Université de Boumerdes UMBB
Faculté des Sciences
Sécurité Informatique
RIAHLA Med Amine

Série N° 1 : Introduction à la sécurité informatique

Exercice 1

Une entreprise remarque que statistiquement, elle souffre chaque année de cinq infections par des virus et de trois défigurations de son site web. La remise en état des machines après une infection par un virus nécessite deux jours de travail à l'administrateur, soit un coût de 2000 euros. Le site web peut être remis en état en quelques heures, soit un coût de 500 euros. La mise en place et la maintenance d'un produit antivirus et d'un système de protection du site web correspond à un coût annuel de 30000 euros.

1. A partir des coûts ci-dessus, calculer le risque annuel dû aux virus et aux défigurations et juger l'utilité de la mise en place des mesures de sécurité énoncées.
2. Critiquer la manière dont le risque est calculé et proposer une méthode plus adéquate.

Exercice 2

Le niveau réel de sécurité d'un système d'information est toujours inferieur au niveau estimé. De plus, si on ne prend pas de précautions, cette différence de niveau de sécurité tend à augmenter à mesure que le temps passe.

1. Donner deux raisons qui expliquent l'augmentation constante de cette différence de niveau de sécurité.
2. Décrire le genre de mesures à prendre pour éviter une baisse du niveau de sécurité.

Exercice 3

Une entreprise a défini une politique globale de sécurité informatique à l'aide de consultants externes, le moment est venu de l'appliquer. Quelles sont les personnes qui doivent lire les documents suivants :

- Le règlement des utilisateurs
- Le plan de reprise et de continuation
- La politique de sécurité

Exercice 4

1. Expliquer les termes suivants :
   - Niveau de sécurité de base
   - Certification de sécurité
   - Politique de sécurité

2. Indiquer à quel terme de la question précédente se rapporte principalement chacune des références suivantes :
   - IT Grundschutz-Handbuch (GSHB)
   - ISO 17799 (anciennement British Standard 7799);
   - Common Criteria (ISO 15408)

Université de Boumerdes UMBB
Faculté des Sciences
Sécurité Informatique
RIAHLA Med Amine

Série N° 2 : Cryptographie

Exercice 1

Le chiffrement de César prend un texte composé de lettres, et décale chaque lettre d'un nombre constant de positions dans l'alphabet. Ce nombre de positions est la clé.

3. Chiffrer le message suivant avec clé =4 : **CHIFFREMENT DE CESAR**
4. Déchiffrer le message suivant avec clé=5 : **HJHTIJUJZYJYWJHFXXJ KFHNQJRJSY**
5. Montrer qu'il est très aisé de déchiffrer le message suivant sans connaitre la clé : **ZSGAS HWSFG RWBHS FBSH**
6. Est-il plus facile de déchiffrer un texte long ou un texte court ?
7. Que remarquez vous dans le cas où clef =13 ?

Exercice 2

Le chiffrement de Vigenère est une sorte de chiffrement de César amélioré. La clé est constituée non pas d'un, mais de plusieurs décalages. Cette clé est spécifiée sous la forme d'un mot.
Par exemple, la clé « BAC », de longueur trois, spécifie que pour chiffrer un message, on décale la première lettre d'une position (lettre B), la deuxième de zéro positions (lettre A), la troisième de deux positions (lettre C), et ainsi de suite en reprenant la clé au début.
(Les lettres ont une valeur de A=0 à Z=25).

1. Chiffrer le message suivant en utilisant la clé = **SECU :**
   CHIFFREMENT DE VIGENERE
2. Sachant que le message a été chiffré , par la méthode de Vigenère, en utilisant la clé « CRYPTO », quel est le message en clair obtenu en déchiffrant le cryptogramme suivant:
   OFBJESUVAJKWVVGCYCTDYIBEWV
3. Déchiffrer le message suivant chiffré par la méthode de Vigenère avec une clé de longueur 2 (sans connaître la clé)
   OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ
   GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF

Exercice 3

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Le groupe décide d'utiliser un système symétrique de chiffrement.

1. Quel est le nombre minimal de clefs symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique connu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

3. Quel est le nombre minimal de couples de clefs asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées/signées ?
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clef(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique connu**.**

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

6. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Exercice 4

Bob, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clef privée mais dispose encore de la clef publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? En recevoir ?
2. Peut-il encore signer des courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 5

Pour résoudre le problème de l'authentification d'une clef publique, on utilise très souvent la solution des certificats.

1. Qu'est ce qu'un certificat et quelles sont les informations qu'il contient ?
2. Discuter les deux scénarios suivants en termes de sécurité :
   - Deux certificats différents sont signés par la même clef privée.
   - Deux certificats différents contiennent la même clef publique.