KERBEROS

Description

Introduction

- **Origine : Projet « Athena ».**
- **Ethymologie.**
- **Description.**
  - **Système de cryptographie à base de clés secrètes.**
  - **Algorithme DES.**
  - **Basé sur la présence d'un service de tierce partie de confiance.**
- **Permet à des utilisateurs distants d'accéder à des services réseaux de façon sécurisée.**
- **Utilisé par windows 2000, XP et server 2003.**

Historique

- Première version = Version 4, publiée par Steve Miller et Clifford Neuman à la fin des années 80.
- La version 5 publiée en 93.
- Kerberos a été classé comme munition et a été interdit d’exportation par les autorités américaines.
- L’IETF est toujours entrain de mettre à jour les spécifications du protocole.

Fonctionnement

Alice

Alice désire accéder au serveur de services « Bob »

SS

Passage par la tierce partie de confiance

TGS

AS

Fonctionnement

1. Alice fabrique sa clé secrète à partir de ses paramètres de connexion.

Alice

2. Demande claire d'accès au SS, ici représenté par Bob.

3. AS vérifie qu'Alice existe dans sa BD et lui envoie:
•A : La clé de session TGS/Alice crypté avec la clé secrète d'Alice (pour communiquer avec le TGS).
•B : Le ticket-Granting ticket, crypté avec la clé secrète du TGS.

AS

Fonctionnement

Alice

4. Alice décrypte A pour obtenir la clé de session TGS/Alice.

7. Le TGS envoie deux messages à Alice:
•E : Ticket d'accès au serveur (qui contient l'ID d'Alice, son adresse IP, le « timestamp ») crypté à l'aide de la clé secrète de Bob.
•F : La clé de session Alice/Bob cryptée à l'aide de la clé de session TGS/Alice.

5.Alice envoie deux messages au TGS:
•C : B et l'ID de Bob.
•D : Son ID et le « timestamp » crypté avec la clé de session TGS/Alice.

6.Le TGS décrypte C, récupère la clé de session TGS/Alice. A l'aide de cette clé, il décrypte D.

TGS

Fonctionnement

Alice

12. Alice décrypte I et vérifie que le « Timestamp » a bien été mis à jour. Elle peut alors faire confiance à Bob et entamer l'envoi des requêtes.

8. Alice décrypte F pour obtenir la clé de session Client/Serveur. Elle se connecte ensuite à Bob.

11. Bob envoie le message suivant à Alice :
•I : Le « timestamp » trouvé dans H + 1 crypté avec la clé de session Alice/Bob.

9.Alice envoie deux messages à Bob:
•G : E
•H : Son ID et le « timestamp » crypté à l'aide de la clé de session Alice/Bob.

10. Bob décrypte G et vérifie la cohérence entre les infos contenues dans G et celles contenues dans H.

SS

13. Fournit les services demandés par Alice/

Intérêt

- Il propose un système d'authentification mutuelle permettant au client et au serveur de s'identifier réciproquement.

- L'authentification proposée par le serveur Kerberos a une durée limitée dans le temps, ce qui permet d'éviter à un pirate de continuer d'avoir accès aux ressources : on parle ainsi d'anti re-jeu.

KERBEROS

Analyse de l’article:

« Kerberos V security : Replay Attacks »

