

TIW4 SÉCURITÉ DES SYSTÈMES D'INFORMATIONS

Contrôle Continu 1 – durée 45'

Master 2 Technologies de l'Information et Web (TIW)
Promotion 2017 – 2018

Aucun document autorisé, sauf les dictionnaires multilingues. Le barème (sur 40) est indicatif. Les réponses doivent être données sur la feuille. Les réponses aux questions ouvertes doivent être claires et courtes.

Exercice 1 : Généralités et EBIOS (/12)

1. Indiquer la ou les réponses correctes : les articles 323-1 à 323-7 du code pénal répriment :

- L'accès frauduleux à un STAD ;
- Le téléchargement des œuvres numériques en P2P et en streaming ;
- La modification frauduleuse de données d'un STAD ;
- Les atteintes à la vie privée des personnes physiques ;

2. Trouver l'intrus :

- Redondance du matériel ;
- Authentification des utilisateurs ;
- Onduleur ;
- Répartiteur de charge ;

3. Trouver l'intrus :

- Dépenses imprévues ;
- Perte de savoir-faire ;
- Surtension du réseau électrique ;
- Perte de notoriété ;

4. Indiquer la ou les réponses correctes :

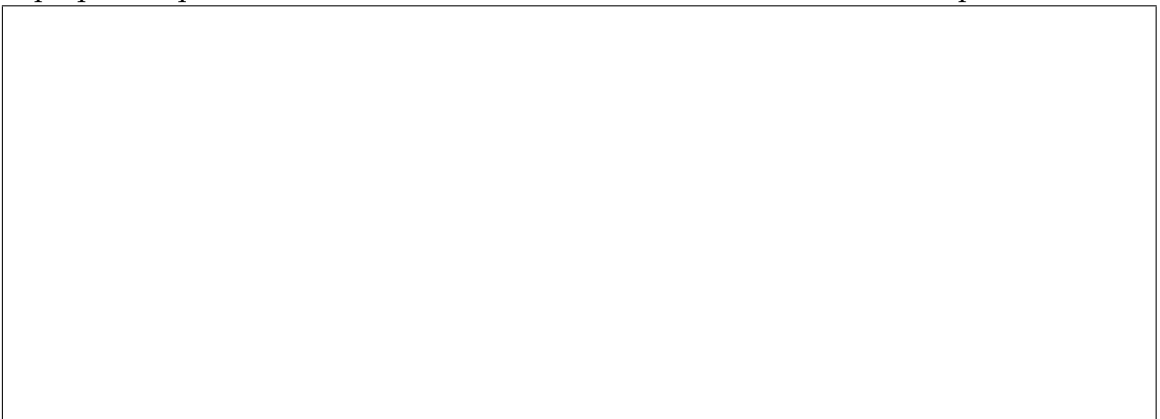
- Il faut *toujours* mettre en œuvre des mesures techniques pour traiter les risques ;
- Les scénarios de menaces concernent les biens essentiels et pas les biens supports ;
- Le risque est le produit d'une gravité et d'une vraisemblance ;
- La prise d'un risque est une façon de le traiter ;

5. Quels sont les *trois* critères traditionnel EBIOS d'évaluation de la sécurité ?

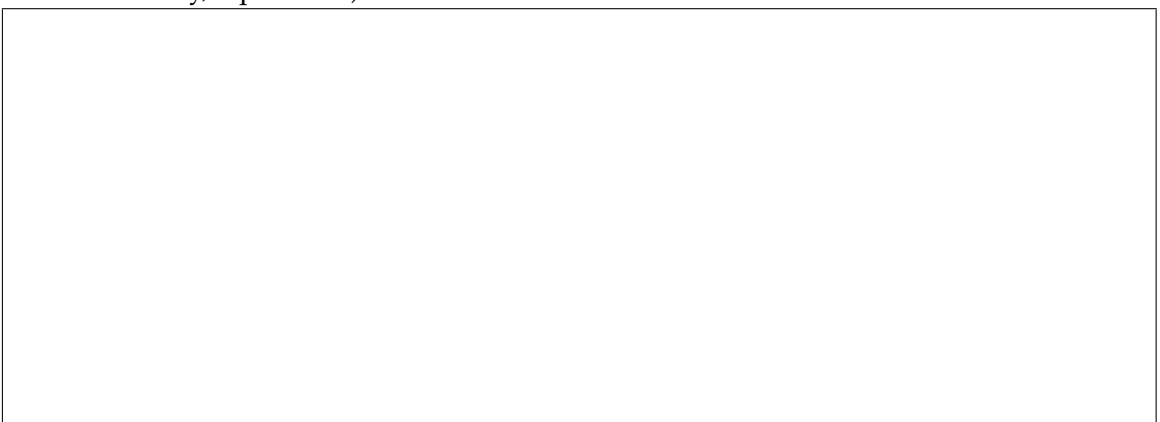
6. Expliquer comment sont classées les sources de menaces *humaines* au sens EBIOS en donnant les différentes dimensions de la classification.



