REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ D'ALGER 1 - BEN YOUCEF BEN-KHEDDA
FACULTE DES SCIENCES
DEPARTEMENT MATHEMATIQUES ET INFORMATIQUE

Spécialité : Ingénierie des Système d'Information et Logiciel (ISIL) **Module :** Sécurité des SI
Année : 2018-2019 **Durée :** 01h30

Corrigé Modèle de l'Examen Semestriel

Partie cours : (05.5 points)

I. Choisissez la bonne réponse (QCS)

1.Pour chacun des scénarios suivant, choisir le type d'attaque correspondant

a. un programme qui rendre tous les fichiers en raccourcis : Virus 0.5pts
b. lorsque Bob a cliqué sur le lien reçu dans le mail, son mot de passe est envoyé à Alice : Spoofing 0.5pts
c. les étudiants refusent d'entrer dans le cours et restent au couloir : Denie de service 0.5pts

2. dans chacun des configurations suivantes, calculer la disponibilité du système et choisir la bonne réponse sachant que le système se compose de 6 serveurs dont leurs disponibilités sont respectivement S1=90%, S2=95%, S3=93%, S4=88%, S5=99%, S6=75% (le signe // désigne 'en parallèle' et le signe – désigne en série)

a. S1-(S2//S3//S4) - (S5//S6): 88% 0.5pts
b. (S1//S2) – (S3//S4//S5) – S6: 75% 0.5pts
c. (S1//S2//S3) – (S4//S6) – S5: 95% 0.5pts

II. Questions

1. L'administrateur veut choisir l'une des deux stratégies de mots de passe :
   - Combien y a-t-il de mots de passe possibles pour chacune des politiques ?
   - Donner deux exemples de mots de passes pour chaque stratégie

a. Minimum 5 caractères, maximum 8 caractères, lettres majuscules, minuscules et chiffres :
Lettres majuscule=26 lettres minuscules=26 chiffres= 10 => 62 valeurs possibles pour chaque caractère => $62^5 + 62^6 + 62^7 + 62^8$ mots de passe possibles 0.25 pts
Exemples : n2AG8 et Kl239dFF 0.5 pts

b. Minimum 4 Maximum 10 : lettres majuscules, minuscules, chiffres, et 15 caractères spéciaux
Lettres majuscule=26, lettres minuscules=26, chiffres= 10, 15 caractères spéciaux => 77 valeurs possibles pour chaque caractère => $77^4 + 77^5 + 77^6 + 77^7 + 77^8 + 77^9 + 77^{10}$ mots de passe possibles 0.25 pts
Exemples : 22#bdF et 1dB(C8@ 0.5 pts

2. effectuer une comparaison en terme de principe, avantage et inconvénients entre le modèle DAC et modèle MAC ? 1 pts

MAC	DAC
- Une seule entité qui contrôle les droits d'accès	- Chaque entité contrôle les droits sur ses propres objets
- Sécurité sûr contre les erreurs	- Problème de gestion et des erreurs
- Lourd en terme d'implémentation	- Facile à implémenter
- Protège la confidentialité	- Protège l'intégrité

Exercice 1 (14.5 points)

Soit le système d'information d'une banque XXX.

Partie I : analyse des risques

1. Pour chacune des ressources suivantes, identifier une menace, une vulnérabilité et une attaque possible sachant qu'on ne connaît rien sur l'entreprise. 3pts (0.25 x 12)

Ressource	**Menace**	**Vulnérabilité**	**Attaque**
Discours dans couloir	Trop parler	Donner mot de passe	Ingénierie sociale
Réseau informatique	Pannes matériel	Circulation des données non chiffrées	Sniffing réseau
Système d'exploitation	Matériel non compatible	Bugs logiciels	virus
Portes de bureaux	Portes en bois (incendie)	Laisser les portes ouvertes	Vole des documents

Partie II : base de données et contrôle d'accès

Les dirigeants de la banque désirant informatiser leur système. Pour cela, ils utilisent la base de données décrites en modèle relationnel suivant :

Client (IDClient, nom, n_compte, adresse, mail, n_tel)
Employeur (IDEmp, nom, adresse, mail, n_tel, poste)
Compte_emp (IDEmp, username, password)
Transaction (IDtrans, IDClientEnv, IDClientRec, IDEmp, montant, date, etat, observation)
Offre (IDOffre, titre, type, description, dateDebut, dateFin)

La politique de sécurité de la banque est stricte et souveraine. Ils utilisent une politique MAC dont seulement le directeur qui est chargé de changer les droits d'accès. Les utilisateurs du système sont classés comme suit :

Directeur : qui a l'accès à la table client par lecture, les tables employeur et offre par tous les droits, la table transaction par lecture et modification.

Employeur : qui est chargé de gérer les différentes transactions. L'employeur peut changer son propre mot de passe et username de la table compte_emp, et il peut créer une nouvelle transaction ou modifier une transaction existante ou même consulter le contenu de la table, ainsi qu'il peut créer une offre, modifier une offre existante ou supprimer une offre et même consulter les offres existantes. Aussi, l'employeur peut ajouter, modifier ou supprimer un client de la table.