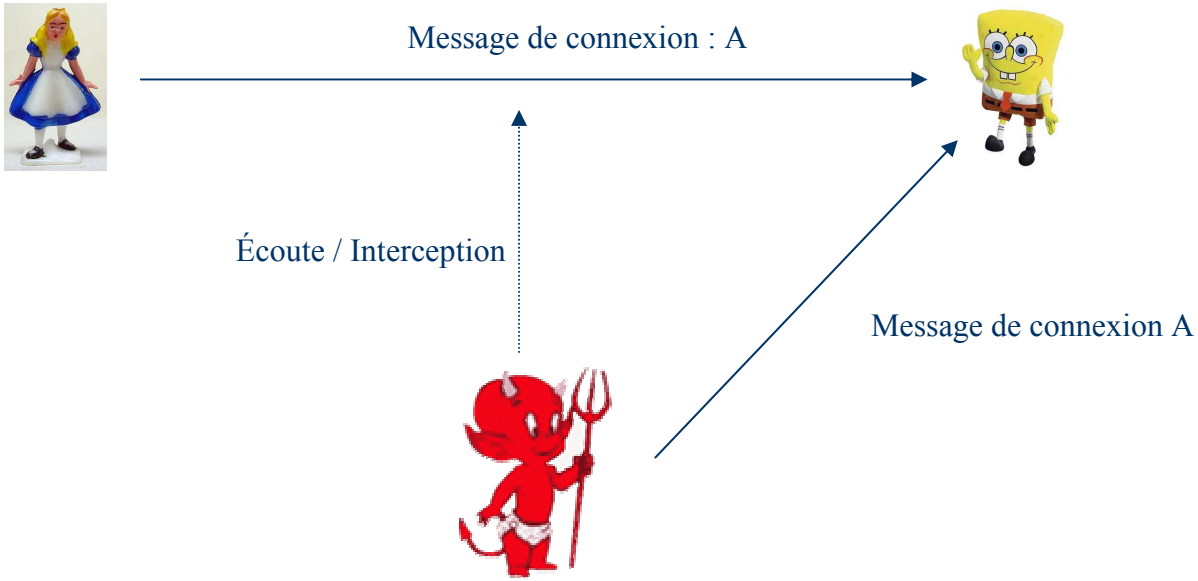
Failles de sécurité de Kerberos

- Différents types d’attaques:
  - « Replay Attacks »
  - Password Attack contre le TGT
  - Attaque contre le NTP
- On ne s’intéresse qu’aux « Replay attacks »

Les Replay Attacks

- Définition:
  - Attaque réseau dans laquelle le pirate réutilise ou retarde une trame de données valide.

- Exemple:



Kerberos Vs Replay attacks (1/4)

12. Alice décrypte I et vérifie que le « Timestamp » a bien été mis à jour. Elle peut alors faire confiance à Bob et entamer l'envoi des requêtes.

8. Alice décrypte F pour obtenir la clé de session Client/Serveur. Elle se connecte ensuite à Bob.

11. Bob envoie le message suivant à Alice :
•Le « timestamp » trouvé dans H + 1 crypté avec la clé de session Alice/Bob.

9.Alice envoie deux messages à Bob:
•G : E
•H : Son ID et le « timestamp » crypté à l'aide de la clé de session Alice/Bob.

10. Bob décrypte G et vérifie la cohérence entre les infos contenues dans G et celles contenues dans H.

13. Fournit les services demandés par Alice/

SS

Kerberos Vs Replay attacks (2/4)

- Kerberos est censé être capable de se protéger contre ces attaques:
  - L'échange 9 inclut l'adresse IP du client.
  - L'échange 9 contient le « Timestamp ».
  - Bob utilise un cache pour enregistrer les données de l'échange 9.
- Mais sur certains environnements :
  - Pas de présence de l'adresse IP dans les messages de l'échange 9.
  - « Timestamp » trop flexible.
  - Malgré l'utilisation du cache, les attaques actives restent possibles.

Kerberos Vs Replay attacks (3/4)

- Moyens de protection contre ce type d'attaque:
  - Attaque nécessite l'écoute sur le réseau souvent à l'aide de la méthode ARP spoofing.
    - Protection contre l'ARP spoofing : Donner des adresses statiques aux machines du réseau.
  - Utilisation du IP secure mode.
  - Data Integrity verification :
    - Alice et le serveur partagent la clé de session que le pirate ne peut pas connaître.
    - Introduction du checksum dans les paquets échangés.

Kerberos Vs Replay attacks (4/4)

- Conclusion:
  - Les « Replay attacks » restent possibles avec des moyens modestes pour deux raisons :
    - Applicatifs utilisant Kerberos contiennent des failles.
    - Configurations par défaut de certains applicatifs sont permissibles aux replay attacks.
  - Lorsqu'un attaquant a accès au réseau, il est difficile d'empêcher les replay attacks.