+1/1/60+

TIW4-SSI sécurité des systèmes d'informations

Contrôle Continu Final – session 1

Promotion 2019 – 2020

Ce contrôle contient un questionnaire qui sera corrigé *en partie* automatiquement. Lorsque vous choisissez une réponse, il faut noircir complètement la case correspondante. Les questions faisant apparaître le symbole ♣ peuvent présenter zéro, une ou plusieurs bonnes réponses. Les autres questions de QCM ont une unique bonne réponse. Les questions ouvertes ont un cadre où répondre, il **ne faut pas** noircir les cases de ces questions, juste répondre dans le cadre.

Ne pas toucher aux cases situées tout en haut de la feuille, elles servent à repérer vos copies lors de la correction automatisée. Répondez *uniquement* sur les feuilles de réponses à la fin de la copie. Les documents sont interdits. Durée 1h30.

1 Cryptographie (/16)

On rappelle pour une fonction de hachage h les propriétés suivantes :

Résistance aux collisions il est difficile de trouver m et m' différents tels que $h(m) = h(m')$

Résistante à la seconde préimage connaissant m, il est difficile de trouver m' différent de m t.q. $h(m) = h(m')$

Question 1 (/2) Que signifie l'adjectif « difficile » dans les définitions de la résistance aux collisions et à la seconde pré-image ?

Question 2 (/4) Pour h une fonction de hachage, montrer que la résistance aux collisions implique celle à la seconde pré-image.

Question 3 (/2) Qu'est ce que la *cipher suite* `ECDHE-RSA-AES128-GCM-SHA256` décrit ? Expliquez chaque acronyme.

Question 4 ♣ (/2). on exécute la commande `openssl genrsa -aes256 -out ./out.key 4096`. Quelles réponses suivantes sont correctes ?

- [A] le fichier `./out.key` est signé
- [B] on génère une clef AES
- [C] on génère une paire (de clefs) RSA
- [D] le fichier `./out.key` est chiffré

Question 5 ♣ (/2). La documentation de l'extension `pgcrypto` de PostgreSQL indique que la fonction `digest(data bytea, type text) returns bytea` calcule un *hash* où `type` est le nom de l'algorithme à utiliser. Quelles valeurs sont admissibles pour ce paramètre ?

- [A] `'des'`
- [B] `'sha256'`
- [C] `'md5'`
- [D] `'sha1'`
- [E] `'aes256'`

Question 6 (/4) La documentation de l'extension `pgcrypto` de PostgreSQL indique que les fonctions `crypt()` et `gen_salt()` sont conçues pour le hachage de mots de passe. Plusieurs fonctions de hachage sont utilisables et la documentation indique que certains (dont `'bf'` et `'XDES'`) sont *adaptatives*. Que signifie cet adjectif ? Pourquoi ce besoin pour hacher des mots de passes et pas des fichiers ?

2 L'autorité de certification (/16)

Dans l'unité d'enseignement de Web MIF13 – Web Avançé et Web Mobile – chaque étudiant dispose d'un serveur avec une IP locale de la forme `192.168.75.xyz` sur lequel il a les droits `root` et installe `nginx`. En 2018–2019 les enseignants demandaient par commencer d'exécuter le script suivant puis de configurer HTTPS sur leur serveur.

```
1 openssl genrsa -out ./server.key 2048
2 openssl req -key ./server.key -new -x509 -days 3650 -sha256 \
3         -out ./server.cert -subj "/C=FR/L=Lyon/O=MIF13/CN=192.168.75.xyz"
```

En 2019-2020, les enseignants souhaitent monter une autorité de certification (CA – *Certificate Authority*), l'idée est de pouvoir distribuer à chaque étudiant son propre certificat signé par l'autorité qu'il installera sur son serveur. Pour cela, ce sont les enseignants eux-mêmes qui tirent les clefs privés qu'ils distribueront aux étudiants.

Question 7 (/2) En 2018–2019, quelles sont les étapes que devaient suivre les étudiants pour mettre en place le certificat sur `nginx` après avoir exécuté le script donné ?

Question 8 (/2) En 2018–2019, on suppose que les étudiants ont *correctement* réalisé la mise en place de HTTPS. Quels messages d'erreurs reçoit-on tout de même quand on visite leurs serveurs avec un navigateur ?

Question 9 (/2) En 2019–2020, quelles sont les étapes que devront suivre les étudiants pour mettre en place le certificat fourni ?

Question 10 (/2) En 2019–2020, que devra faire le *visiteur* d'un site étudiant pour ne pas avoir de message d'erreur ?

Question 11 (/2) Les enseignants ont généré le certificat racine de leur CA. Quelles commandes `openssl` ont-ils exécuter ? On ne demande pas *nécessairement* le détail des commandes mais ce qu'elles font.

Question 12 (/4) Quelles commandes `openssl` les enseignants doivent-ils exécuter pour produire les certificats qu'ils distribueront aux étudiant ? On ne demande *pas* le détail des commandes mais ce qu'elles font.

