Université Paris XII
UFR de Sciences et Technologie
Département Informatique
Master deuxième année
2006/2007

EXAMEN SERE

2 heures

Attention ! Chacun des quatre exercices devra être rédigé sur une copie double indépendante (correcteurs différents) en spécifiant bien l'exercice.

Les documents ne sont pas autorisés sauf pour le quatrième exercice.

Exercice 1.- (Maryline, 3 points, **sans support de cours**)

- 1^o) Quelle est la différence de protections offertes entre AH et ESP? Existe-t-il un besoin précis qui nécessitera l'usage de ESP?

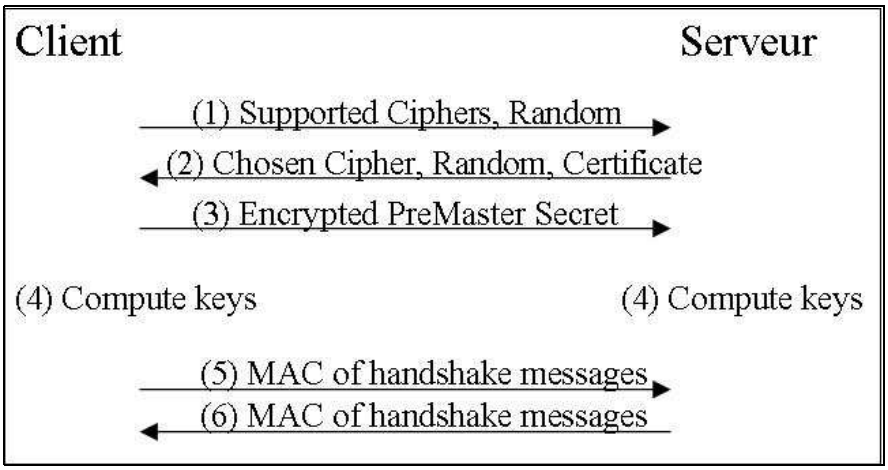

Figure 1: Premiers échanges du protocole *SSL Hanshake Protocol*

- 2^o) Dans les protocoles de sécurité de type SSL ou IPsec, quel est le rôle joué par la cryptographie symétrique et la cryptographie asymétrique? Donnez les raisons de ce choix.

- 3^o) Considérons le protocole SSL dont les premiers échanges *Handshake* sont donnés à la figure 1.

1. Quels sont les paramètres de sécurité négociés par le client et le serveur SSL?
2. Expliquez comment se passe la négociation de ces paramètres.
3. À quoi correspondent le message (3) et l'étape (4) de la figure 1? Expliquez.
4. Comment le client est-il sûr de communiquer avec le serveur déclaré dans les échanges?

- 4^o) Quels sont les services de sécurité rendus par le sous-protocole AH?

- 5^o) Quels sont les atouts et les inconvénients de l'usage des protocoles IPsec par rapport à SSL? Expliquez.

Exercice 2.- (Olivier, 3 points, **sans support de cours**)

En quoi le fait d'empêcher l'usurpation d'adresses permet-il de limiter les attaques de dénis de service ? Donnez un exemple de méthode permettant de réaliser ce service et expliquez comment elle fonctionne.

Exercice 3.- (Alexander, 6 points, **sans support de cours**)

Reporté à plus tard

Exercice 4.- (Patrick, 8 points, **avec documents sur les formats**)

On a récupéré avec Ethereal la trame suivante provenant d'une interface Ethernet. Analyser cette trame.

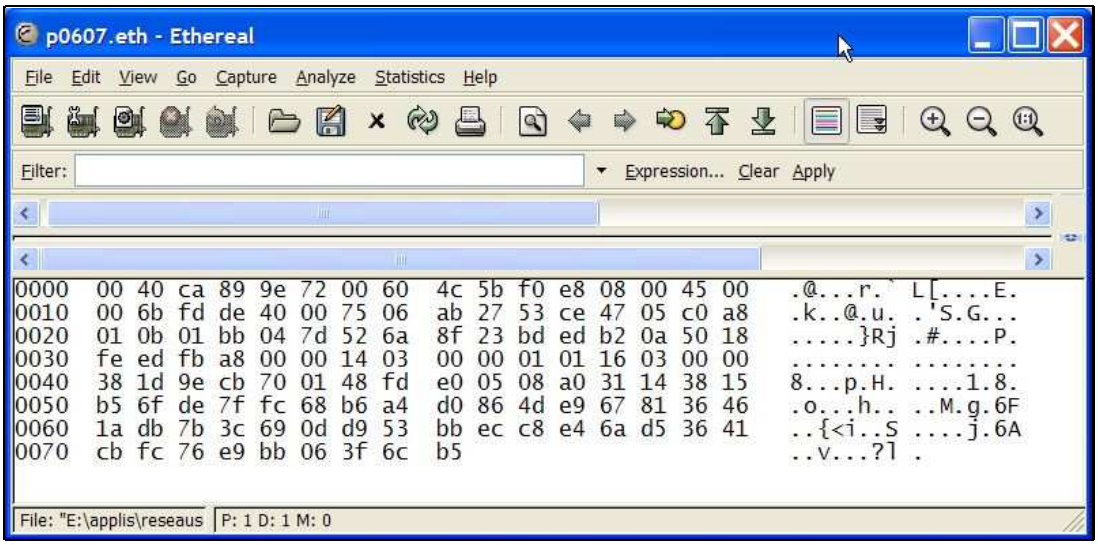

Figure 2: Trame Ethernet

On entourera en particulier l'adresse MAC de l'expéditeur, son adresse IP, le port de destination et la longueur de la fenêtre TCP.