` est une liste des serveurs auxquels le client est autorisé d'accéder.

(c) Ensuite `C` envoie le message suivant à `S` :
`{V,L}Ks,as||{C,Kc,s,V}Ks,as||{C,requête}Kc,s`

(d) A partir de `{V,L}Ks,as`, le serveur `S` vérifie que le client est autorisé à accéder au service demandé dans la requête. Si c'est le cas, il exécute la requête et renvoie si nécessaire le résultat au client.

Questions :

1. Concevoir un protocole d'authentification qui pourrait être entre `C` et `AS`. Ce protocole ne doit pas nécessiter l'envoi de mots de passe ou de hachés de mots de passe en clair sur le canal.
2. On considère dans la suite un pirate qui a pu être correctement authentifié par le serveur `AS` (par exemple, le pirate est un employé de la société Amane) mais qui n'a pas les droits d'accès pour un certain serveur `S'`.
   Proposer une attaque telle que `S'` accepte la requête forgée par le pirate.
3. On considère maintenant un pirate qui n'a pas pu être authentifié par le serveur `AS`. Expliquer quelle type d'attaque le pirate peut tenter et pourquoi une telle attaque est possible.
4. Comment peut-on modifier le protocole pour éviter les attaques des deux questions précédentes ?
5. Nous remarquons que `C` doit contacter `AS` à chaque fois qu'il veut interroger un nouveau serveur `S`. Pourquoi ? Comment peut-on modifier le protocole pour éviter ce problème, sans ajouter d'entité dans l'architecture.