Institut National des Sciences Appliquées de Lyon

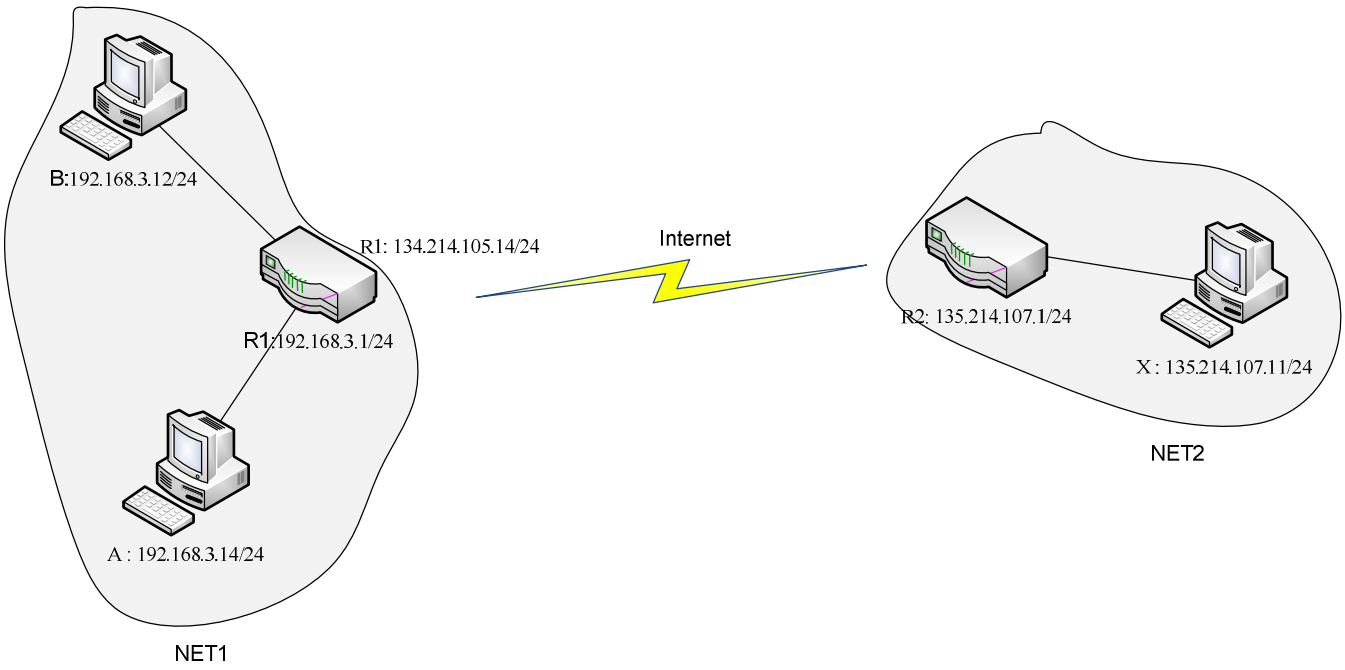
Département Informatique, 4ème année, 2007-2008

Réseaux avancés et sécurité

(Documents manuscrits et copies des supports de cours autorisés)

A. Questions d'ordre général (6 points)

Deux réseaux, NET1 et NET2 (figure suivante) sont connectés via l'Internet. NET1 est connecté à l'Internet via un routeur implémentant un NAT/PAT/masquage, avec une adresse publique (134.214.105.14) partagée par les ordinateurs du réseau (A et B). Le réseau NET2 est un réseau avec plan d'adressage public (l'ordinateur X est visible sur Internet).



A-1 Un navigateur Web s'exécute sur la machine A. Il se connecte au serveur Web situé sur la machine X. Le serveur Web met à jour un log avec les clients qui lui ont envoyé des requêtes. Il utilise dans ce but une primitive de type GetPeerName qui fournit l'adresse IP et le port de la machine distante. Quelle est l'adresse IP et le port qu'il va obtenir ? Expliquez le résultat.

A-2 Un serveur Web est démarré sur la machine B. Quel est le mécanisme à mettre en œuvre pour qu'un navigateur s'exécutant sur la machine X puisse se connecter à ce serveur ? Quel est l'URL nécessaire pour afficher la page racine d'un site hébergé par le serveur B ? Justifiez votre réponse.

A-3 Vous devez implémenter un logiciel de chat vous permettant de communiquer entre les machines A, B et X. Ce logiciel utilisera un protocole basé sur UDP avec les primitives : CONNECT, SEND_MSG, EXIT, ACK. Décrivez la configuration réseau à mettre en œuvre, sachant que A et B ont des adresses privées. Décrivez les paramètres que vous imaginez pour ces primitives (adresses IP, ports …) pour que la communication puisse avoir lieu correctement, en précisant d'éventuels modules supplémentaires (ou d'autres primitives de communication). Décrivez en utilisant un formalisme de votre choix un cas normal d'utilisation pour un chat entre X et A.

B. Question d'ordre général (4 points)

Les étudiants de 2ème année INSA (2PC) visitent le département informatique. Le directeur du département vous a confié la tâche de faire un « exposé technologique » sur le thème : technologies de sécurisation d'applications réparties » et de rédiger une courte synthèse (2 pages maximum) qui sera distribuée aux étudiants : à vos plumes ! Remarque importante : attention ! Le sujet porte sur les technologies, ***pas*** les méthodologies telles EBIOS, Mehari, etc.

