M2-TIW4 sécurité des systèmes d'informations
Contrôle continu final – durée 1h30

Master Technologie de l'Information, promotion 2014 – 2015

Jeudi 18 décembre 2014

Aucun document autorisé. Le barème est indicatif. Ne pas donner de réponses sur le sujet mais uniquement sur la copie anonymisée. La concision, la précision et la clarté des réponses aux questions ouvertes font partie intégrante de l'évaluation.

Exercice 1 : Cryptanalyse (/8)

1. (/2) Classer ces modèles d'attaque de celui où l'attaquant a le moins de pouvoir à celui où il en a le plus et expliquer les différences entre ces modèles :
    1. Attaque à clairs connus (known-plaintext)
    2. Attaque à chiffrés connus (ciphertext-only)
    3. Attaque à clairs choisis (chosen-plaintext)
2. (/1) Le chiffrement de Vigenère est un système à substitution poly-alphabétique qui étend le chiffre de César. S'agit-il d'un chiffrement à flot ou à blocs ? Justifier.
3. (/1) Le chiffrement de Vigenère ne résiste pas à une attaque à clairs connus chiffrés avec le même mot de passe. Expliquer comment retrouver le secret et ainsi casser complètement le code.
4. (/2) Expliquer quelles conditions sur le mot de passe rendent le chiffrement de Vigenère inconditionnellement sûr et en quoi ces hypothèses sont très difficiles à utiliser en pratique.
5. (/1) L'extrait suivant est tiré de `http://www.picsi.org/`, expliquer de quel modèle d'attaque il s'agit :
   « *La cryptanalyse différentielle : le principe général de cette attaque consiste à considérer des couples de clairs X et X' présentant une différence ΔX fixée et à étudier la propagation de cette différence initiale à travers le chiffrement [pour en déduire des bits de la clef].* »
6. (/1) On arrive avec la cryptanalyse différentielle à retrouver la clef utilisée par l'algorithme FEAR-4 avec seulement 8 couples de clairs. Pour DES en revanche on parvient à retrouver la clef en testant de l'ordre de 2^{47} couples de clairs. La clef utilisée par DES est de 56 bits. Peut-on conclure que DES est résistant à cette attaque ou pas ?

Exercice 2 : Modélisation avec les rôles (/8)

On considère la description de l'entreprise *Plâtrerie & Peintures Montiliennes* pour laquelle on va définir une politique RBAC dans une application de gestion.

- Alexandre (A) est un plâtrier qui est aussi quelques fois chef de chantier.
- Bernadette (B) est une électricienne.
- Charles (C) est un apprenti plombier qui est aussi quelques fois attaché de direction.
- Denis (D) est un plombier confirmé.
- Edouard (E) est un apprenti plâtrier et aussi un apprenti électricien.
- Françoise (F) est la chef de l'entreprise et quelques fois électricienne.

A cause de la prolifération de normes et règlements, un ensemble de règle interne définit quelles sont les opérations autorisées sur les chantiers. Les intitulés de permissions à utiliser par la suite sont donnés en *italique*.

- Les plâtriers peuvent poser des revêtement de *sol*, de *mur* et de *plafond*.
- Les électriciens peuvent installer des *câblages* ou des *disjoncteurs* et *tester* les câblages.
- Les plombiers peuvent poser de la *tuyauterie* et des *vannes*.
- Les apprentis peuvent *aider* et peuvent réaliser eux-mêmes quelques tâches :
  - les apprentis plâtriers peuvent poser des revêtements de `sol`,
  - les apprentis électriciens peuvent *tester* les câblages,
  - les apprentis plombiers peuvent poser de la *tuyauterie*.
- Les électriciens et les plombiers peuvent réaliser les *plans* de leurs installations.
- Les chefs de chantier peuvent *superviser* les travaux et *aider* quand nécessaire.
- Les attachés de direction peuvent réaliser les *plannings*, commander les *fournitures* et *facturer* les clients.
- Tous les employés peuvent *consulter* les plans.

1. (/1) Indiquer quels sont, au sens d'EBIOS, les biens essentiels qui apparaissent dans cette étude de cas.
2. (/6) Définir un ensemble de rôle hiérarchisés qui modélise ce problème. On donnera des noms évocateurs aux rôles et on précisera la hiérarchie en la dessinant. Définir les relations User-Role Assignment et Permission-Role Assignment en faisant en sorte que chaque permission soit associée à *exactement* un seul rôle. (*Note : pour respecter cette consigne il faut intégrer quelques rôles techniques qui ne correspondent pas directement à des métiers*)
3. (/1) On désire s'assurer d'une règle de séparation des tâches précisant que *plâtrier, électricien et plombier* sont des fonctions incompatibles. Discuter de la validité de cette règle et de sa réalisation sur le cas d'étude.

Exercice 3 : Droit au déréférencement d'après la CNIL (/4)

Dans son document intitulé *Droit au déréférencement. Les critères communs utilisés pour l'examen des plaintes* la CNIL a établi, avec toutes les précautions d'usage, une liste de critères devant servir à déterminer si un contenu doit ou non être déréférencé d'un moteur de recherche.

1. Les résultats de recherche sont-ils relatifs à une personne physique ? Le résultat apparaît-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ?
2. S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?
3. Le plaignant est-il mineur ?
4. Les données sont-elles exactes ?
5. Les données sont-elles pertinentes et/ou excessives ? Plusieurs sous critères sont ajoutés :
   - Les données sont-elles relatives à la vie professionnelle du plaignant ?
   - L'information est-elle potentiellement constitutive de diffamation, d'injure, de calomnie ou d'infractions similaires à l'encontre du plaignant ?
   - L'information reflète-t-elle une opinion personnelle ou s'agit-il d'un fait vérifié ?
6. L'information est-elle sensible (au sens de l'article 8 de la Directive 95/46/CE) ?
7. L'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ?
8. Le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ?
9. Les informations issues du moteur de recherche créent-elles un risque pour le plaignant ?
10. Dans quel contexte l'information a-t-elle été publiée ? À nouveau plusieurs sous-critères :
    - Le contenu a-t-il volontairement été rendu public par le plaignant ?
    - Le contenu devait-il être public ? Le plaignant pouvait-il raisonnablement savoir que le contenu serait rendu public ?
11. Le contenu a-t-il été rendu public à des fins journalistiques ?
12. La publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ?
13. L'information est-elle relative à une infraction pénale ?

1. (/1) Concernant le critère n° 4, une réponse négative est un argument fort pour que le déréférencement soit autorisé. Expliquer en quoi ce retrait est en cohérence avec la *loi modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
2. (/1) Donner trois exemples d'informations sensibles entendues par le critère n° 6.
3. (/1) La CNIL souhaite permettre le déréférencement de « campagnes de dénigrement » organisées. Parmi les critères précédents, indiquer quels sont ceux qui s'y rapportent le plus particulièrement.
4. (/1) Parmi les critères précédents, indiquer quels sont ceux qui se rapportent directement à la notion de *proportionnalité* de la loi « *informatique et libertés* ».

Exercice 4 : Pot-pourri (/2)

1. (/2) Commenter la citation suivante de Kevin Mitnick du point de vue de la sécurité
   « *Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people.* »