7. Expliquer ce qu'est un *événement redouté* au sens EBIOS. Donner deux exemples :



8. Commenter la formule « Security is not a product, it's a process » (*Bruce Schneier, Information Security, April 2000*)



Exercice 2 : Meltdown et Spectre (/10)

On s'intéresse à l'actualité de la sécurité sur Meltdown et Spectre qui viennent de faire grands bruits. Voici quelques extraits à ce sujet :

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. [...] What are CVE-2017-5753 and CVE-2017-5715? CVE-2017-5753 and CVE-2017-5715 are the official references to Spectre.

extrait de <https://spectreattack.com/>

CVE-2017-5715 : Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVSS Version 3 Metrics :

- Attack Complexity (AC) : High
- Privileges Required (PR) : Low
- Integrity (I) : None

...

extrait de <https://nvd.nist.gov/vuln/detail/CVE-2017-5753>

Speculative execution is an optimization technique where a computer system performs some task that may not be needed. Work is done before it is known whether it is actually needed, so as to prevent a delay that would have to be incurred by doing the work after it is known that it is needed. If it turns out the work was not needed after all, most changes made by the work are reverted and the results are ignored.

extrait de https://en.wikipedia.org/wiki/Speculative_execution

[...] après lecture plus approfondie des documents publiés par Intel et Google, on s'aperçoit que les données attaquables sont celles résidant en mémoire cache de niveau 1 au moment de l'attaque, ce qui est une infime portion de la mémoire de la machine. Le problème réside dans le fait que lors de l'exécution spéculative d'un programme le cache processeur peut charger des données non-autorisés, qui resteront même si l'exécution spéculative n'est pas réellement exécuté et que le contenu du cache peut être observable.

extrait de <http://david.monniaux.free.fr/dotclear/index.php/post/2018/01/09/Retour-sur-quelques-questions-sur-MELTDOWN>

1. Qu'est ce qu'une CVE?

2. Justifier les valeurs des métriques AC, PR et I de la CVE.

3. Il s'agit d'une attaque dite *locale* et par *analyse de canaux-cachés*. Expliquer ce que cela signifie.

4. Donner un exemple d'attaque de lecture *directe* de la mémoire système. Donner un exemple d'impact *important* de ce type d'attaque.

5. Il existe des attaques par canaux-cachés sur l'implémentation des algorithmes de chiffrement qui s'appuient sur l'analyse de la consommation électrique du processeur. Donner un exemple de contre-mesure contre ces attaques.

6. David Monniaux exprime son scepticisme quant à la capacité à accéder à des données sensibles via l'attaque Spectre. Justifier son point de vue.

Exercice 3 : Cryptographie et application (/12)

1. Trouver l'intrus

- md4 ;
- elgamal ;
- sha ;
- md5 ;

2. Indiquer la ou les réponses correctes : la commande `openssl aes-256-cbc -in secret -out secret.enc` calcule un fichier `secret` produit avec

- un algorithme asymétrique ;
- un algorithme de hachage ;
- un algorithme symétrique par flux ;
- un algorithme symétrique par bloc ;

3. Indiquer la ou les réponses correctes : Alice utilise un chiffrement asymétrique, elle perd sa clef privée

- Alice peut toujours chiffrer des courriers qu'elle envoie ;
- Alice peut toujours déchiffrer des courriers qu'elle reçoit ;
- Alice peut toujours signer des courriers qu'elle envoie ;
- Alice peut toujours vérifier la signature des courriers qu'elle reçoit ;

4. `crypt` est le chiffrement historique Unix DES des mots de passes, limité à 8 caractères. Indiquer la ou les réponses correctes : la commande `openssl passwd -crypt -salt 5r bonjour6` produit le résultat `5rtZCdsmrZf86`

- La taille de l'espace des mots de passes de cet exemple est de l'ordre de (36^8) ;
- Le résultat est le même que celui de `openssl passwd -crypt bonjour6` ;
- Le résultat est le même que celui de `openssl passwd -crypt -salt 5r bonjour69` ;
- Sur une machine personnelle contemporaine, on peut hacher environ 10.000 mots de passes par seconde ;

5. Qu'est qu'une attaque dite de « l'homme du milieu » (*man-in-the-middle*) ?

6. Qu'est que sont les attaques à la seconde pré-image d'une fonction h de hachage cryptographique ?

7. Expliquer ce que sont les attaques à clairs connus (*known-plaintext*) et à clairs choisis (*chosen-plaintext*) en décrivant quelles sont la capacités de l'attaquant.

8. Dans le cadre du hachage de mot de passe pour authentification, expliquer ce qu'est le sel et son intérêt.

9. Qui sont Alice, Bob, Eve et Mallory¹ ? Préciser leurs rôles.

Exercice 4 : Un protocole de quorum (/6)

Le conseil du département est composé du directeur de département, 5 professeurs, 5 maîtres de conférences et 2 étudiant. Le directeur n'est pas un des 5 professeurs ni un des 5 maîtres de conférences. Pour que le conseil soit valablement réuni, il faut qu'au moins 3 professeurs, 3 maîtres de conférences et le directeur soient présents, c'est le *quorum*.

Dans l'objectif de dématérialiser les réunions, on désire construire un protocole cryptographique assurant que le *quorum* est bien atteint lors des réunions. Ce protocole sera intégré au système de visio-conférence utilisé par le conseil. On rappelle le fonctionnement du protocole de partage de clé secrète de Shamir pour un schéma de seuil $(k; n)$ et un secret S :

1. Choisir au hasard $(k - 1)$ coefficients a_1, \dots, a_{k-1} ;
2. Construire le polynôme $f(x) = S + a_1x + a_2x^2 + a_3x^3 + \dots + a_{k-1}x^{k-1}$;
3. Choisir au hasard n valeurs v_1, \dots, v_n et distribuer un couple $(v_i, f(v_i))$ à chacun des n participants.

1. https://en.wikipedia.org/wiki/Alice_and_Bob

Proposer un protocole de *quorum* pour le conseil en expliquant qui tire les clefs, qui les reçoit et comment on ouvre une réunion avec votre protocole.