Cours-L3-2016

Sécurité Informatique

1. Motivations de sécurité informatique
2. Types de sécurité
    a. Externe
    b. Interne
3. Analyses des risques et préjudices
    a. Définition du Risques
    b. Définition Préjudice
    c. Formule d'estimation du risque
    d. Matrice des risques
4. Politiques de sécurité
    4.1 Définition d'une politique de sécurité
    4.2 Objectifs
        a. Confidentialité
        b. Intégrité
        c. Disponibilité
        d. La non-répudiation
        e. Traçabilité
        f. Identification/Authentification

5. Les normes de la sécurité de l'information
    5.1 La norme ISO 27000
        - ISO 27001 (2005)
        - ISO27002 (2005)
        - ISO 27006 (2007)

    5.2 Les phases de la norme ISO 27000

        a. Phase Plan
        b. Phase Do
        c. Phase Check
        d. Phase Act

6. Les attaques
    a. Les Intrusions (IDS)
    b. Le déni de service (Dos)
7. Les techniques de sécurité appliquées

1**. Motivations de sécurité informatique**

La sécurité informatique est imposée par le fait de :

Partager les ressources matériels et logiciels par différents utilisateurs. Ces utilisateurs sont dispersés et ne se connaissent même pas. L'arrivée des réseaux informatiques et internet compliquent les choses et augmentent la vulnérabilité de l'information.

Elle consiste à :

a. Pour les citoyens, c'est se sentir en sécurité et protéger ses données personnelles et sa vie privée.
b. Pour les entreprises, c'est garantir la disponibilité des fonctions stratégiques et à protéger les données confidentielles en assurant la sécurité des opérations et des informations.
c. Pour les États, c'est protéger les citoyens, les entreprises, les infrastructures vitales et les systèmes informatiques des administrations contre les attaques et la fausse manipulation des données

2. Types de sécurité

La sécurité des systèmes d'information recouvre l'ensemble des moyens techniques, organisationnels et humains mis en place pour établir, conserver et garantir la sécurité des systèmes informatiques (à savoir, Systèmes d'information, réseaux,…)et des données(base de données, données transmises,…)

a. Sécurité Externe

Elle consiste à sécuriser l'infrastructure informatique. La sécurité au niveau des infrastructures matérielles) : salles sécurisées, lieux ouverts au public, espaces communs. La connectivité internet, réseau locaux câblé, réseau sans fil, téléphonie et Réseaux distant

b. **Sécurité Interne**

Ce type de sécurité est lié au contenu de l'infrastructure informatique. Elle consiste à sécuriser : les données, les applications et les services.

3. Analyses des risques et préjudices

En fait toute opération de sécurisation qu'elle soit interne ou externe ; il est important de procéder à une analyse des risques et des préjudices.

Les vulnérabilités d'un système sont au centre des préoccupations car ce sont les failles de sécurité. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non. *Donc c'est le Niveau d'exposition face à une menace dans un certain contexte*.

Cette étape d'analyse se fait grâce à un audit au sein de l'entreprise ou organisme. Elle consiste à étudier avec les utilisateurs l'existant en matériels, logiciels et information et

données. Elle consiste aussi à déterminer les objectifs de la sécurité demandée par les utilisateurs.

L'analyse de risque permet de définir la feuille de route pour sécuriser un système informatique ou numérique.

Définition du risque : Le risque = préjudice *Probabilité de production

Exemple : le risque « être piraté » = perte d'information * 0,5

La perte d'information est le préjudice et la valeur 0,5 est la probabilité. Ceci nous permettra d'évaluer le niveau du risque et de dresser la matrice des risques. Cette matrice est très utile car elle apporte une idée très claire (cartographie des risques) pour mettre en œuvre une politique de sécurité.

Un risque peut avoir trois types de gravité :

Risque critique : les dégâts et préjudices sont très importants et dans quelques cas sans solution (le risque est inacceptable)

Risque majeur : les dégâts et préjudices sont assez important mais on peut trouver des solutions (le risque est moyennement acceptable.)

Risque mineur : les dégâts et préjudices sont acceptables

Exemple de matrice des risques : accéder à la base de données scolarité Univ Annaba.

4 TRES GRAVE	4	5	6	7
3 GRAVE	3	4	5	6
2 MOYENNE	2	3	4	5
1 FAIBLE	1	2	3	4
GRAVITE / FREQUENCE	1 IMPROBABLE	2 PEU PROBABLE	3 PROBABLE	4 FREQUENT

Les cases vertes montrent que le risque est acceptable et la gravité est faible.

