Université d'Alger1
Faculté Des Sciences
Département Mathématiques – Informatique
Module : Sécurité des systèmes d'information

Durée : 1h
Licence ISIL - 2020/2021

Solution examen

1. Quelle est le nombre de clés dans un système à clés secrète (pour n utilisateurs) ?
   n (n-1)/2 0.5
2. Quels sont les avantages/inconvénients de la cryptographie asymétrique (à clé publique) par rapport à la symétrique (à clé secrète) ?

Avantage de l'asymétrique : (une de ces réponses)
On peut chiffrer pour quelqu'un sans partager de secret préalable.
Seul le destinataire peut déchiffrer. 0.5
Difficile à déchiffrer (plus sécurisé)

Par contre, est plus lente que la crypto symétrique. 0.5

3. L'algorithme RSA est basé sur un problème calculatoire difficile, lequel ?
   Factorisation des entiers premiers 0.5
4. Le standard de signature DSS est basé sur un problème calculatoire difficile, lequel ? **Logarithme discret** 0.5
5. Soit un message m dont le haché est H(m)=100, générer la signature DSS du message m en spécifiant les clés publiques et privés. On prendra p=467, g=2, a=127, k=213.
   Clé publique (p,g,A)=(467,2,132) 1
   Clé privé a=127 1
   La signature :
   $r=g^k \bmod 467 = 2^{213} \bmod 467 = 29$ 1
   $s=k^{-1}(h(m) - ar) \bmod p-1 = 51 \bmod 466$ 1

   NB. $2^{213} \bmod 467 = 29$ et $2^{127} \bmod 467 = 132$

6. Pourquoi utilise-t-on les fonctions de hachage cryptographiques dans les procédés de signature ?

But : Signer des messages plus longs en garantissant l'intégrité du texte clair. 1

7. Citer trois particularités des fonctions de hachage.
   - **la fonction peut prendre en entrée des données de différentes tailles** 0.5
   - **on ne peut pas retrouver les données d'entrée à partir du haché** 0.5
   - **on ne peut pas trouver deux mots avec le même haché** 0.5
8. Indiquer pour chacun des objectifs de sécurité suivants, par quels moyens ils peuvent être assurés : la confidentialité, l'intégrité et la non-répudiation
   - **Confidentialité (par le chiffrement)** 0.5
   - **Intégrité (par la fonction de hachage)** 0.5
   - **non-répudiation (par les signatures)** 0.5

9. Donner la différence entre vulnérabilité et menace

Menace : un danger externe 1

Vulnérabilité : un défaut interne 1

10. Donner la différence entre : spoofing, sniffing

Le Spoofing : Utiliser l'identité ou l'adresse de la victime (remplacer l'adresse IP de l'expéditeur par l'adresse IP d'une autre machine) 0.5

Les sniffing : capturer des paquets IP transitant sur un réseau de manière transparente pour qu'ils soient ensuite analysés 0.5

11. Qu'est-ce qu'une attaque de déni de service ? citer un exemple.

Une attaque réseau dont le but est d'arrêter un système, bloquer une connexion ou interdire l'accès à une ressource. 1

Exemple : SYNFlooding ou autre 0.5

12. Citer trois avantages de la gestion des risques 1
    - **Avoir un niveau de sécurité qui est parfaitement adapté au contexte et aux risques auxquels on est réellement confronté**
    - **Faire des économies : car on va pouvoir déterminer des mesures de sécurité proportionné aux risques donc moins de dépense**
    - **Contribuer à la conformité aux obligations légales et aux normes et standards internationaux**
13. Donner la différence entre risque initial et risque résiduel

Risque initial : risque évalué avant l'application des mesures de sécurité 0.5

Risque résiduel : risque subsistant après l'application des mesures de sécurité 0.5

14. Donner la différence entre la gravité et la vraisemblance d'un risque

Gravité : l'intensité des effets d'un risque 0.5

Vraisemblance : la faisabilité ou la probabilité qu'in risque se réalise 0.5

15. Remplir le tableau ci-dessous associé à l'exemple suivant :

Un site de e-commerce se dispose d'une base de données clients, présente sur un serveur de son parc informatique et contenant les informations bancaires de ces derniers. Un utilisateur externe a pu accéder à la BD des clients à travers le réseau.

Valeur métier	Bien supports	Evènement redouté	Source de risque et objectifs visés
Information des clients 0.5	**BD du système et le Serveur du site** 0.5	**Fuite des informations des clients** 0.5 **Objectif : confidentialité Impact : financier**	**Un utilisateur externe qui a pour but par exemple récupérer les informations bancaires du client** 0.5