Question 13 (/2) Pour 2020–2021, les enseignants songent à générer des autorités intermédiaires de certification. Quels sont les avantages plutôt que signer les certificats étudiants directement par l'autorité ?

3 Modélisation des droits d'accès (/24)

On donne le schéma de la base de données de gestion des rôles applicatifs d'un logiciel de gestion de documents ci-dessous. L'attribut privilege est une chaine de caractères qui peut prendre les valeurs `owns`, `reads` ou `writes`. Le schéma suit les conventions usuelles (les ensembles d'attributs qui constituent une clef primaire sont soulignés,les clefs étrangères sont préfixées d'une dièse, les « ... » désignent les autres attributs qui ne nous intéressent pas ici).

rbac_role(idRole, ...)
rbac_inherits(#idRoleChild, #idRoleParent, ...)
rbac_perm(#idDoc, privilege, ...)
rbac_ura(#idRole, #idUsr, ...)
rbac_pra(#idRole, #idDoc, privilege, ...)
app_document(idDoc, ...)
app_user(idUsr, ...)

On donne aussi la définition suivante de la vue rbac_ancestors :

```
1  CREATE OR REPLACE RECURSIVE VIEW rbac_ancestors(idRoleChild, idRoleParent) AS (
2      SELECT idRole, idRole
3      FROM rbac_role
4    UNION
5      SELECT idRoleChild, idRoleParent
6      FROM rbac_inherits
7    UNION
8      SELECT rbac_inherits.idRoleChild, rbac_ancestors.idRoleParent
9      FROM rbac_inherits INNER JOIN rbac_ancestors
10       ON rbac_inherits.idRoleParent = rbac_ancestors.idRoleChild
11 );
```

Question 14 (/2) Expliquez ce que calcule la vue rbac_ancestors.

Question 15 (/4) Qu'est ce qui change sur la vue rbac_ancestors selon que la définition de la clef primaire soit l'une des suivantes, expliquez dans chaque cas :

1. rbac_inherits(#idRoleChild, #idRoleParent, ...)
2. rbac_inherits(#idRoleChild, #idRoleParent, ...)
3. rbac_inherits(#idRoleChild, #idRoleParent, ...)

Question 16 (/4) Ecrire une requête SQL qui, pour un utilisateur `$usr` supposé fixé, calcule la liste des documents dont `$usr` est le propriétaire. On prendra bien sûr en compte l'héritage des rôles.

Question 17 (/6) Cette modélisation n'assure pas, par construction, que tout utilisateur qui peut écrire un document peut aussi le lire. Comment faire pour que ce soit le cas ? Proposer trois idées (sans les détailler) de solutions différentes

Question 18 (*/8*) Dans ce logiciel de gestion de documents il existe une notion d'équipe : chaque utilisateur est rattaché à une ou plusieurs équipes et chaque document appartient à une unique équipe. Après reflexion, il s'avère également que la modélisation du privilège `owns` n'est pas satisfaisante et qu'il vaut mieux en faire une relation qu'un attribut de `rbac_pra`. Modifier le schéma de base de données pour prendre en compte ces nouvelles spécifications. Ne donner que les nouvelles relations et celles qui ont changé.

Question 19 (*/8*) Le rôle propriétaire d'un document peut toujours le lire. De plus, un utilisateur membre de l'équipe à laqauelle appartient un document peut aussi le lire. Sur le nouveaux schéma, écrire une requête SQL qui, pour un utilisateur `$usr` et un document `$doc` fixés, détermine si l'utilisateur a le droit de lire le dit document.

+1/5/56+

TIW4-SSI sécurité des systèmes d'informations

Contrôle Continu Final – session 1

Feuille de réponse

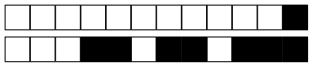
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
8	8	8	8	8	8	8
9	9	9	9	9	9	9

Remplissez le cartouche de la copie-double anonymisée avec nom, prénom, numéro d'étudiant-e et signature puis coller le rabat. **N'écrivez rien d'autre sur la copie-double** elle ne sera pas lue et est utilisée uniquement pour le numéro d'anonymat. Reportez votre **numéro d'anonymat** à 7 chiffres présent sur la copie-double sur le sujet dans la grille ci-dessous. Si votre numéro ne comporte que 6 chiffres, préfixez-le d'un zéro (0).

Question 1 : F J

Question 2 : F I PJ J

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.



+1/6/55+

Question 3 : F J

Question 4 : A B C D

Question 5 : A B C D E

Question 6 : F I PJ J

Question 7 : F J

Question 8 : F J

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.

Question 9 : F J

Question 10 : F J

Question 11 : F J

Question 12 : F I PJ J

Question 13 : F J

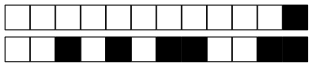
Question 14 : F J

Question 15 : F I PJ J

Question 16 : F I PJ J

Question 17 : F I PJ J

Question 18 : F I PJ J



Question 19 : F I PJ J

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.