Université Paris Diderot
M2 informatique
Protocoles et services internet
2011-2012

Examen Protocoles et Services Internet

(durée 2 heures, documents interdits)

Tous les exercices sont indépendants. La plupart des questions sont des questions de réflexion pour lesquelles plusieurs réponses peuvent être admises si elles sont correctement justifiées.

Exercice 1.— Définir ce que l'on entend par un proxy? En présence d'un proxy, le code des applications doit-il être modifié? A quoi un proxy peut-il servir? Quelles sont les di□érences (et les ressemblances) entre un pare-feu (firewall) et un proxy.

Exercice 2.—

1. Supposons que Bob veuille envoyer un message m à Alice, comment avec un système de cryptage avec des clés publiques, assurer l'authentification des messages provenant de Bob à Alice? Qu'est ce que la propriété de non-répudiation? Décrire un protocole assurant ces deux propriétés utilisant un système à clés publiques.
2. Décrire le principe des certificats établis par des autorités de certifications pour des systèmes à clés publiques.
3. Décrire le mécanisme des distributions de clés pour Alice et Bob pour un système de cryptage à clés symétriques. On supposera l'existence d'un centre de distribution de clés, on supposera aussi que Alice (respectivement Bob) a une clé symétrique lui permettant de communiquer avec ce centre de distribution de clés.
4. Est-il possible d'assurer l'authentification et la non répudiation en utilisant uniquement des clés symétriques? Si oui comment?
5. Pourquoi même avec un système de cryptographie avec des clés publiques, le codage symétrique est-il utile? Donner des exemples d'utilisation.

Exercice 3.— Expliquer succinctement en quoi consiste le modèle client serveur. Même question pour le modèle Pair à Pair. Au niveau des connexions avec des socket (par exemple Java), la notion de pair à pair a-t-elle du sens? Si non pourquoi et si oui de quelle façon?

Exercice 4.—

1. Qu'est ce que le DNS, quel est son rôle? Décrire dans les grandes lignes son fonctionnement. Pourquoi le fonctionnement du DNS est important du point de vue de la sécurité?
2. Si on suppose que les adresses des sites ne dépendent pas de la localisation (en particulier ne dépendent pas du réseau local) quels problèmes se posent.
3. Soit A un ordinateur portable qui peut donc se connecter sur di□érents réseaux locaux. En supposant que A soit identifié par une adresse IP sur un réseau fixe particulier, proposer une (des?) solutions pour assurer qu'il soit joignable sur le réseau local sur lequel il est à un moment donné.

   Si maintenant A est identifié par un nom internet, comment peut-on procéder?