Université Paris XII
UFR de Sciences et Technologie
Département Informatique
Master deuxième année
2005/2006

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

- 2^o) En quoi la gestion de la sécurité dans le contexte IPsec est-elle plus lourde que pour SSL? Expliquez.

- 3^o) Expliquez quels sont les objectifs du service d'intégrité.

- 4^o) En quoi consiste la protection en intégrité des données dans SSL? Décrivez le mécanisme.

- 5^o) Ce même mécanisme sert-il à authentifier l'origine des données?

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

Donnez les grandes phases existant aujourd'hui dans les techniques de lutte contre les attaques de déni de service. Expliquez les objectifs de chacune d'entre elles en donnant éventuellement des exemples d'attaques illustrant ceux-ci.

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

- 1^o) Caractériser des protections de systèmes bancaires : organisation, structures de réseaux de grandes banques et mécanismes de protection et de sécurisation.

- 2^o) Expliquer des objectifs d'un audit de sécurité des systèmes téléinformatiques ; présenter des types d'audits et indiquer leurs spécificités.

- 3^o) Expliquer les principes de sécurisation de nouveaux réseaux ; comment sont réalisés les systèmes autocorrectifs ; donner des exemples des mécanismes d'auto-rétablissement dans le cas d'une panne franche d'un routeur ou d'un brasseur.

- 4^o) Calculer les paramètres de fiabilité et de disponibilité globaux (MTBF et MTTR) du système téléinformatique suivant décrit par le diagramme avec les paramètres avec cinq composants S.1 à S.5 caractérisés par des valeurs individuelles sur la base 7/24 de MTBF et MTTR suivantes:

S.1 : 800h, 3h; S.2: 200h, 24h; S.3: 1000h, 30h; S.4: 2000h, 10h et S.5: 500h, 12h.

Quel composant faudra-t-il doubler en parallèle en premier ordre pour améliorer la disponibilité globale?

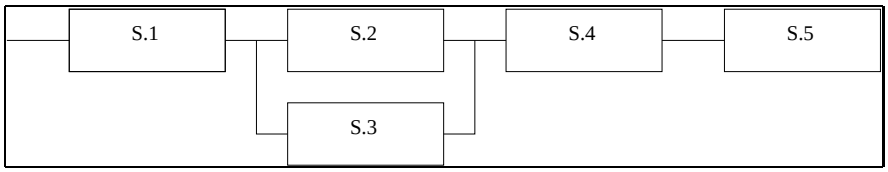

Figure 1: Système téléinformatique

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.

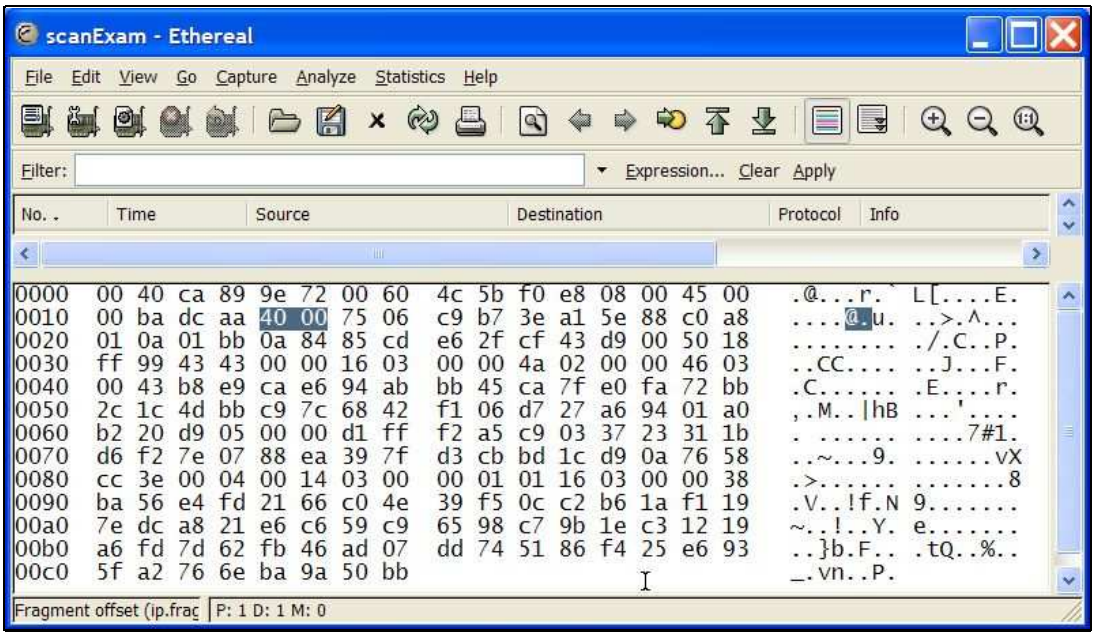

Figure 2: Trame Ethernet

On entourera en particulier l'adresse MAC de l'émetteur, son adresse IP, le port de destination, la version SSL utilisée et les algorithmes de sécurité.