C. Conception de protocoles et sécurité (10 points) : cap sur l'espace (de données) !

Le docteur Benela reçoit, sur rendez-vous, des patients à l'hôpital et à son cabinet de ville ; il visite également ses patients à leur domicile. Enfin, le soir, il travaille chez lui (gestion financière de son activité).

Les informations professionnelles qu'il manipule sont ainsi disséminées dans 4 serveurs de données : le serveur de l'hôpital, l'ordinateur de son cabinet, son ordinateur portable (utilisé lors de ses visites à domicile), son ordinateur personnel fixe.

On appelle espace de données (« data space ») du Dr Benela l'ensemble des données stockées dans ces serveurs auxquelles le Dr Benela a accès, c'est-à-dire celles dont il est responsable (il a donc sur ces données le droit de lecture-écriture ; ex : dossiers de ses patients, données financières personnelles) et celles qui lui sont seulement accessibles en lecture (ex : bases de données de médicaments, bases de protocoles thérapeutiques, etc.).

On suppose que :

- Chaque fichier est identifié par un identificateur unique par rapport à l'ensemble des serveurs
- Chaque fichier est décrit par un ensemble de meta-données (ex : date de modification, mots-clefs…)
- Tous les serveurs disposent d'un module d'interface (*Dataspace_Server*) fournissant l'API suivant :
    - GET(idFile) : prend en paramètre l'identificateur d'un fichier et retourne ce fichier
    - SEARCH(metadata) : prend en paramètre des valeurs de méta-données et retourne la liste des fichiers correspondant à ces méta-données ainsi que, pour chaque fichier, l'ensemble de ses meta-données. Ex :
        - search(modif_date: « 05/05/2008 ») : retourne la liste des fichiers modifiés le 05/05/2008 (et leurs meta-données)
        - search(keyword: « Jean Dupont ») : retourne la liste des fichiers (ex : prescriptions, radiographies, examens sanguins, etc.) concernant Mr Jean Dupont (et leurs meta-données)
- les champs de meta-données sont les mêmes dans tous les serveurs (ex : quel que soit le serveur, le champ « modif_date » représente la date de dernière modification)
- les droits d'accès sont représentés par des listes de contrôle d'accès (Access Control Lists : ACL) : l'ACL d'un fichier contient la liste des utilisateurs ayant soit un droit de lecture-écriture, soit un droit de lecture seule sur le fichier (les utilisateurs n'apparaissant pas dans cette liste n'ont donc aucun droit sur le fichier)[1]

Le Dr Benela a de la chance : il utilise la même interface graphique (*MyDataspace*) qu'il travaille sur son portable, sur l'ordinateur de l'hôpital, sur celui de son cabinet ou sur celui de son domicile. Cette interface permet :

[1] Dans la suite du problème, on ne s'intéressera qu'à des accès en lecture uniquement (read only).

- de spécifier des requêtes de recherche de fichiers. Une requête de recherche est constituée :
    - de valeurs de meta-données (« critères de recherche »). Ex : modif_date = « 12/08/2007 »
    - de la liste des serveurs concernés. Ex :
        - servers = portable : la recherche ne sera lancée que sur le portable
        - servers = all : la recherche sera lancée sur les 4 serveurs

La réponse à une telle requête est la liste (identifiant, meta-données) de l'ensemble des fichiers stockés dans les serveurs concernés qui correspondent aux critères de recherche spécifiés dans la requête.

- de spécifier des requêtes de consultation de fichiers. Une telle requête est constituée d'une liste d'identifiants de fichiers. En réponse, l'ensemble des fichiers est téléchargé sur l'ordinateur d'où est émise la requête. L'interface offre alors des outils conviviaux de consultation de ces fichiers.

Le but du problème est d'étudier les modules de communication qui doivent être mis en place (sur les serveurs et le portable).

C-1 Accès aux données

Décrire les protocoles de communication (fondés sur INET) mis en œuvre :

- dans le traitement des requêtes de recherche de fichiers,
- dans le traitement des requêtes de consultation.

C-2 Gestion de la sécurité

Les données (et meta-données) manipulées dans cette application sont, pour certaines, confidentielles (ex : éléments de dossiers médicaux). Il est donc indispensable de mettre en place un mécanisme de contrôle d'accès. Le responsable du projet vous demande d'étudier une solution à base de certificats et de PKI :

- décrire les éléments (serveurs, logiciels) de la PKI à mettre en place
- décrire les données stockées (« champs ») dans les certificats
- décrire un mécanisme et les protocoles de contrôle d'accès associés mis en œuvre lors des opérations SEARCH et GET (les protocoles seront fondés sur INET)
- décrire les mécanismes et les protocoles (fondés sur INET) mis en œuvre dans la gestion des certificats

C-3 Réplication

En vue d'accélérer certains traitements, les meta-données de l'ensemble des fichiers de l'espace de données du Dr Benela sont répliquées sur le serveur de l'hôpital : proposer un protocole de réplication.

Vous avez toute latitude pour préciser des points spécifiques, proposer (et utiliser) des serveurs ou services additionnels à implanter, préciser certaines hypothèses sur l'application dès lors que vos propositions sont argumentées.

Bonnes vacances (et bon stage) !!!