Composition de Sécurité logique et réseaux 2003

La composition est décomposée en trois parties :
?? Une partie d'étude de certaines techniques de sécurité
?? Une partie d'étude de cas réel
?? Une partie théorique d'analyse cryptographique

Il est recommandé aux élèves de bien choisir l'ordre des parties selon leurs compétences et rapidités.

Le support de cours et documents sont permis.

Les questions sont pour les élèves ingénieurs et maîtrise sauf les parties 1.3 (Ingénieurs) et 1.4 (Maîtrise)

1. Techniques de Sécurité

1.1 Sécurité Carte Wireless (WIFI, Bluetooth) (3 points)

Un réseau local est formé :
de trois portables utilisant chacun une carte wireless ,
un point d'accès wireless (switch),
Un serveur.

Les adresses MAC des cartes sont les suivantes : 00022D1EX530, 00022D1EX531, 00022D1EX532.

1) Quels sont les trois risques les plus importants au niveau de l'accès de chaque carte au réseau.(3 lignes, 2 points)
2) Décrire les règles de filtrage au niveau du point d'accès au réseau en utilisant les adresses MAC.(1 point)

1.2 Sécurité Administrateur (4 points)

Un réseau local connecte plusieurs hosts et un serveur. Les diverses machines utilisent des cartes Ethernet. Le but de cet exercice est d'améliorer l'accès de l'administrateur.
Le serveur est un portail interne d'entreprise (Ports 80 et 443) pour les divers utilisateurs.
L'administrateur utilise uniquement les port telnet pour l'administration et ftp pour la mise à jour des pages Web du serveur.
Les adresses IP sont fournies dynamiquement par un serveur DHCP dans la plage 192.168.1.x.

1) Proposer la meilleure plan d'adressage du serveur DHCP.(2 lignes 0,5 point)
2) Décrire les règles de filtrage du firewall du serveur. (1,5 points)
3) Que proposez vous pour chiffrer l'accès telnet de l'administrateur au serveur (1 ligne 0,5 point)
3) Quelle conséquence implique la solution de chiffrement (1 ligne 0,5 point)
4) Quelle solution matérielle supplémentaire améliore-t-elle la sécurité de l'accès de l'administrateur au serveur ?(1 ligne 0,5 point)
5) Quelle conséquence implique la solution matérielle (1 ligne 0,5 point)

1.3 Implémentation par PKCS11 du schéma d'authentification par calculettes (3 points)

Un projet d'accès à un serveur Web nécessite l'utilisation de calculettes pour l'authentification selon le schéma suivant :

Le serveur génère une valeur aléatoire Q qu'il envoie au client ayant l'identité ID.
Le client saisit la valeur aléatoire transmise par le serveur sur sa calculette. Pour cet exercice on suppose que la fonction utilisée par la calculette est f(Q) = DES(Q) avec une clé Ki unique et statique propre à chaque calculette.
L'utilisateur envoie le résultat f(Q) affiché au serveur.
Le serveur possède les clés Ki des clients dans un dispositif PKCS11. Chaque clé Ki est identifiée par l'identité IDi de chaque client. L'accès par le serveur à la liste des dispositifs est protégé par une passphrase PWD.

1) Implémenter la fonction f(Q) en utilisant les requêtes PKCS11. (1,5 points)
2) Implémenter la vérification côté serveur en utilisant les requêtes PKCS11. (1,5 points)

1.4 Implémentation de tunnels SSH (3 points)

Pour chiffrer l'accès au serveur (192.168.1.5) de messagerie POP3 (port 110) et SMTP (port 25) d'une entreprise, la fonction tuneling de ssh est utilisée. Le serveur de messagerie est administré par telnet (port 23) à partir du host (192.168.1.4).

1) Définir la requête de lancement de ssh côté poste client pour permettre le tuneling. (1,5 points)
2) Le client utilise Outlook. Définir les paramètres à modifier dans Outlook pour utiliser la fonction de tuneling. (0,5 point)
3) Définir les règles de filtrage sur le firewall du serveur de messagerie ? (1 point)

2. Etude de Cas dans le domaine de la médecine (10 points)

Le but de cet exercice est d'implémenter les divers mécanismes de sécurité dans le cas des dossiers de patients gérés par les médecins ou cliniques.

