ANNÉE 2010-2011

Étape : Master Sciences Technologies (semestre 3)
Épreuve de : Sécurité des réseaux
Date : 15 Décembre 2010
Heure : 14h
Documents documents interdits
Épreuve de Monsieur Guermouche

SESSION DE DÉCEMBRE 2010

UE : MHT914/INF585
Durée : 1h30

Questions générales

1. Expliquer brièvement les différents modes de fonctionnement d'IPSec. Il vous est tout particulièrement demandé d'insister sur ce qui est chiffré et ce qui est en clair dans chacun des cas.
2. Expliquer brièvement le fonctionnement du protocole SSL/TLS. En quoi ce protocole est il différent d'IPSec ?
3. Expliquer brièvement ce qu'est une clé PGP et donner quelques exemples d'utilisation de ce genre d'objets. En quoi une clé PGP est différente d'un certificat X509 ?

Exercice 1

Un utilisateur qui a pour habitude d'utiliser la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? Lire le contenu (non-chiffré) des messages reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 2

Soit la configuration réseau suivante dans laquelle nous voulons mettre en place un support IPSec entre les machines A et B :

Parmi les configurations IPSec suivantes, indiquer celles qui peuvent être utilisées avec de la translation d'adresse (NAT) :

1. ESP en mode tunnel.
2. ESP en mode transport.
3. AH en mode transport.

Rappel : Lorsqu'on utilise une passerelle NAT :
- l'adresse source, et éventuellement le port source, du paquet émis est modifiée par la passerelle lorsqu'il la traverse,
- l'adresse de destination, et éventuellement le port de destination, du paquet est modifiée par la passerelle lorsque le paquet qui doit être reçu traverse la passerelle.

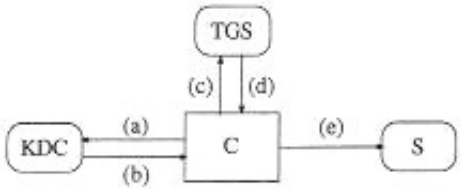
Exercice 3

Un pirate a remarqué qu'une requête de transfert de zone DNS (utilisée notamment pour fournir à un serveur DNS l'information qu'il doit connaître concernant la ou les zones qu'il doit desservir) fait toujours 27 octets de long, et que la réponse du serveur DNS `dns.metal.fr` fait 745 octets. On supposera que les communications se font au moyen d'UDP. De plus, le pirate dispose d'une ligne à 256 Kbps et le serveur `pauvre.victime.com` dispose d'une ligne à 5 Mbps. Enfin, le serveur `dns.metal.fr` dispose quant à lui d'une bande passante de 1 Gbps.

1. Comment le pirate peut-il réaliser une attaque par déni de service (DoS) contre le serveur `pauvre.victime.com` ? Expliquer.

Exercice 4

On s'intéresse dans cet exercice au procédé d'authentification Kerberos V. Kerberos considère quatre entités : le client (C), le centre de distribution des clés (KDC), le serveur de tickets (TGS) et le serveur (S) qui offre le service désiré. Comme indiqué dans la figure suivante, le client s'adresse successivement à chacun de ces serveurs.



a. Le client C envoie une requête au KDC afin d'obtenir un ticket d'octroi de ticket (TGT) qui pourra utilisé auprès du TGS.

b. Le KDC possède l'identité du client C ainsi que la clé K_C qui lui est associée. Le KDC envoie donc au client la clé de session $K_{C,TGS}$ chiffrée avec K_C qui sera alors utilisée entre le client et le TGS ainsi que le ticket $T_{C,TGS}$ chiffré avec la clé du TGS, K_{TGS}. Le ticket contient essentiellement l'identité du client, une copie de la clé de session $K_{C,TGS}$ ainsi qu'une période de validité.

c. Le client transmet $T_{C,TGS}$ au TGS ainsi qu'un authentificateur A_C contenant l'identité du client ainsi qu'un horodatage ; l'authentificateur étant chiffré avec la clé de session $K_{C,TGS}$. Le TGS s'assure que le client est bien le détenteur légitime du ticket en vérifiant que l'authentificateur est chiffré avec la clé $K_{C,TGS}$ contenue dans le ticket.

d. Le TGS envoie ensuite au client la clé de session $K_{C,S}$ chiffrée avec $K_{C,TGS}$ qui sera utilisée entre le client et le serveur ainsi que le ticket $T_{C,S}$ chiffré avec la clé du serveur K_S. Le ticket contient essentiellement l'identité du client, une copie de la clé de session $K_{C,S}$ ainsi qu'une période de validité.

e. Le client transmet $T_{C,S}$ au serveur ainsi qu'un authentificateur A_C qui contient l'identité du client et un horodatage. Le serveur peut alors délivrer le service au client.

Remarque : K_C (resp. K_S) est la clé secrète du client (resp. serveur).

1. Comment peut-on vérifier que l'authentificateur a bien été crée par le détenteur légitime du ticket ?
2. On s'interroge maintenant sur la possibilité d'usurper le ticket d'un autre client : un pirate espionne le réseau et voit le ticket que le TGS envoie au client. Le pirate connaît aussi l'identité du client à qui est destiné le ticket. Qu'est ce qui empêche le pirate d'utiliser le ticket pour obtenir un service à la place du client légitime ?