Administrateur informatique : celui-là est un **employeur** qui est chargé de créer les comptes d'employeurs après recrutement.

Client : qui a le droit de consulter les offres existantes.

2. Donner la matrice de contrôle d'accès correspondantes à ce système 3.25 pts (0.25 x 13)

	Client	**Employeur**	**Compte_emp**	**Transaction**	**Offre**
Directeur	Select*	All*		Select*, update*	All*
Employeur	Insert, update, delete		Update (password, username)	Select, insert, update	Select, update, insert, delete
Admin_info	Insert, update, delete		Update (username, password), insert	Selectn insert, update	Select, update, insert delete
Client					select

Remarques : - modèle MAC avec directeur responsable ce qui veut dire que c'est le seul qui a des '*' (chaque case manque d'un * sera considérée comme fausse)

- All et 'select, update, insert, delete' n'est pas la même chose
- Chaque case est notée sur 0.25 donc la moindre erreur signifie un 0 sur la case

3. Donner les requêtes SQL d'octroi de droits permettant de remplir la matrice 3.75 pts (0.25 x 15)

Grant select on client to directeur with grant option

Grant all on employeur to directeur with grant option

Grant select, update on transaction to directeur with grant option

Grant all on offre to directeur with grant option

Grant insert, update, delete on client to employeur

Create view V1 (user, pass) as select username, password from compte_emp

Grant update on V1 to employeur

Grant select, insert, update on transaction to employeur

Grant select, update, insert, delete on offer to employeur

Grant insert, update, delete on client to admin_info

Grant update on V1 to admin_info

Grant insert on compte_emp to admin_info

Grant select, insert, update on transaction to admin_info

Grant select, update, insert, delete on offer to admin_info

Grant select on offre to client

4. Pour la table compte_emp, les mots de passe doivent être sécurisés. Donner la méthode exacte de stockage des mots de passe.

La méthode exacte pour le stockage est de le concaténer avec le username, hasher le résultat puis chiffrer le tout et stocker le résultat final 0.75 pts

Après un certain temps, la banque a connu un succès remarquable ce qui a exigé de changer sa structure en introduisant le poste de chef de service qui sera chargé de gérer les droits d'accès aux tables afin d'aider le directeur dans son travail.

5. Donner les requêtes SQL permettant d'attribuer les droits d'accès à l'utilisateur chef de service 1pts (0.25 x 4)

Grant select on client to chef_serv with grant option

Grant all on employeur to chef_serv with grant option

Grant select, update on transaction to chef_serv with grant option

Grant all on offre to chef_serv with grant option

6. Donner la nouvelle matrice de contrôle d'accès 1 pts (0.25 x 4)

	Client	Employeur	Compte_emp	Transaction	Offre
Directeur	Select*	All*		Select*, update*	All*
Chef_serv	Select*	All*		Select*, update*	All*
Employeur	Insert, update, delete		Update (password, username)	Select, insert, update	Select, update, insert, delete
Admin_info	Insert, update, delete		Update (username, password), insert	Selectn insert, update	Select, update, insert delete
Client					select

Remarques : - chaque requête est notée sur 0.25 donc la moindre erreur (grant option manquante ou grant option de plus ou droit manque ou de plus) sera notée en 0

Partie III : cryptographie

La banque utilise un système de sauvegarde des fichiers log permettant de sauvegarder l'historique des opérations faites chaque jour. Ces informations contiennent les informations liées aux employeurs présents, les transactions faites par chacun d'eux. Les informations de chaque employeur sont stockées dans un fichier appelé « userlog ». Ces fichiers doivent être protégés contre la lecture et seul un nombre limité des utilisateurs peut le lire.

Pour la sécurisation de ces fichiers, les dirigeants de la banque ont été optes d'utiliser l'outils openSSL pour chiffrer les fichiers et les déchiffrer en cas de lecture. Le consultant informatique les a recommandé d'utiliser l'algorithme RSA pour le chiffrement des fichiers et l'algorithme DES pour le chiffrement des clés secrètes RSA.

7. Donner la commande openSSL permettant de générer une clé secrète RSA protégée par une clé secrète DES.

Genrsa –out clé.priv –des 0.5 pts

8. Donner la commande openSSL permettant de générer une clé publique RSA à partir de la clé secrète générée précédemment.

Genrsa –in cle.priv –pubout –out cle.pub 0.5 pts

9. Donner la commande openSSL permettant le chiffrement de fichier « userlog » dans un fichier appelé « securedlog ».

Rsautl –inkey cle.pub –in userlog –out securedlog 0.5 pts

10. Quelle **information** aura-t-il un utilisateur besoin pour déchiffrer le fichier « securedlog ».

L'information qu'un utilisateur aura besoin pour déchiffrer est le passphrase pour utiliser la clé secrête de déchiffrement 0.25 pts