1) Pour quelle raison la confidentialité des dossiers des patients est importante? (1 ligne 0,5 point)

2) Que proposez vous d'implémenter comme techniques de sécurité sur le poste du médecin (2 lignes 0,5 point)

3) Chaque médecin possède une carte à puce. Deux certificats X509 sont utilisés par chaque médecin (signature et chiffrement). (2 points)
   - ?? Définir le mapping de la carte de chaque médecin (clés RSA 1024 bits, chaque Certificat a une taille de 1 Koctets).
   - ?? Plusieurs cartes sont proposées (1 Ko, 2 Ko, 4 Ko, 8 Ko). Quelle carte utiliser ?

4) Trois types de lecteurs de carte à puce sont proposés. La fréquence utilisée par le lecteur définit la vitesse de la signature RSA.
   - ?? lecteur à fréquence 4 Mhz simple sans pinpad à 50 $,
   - ?? lecteur à fréquence 4 Mhz avec pinpad à 100$,
   - ?? lecteur à fréquence 8 Mhz avec pinpad à 400$.

   Quel est le meilleur lecteur adapté au médecin ? (2 lignes 1 point)

5) Le diagnostic d'un médecin implique sa responsabilité professionnelle. Que proposez vous pour protéger l'intérêt du patient? (2 lignes 1 point)

6) En attendant le déploiement des diverses solutions de sécurité chez tous les médecins, que proposez vous à un médecin possédant une messagerie sécurisée et qui doit envoyer un message sécurisé à un médecin ne possédant pas de solution de sécurité ? (2 lignes 1 point)

7) Pour des raisons de statistiques les cliniques doivent envoyer les fichiers de séjour des patients à un centre d'étude. Une loi interdit l'échange des fichiers de séjour incluant les informations nominatives des patients (noms et numéros de sécurité sociale des patients).Or les fichiers sont générés d'une façon nominative par des applications des cliniques. Que proposez vous ? (2 lignes 1 point).

8) Plusieurs solutions sont proposées pour le centre d'étude :
   - ?? Un développement en interne de 5 années-Homme. Le salaire brut moyen est de 25000$/année.
   - ?? Un logiciel fourni par une société de service à 150000$ avec une maintenance de 15% par année.

   Quelle solution préconisez vous ? Pourquoi ? (1,5 points)

9) Chaque clinique (total 200 cliniques) envoie en moyenne 1 fichier/mois par messagerie. Chaque fichier a une taille moyenne de 10 Mo. Toutes les informations des fichiers sont importées dans une base de donnée. Une fois importé un fichier est effacé de la messagerie. Les informations doivent être gardées pendant 18 mois. Quelle taille de stockage faut il prévoir ? Que préconisez vous pour les informations dépassant les 18 mois ? (1,5 points)

3.Une Analyse Cryptographique sur le RSA (4 points)

Le but de cet exercice est de trouver si chaque habitant de la terre peut avoir une bi-clé RSA unique pour des tailles actuelles de clés.

Toutes les notions mathématiques nécessaires ont été simplifiées.

Le modulo N=p*q avec p < q ; p et q sont des nombres premiers.

On va considérer les hypothèses et approximations suivantes :

- ?? Les nombres premiers p et q sont de la taille de 512 bits, et que $2^{512} < p$ et $q < 2^{513}$
- ?? Le nombre p(x) de nombres premiers sur un intervalle [0..x] est de l'ordre de x/Ln(x) où Ln(x) est le log népérien de x.
- ?? Ln (2) = 0,69
- ?? Le nombre des habitants est de 6 Milliards $= 3 * 2^{31}$
- ?? $Ln (x^y) = y * Ln (x)$
- ?? On suppose que les nombres premiers sont uniformément répartis pour les questions 1,2, 3 et 4.

1) Définir le nombre des nombres premiers pour les intervalles $[0..2^{512}]$ et $[0..2^{513}]$ (0,25 point)
2) Définir le nombre premiers pour l'intervalle $[2^{512}..2^{513}]$ (0,25 point)
3) Définir le nombre de combinaisons possibles pour N (Ne pas oublier que p < q). (1 point)
4) Conclure sur la possibilité que chaque habitant de la terre peut oui ou non obtenir une bi-clé RSA unique (1 point).
5) On définit la densité d(x)des nombres premiers sur un intervalle [0..x] par p(x)/x. Définir la limite de d(x) quand x tend vers l'infini (0,5 point) (Phénomène de raréfaction des nombres premiers).
6) A partir de la limite trouvée de la densité, déduire que dans le cas de l'utilisation théorique de clés RSA de taille infinie, le RSA devient globalement faible(1 point).