TELECOM Paris - Université Pierre et Marie Curie
Master Réseaux (M2), Examen SECRES

Février 2022, Durée 2h

Documents autorisés

Exercice 1 : (Entropie d'un mot de passe) - 4 points

Pour calculer la force d'un mot de passe, on calcule ce qu'on appelle l'entropie du mot de passe. Elle est définie comme le logarithme en base 2 (log2) du nombre de tentatives nécessaires à trouver un mot de passe avec certitude par le biais d'une attaque brute-force.

Si on choisit **L** éléments qui peuvent avoir **N** valeurs possibles, l'entropie H est calculée donc comme ceci :

H = log2 N^L , dont le résultat est exprimé en bits.

1) Calculer l'entropie d'un mot de passe d'une valise *samsonite* de 3 chiffres. Que signifie le résultat ?

2) Calculer l'entropie du mot de passe Morgane08.

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).

Figure 1. Recommandations de l'ANSSI

Politiques de mot de passe

Les utilisateurs doivent souvent créer leur mot de passe conformément à une politique de sécurité concernant la longueur minimale du mot de passe ou si le mot de passe doit contenir des chiffres ou des caractères spéciaux. Pour simplifier, nous supposons que les mots de passe ont les caractéristiques suivantes :

- Au moins 6 caractères et au plus 8 caractères de long
- Un mot de passe doit être composé de caractères suivants
  - Lettres minuscules a-z (taille = 26)
  - Lettres majuscules A-Z (taille = 26)
  - Chiffres 0-9 (taille = 10)
  - Caractères spéciaux / symboles (taille = 32)

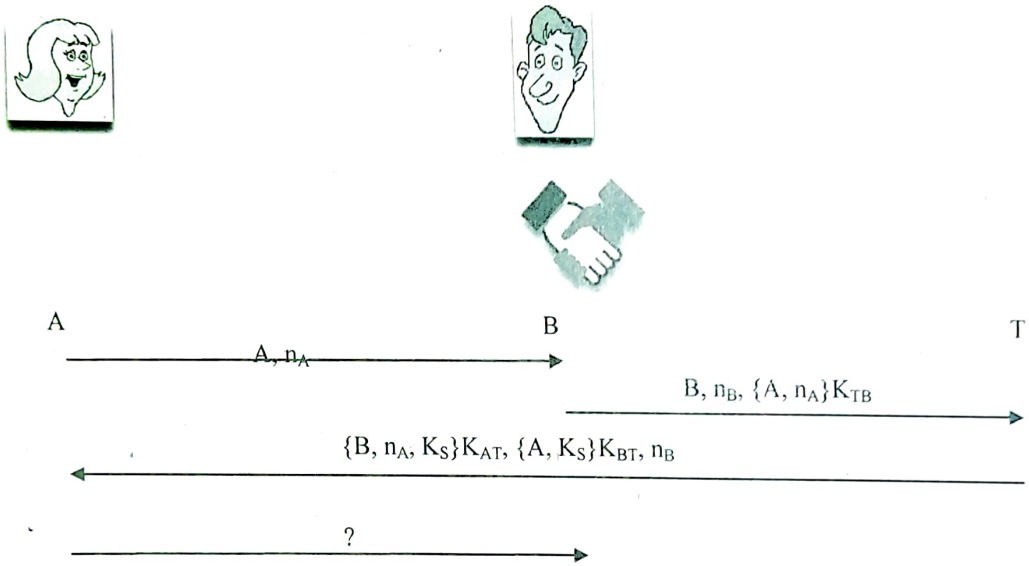
Pour chacune des deux politiques suivantes, calculez le nombre de mots de passe possibles et combien de temps un attaquant aurait besoin en moyenne pour craquer un mot de passe créé selon cette politique. Pour calculer la valeur moyenne, vous pouvez supposer que l'attaquant ne doit tester que la moitié du nombre total de mots de passe possibles pour réussir. L'attaquant utilise une machine capable de tester 2 500 000 (2,5 millions) mots de passe par seconde.

a) Politique 1: "L'utilisateur peut choisir librement son mot de passe."

b) Politique 2: "Le mot de passe doit avoir au moins un chiffre ou au moins un caractère spécial."

Exercice 2 : (Scénario d'authentification) – 2 points

Considérons le protocole suivant dans lequel A et B utilisent un tiers de confiance T pour effectuer une authentification mutuelle et établir une clé de session Ks. Supposons que A et T partagent au préalable la clé symétrique K_{AT} et B et T partagent la clé symétrique K_{BT}. A et B génèrent les valeurs aléatoires n_A et n_B, respectivement. Il y a quatre messages dans le protocole, les trois premiers sont présentés ci-dessous.



a) Quel message A doit envoyer à B dans l'étape 4 pour compléter le protocole ?
b) Si le message à l'étape 2 est remplacé par B, n_B, n_A, {A}K_{TB}, le protocole garde-t-il le même niveau de sécurité ?
c) Si le message à l'étape 2 est remplacé par B, {A, n_B, n_A}K_{TB}, le protocole garde-t-il le même niveau de sécurité ?

Exercice 3 : (Signature RSA) - 2 points

Bob qui a construit un cryptosystème RSA. Les données publiques sont n = 989 et e = 23 les données privées sont p = 23; q = 43.

a) Calculer la signature RSA (sans fonction de hachage) de m = 123.
b) Montrer comment Alice peut vérifier cette signature.

Exercice 4 : (Sécurité avec SSH) - 2 points

Alice tente de se connecter à une machine distante grâce à SSH.

login@machine1 :~> ssh –l Alice machine-distante

Elle obtient le message suivant:

The authenticity of host 'machine-distante (192.168.36.23)' can't be established.

RSA key fingerprint is 3a:1f:23:5e:9c:d4:86:22:33:0d:39:01:28:0b:ea:c5

Are you sure you want to continue connecting (Yes/No)?

a) Expliquez le message et décrire précisément la procédure qu'Alice devra suivre avant de poursuivre la connexion.

b) Est-ce que dans une connexion SSL on obtient le même message ? pourquoi ?

Questions de cours - 10 points

a) Le trafic réseau qui traverse un pare-feu est comparé à des règles pour déterminer s'il doit être autorisé ou non. Expliquer le rôle des règles ci-dessous :

1. *sudo iptables -D INPUT -m conntrack --ctstate INVALID -j DROP*
2. sudo iptables -D INPUT -m conntrack --ctstate INVALID -j REJECT

b) Les performances des IDS sont généralement évaluées à l'aide de leur sensibilité et spécificité. Que signifie la sensibilité d'un IDS ? la spécificité ?

c.) Proposez une mise en œuvre d'une attaque de l'homme en milieu dans un réseau local, en décrivant d'une manière détaillée l'ensemble des échanges entre les équipements (Faire une figure).

d.) Qu'est ce qu'un PKCS (Public Key Cipher System)?

e.) Quel est le rôle d'un certificat X509 en PKI? Expliquer comment vérifie-t-on un certificat dans le cadre d'une connexion TLS.

f.) Dans le cadre des attaques DDoS que signifie un système de défense pour lutter contre ces attaques. Expliquer chaque module de ce type de système.

Bon Courage