Les cases orange montrent que le risque est sont acceptables

Les cases rouges montrent que c'est inacceptable.

Remarques : un risque peu probable peut avoir une gravité extrême.

4. Politique de sécurité

Une politique de sécurité exprime la volonté de protéger les valeurs informationnelles et le ressources informatiques de l'organisation. Elle spécifie les moyens (ressources, procédures, outils, ...). Elle évite que le système ne devienne une cible d'attaques par prise de contrôle à distance.

Cette protection est assurée par Des règles telle que :

- Classification de l'information
- Des outils: chiffrement,
- Firewall
- Des contrats: clauses, obligations
- Enregistrement, identification

La définition de la politique de sécurité doit être

- Simple
- Compréhensible
- Adoptable par un personnel préalablement sensibilisé voire formé
- Aisément réalisable
- De maintenance facile
- Vérifiable et contrôlable
- Elle ne doit pas être statique mais périodiquement évaluée et adaptée
- Elle doit pouvoir être configurable et personnalisable

Après évaluation des risques, elle doit comporter la liste des points à sécuriser suivants :

- Politique de contrôle d'accès: gestion des identités, des profils, ...
- Politique de protection: prévention des intrusions, Déni de service, ...
- Politique de réaction: gestion des crises, des sinistres, intrusion, perte d'information...
- Politique de suivi: audit, évaluation, optimisation
- Politique d'assurance

4.1. Objectifs

a. **Confidentialité :** les données sont incompréhensible ; seul le destinataire désigné ou l'utilisateur autorisé peut accéder aux messages et aux données
b. **Intégrité** : les données ou les messages ne peuvent être modifiés sans que les concernés ne le sachent
c. **Disponibilité :** Assurer à tout moment l'utilisateur peut accéder à l'information ou au service assuré par le système.
d. **La non-répudiation :** preuve qu'une opération a eu lieu, ou qu'un message a été envoyé ou reçu (ainsi, une des parties à l'opération ne peut nier que l'opération a eu lieu)

e. **Traçabilité :** Elle permet avoir une trace sur toute l'activité du système et son fonctionnement afin d'avoir des reprises en cas d'incidents grave.
f. **Identification/Authentification** : preuve que les parties participant à une opération sont bien les personnes qu'elles disent être.

5. Les normes de la sécurité de l'information

Il existe plusieurs normes internationales de gestion de la sécurité informatique. Nous présentons la norme ISO 27000 qui comprend trois produits de sécurité.

5.1 La norme ISO 27000

La famille de normes ISO 27000 aide les organisations à assurer la sécurité de leurs informations. Ces norme facilitent le management de la sécurité des informations, notamment les données financières, les documents soumis à la propriété intellectuelle, les informations relatives au personnel ou les données qui sont confiées par des tiers.

Cette norme concerne essentiellement la gestion de sécurité de l'information. Elle comporte :

- **ISO 27001 (2005) :** ISO/IEC 27001, qui expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI), est la norme la plus célèbre de cette famille. Elle présente les exigences et mesures de sécurité
- **ISO27002 (2005)** : Elle présente les 133 bonnes pratiques à avoir pour assurer la sécurité
- **ISO 27006 (2007) :** Elle concerne la certification.

5.2 Les phases de la norme ISO 27000

a. **Phase Plan :** Durant cette phase on identifie les risques et on rédige un document qui sera une référence pour la gestion de la sécurité en fonction de la politique adoptée.

b. Phase Do : Durant cette phase on met en exécution la politique de sécurité adoptée. Elle consiste à : affecter les ressources nécessaires, former le personnel, appliquer les mesures sécuritaires et identifier les risques résiduels.

c. **Phase Check :** Durant cette phase on procède au control à travers les différents journaux de trafic, d'accès aux bases de données pour analyser et corriger et voire même améliorer la politique de sécurité.

d. **Phase Act :** Durant cette phase passer à l'acte et on peut aussi aller à la **phase Plan.**

6. Les attaques

Les attaques : elles représentent les moyens d'exploiter une vulnérabilité soit par pirate ou machine infectée. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

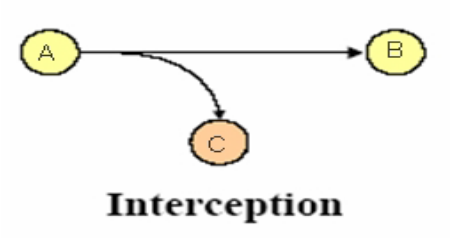
Les contre-mesures : ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).

Les contre-mesures représentent aussi l'ensemble des actions mises en œuvre en prévention d'une menace.

6.1. Les différents types d'attaques

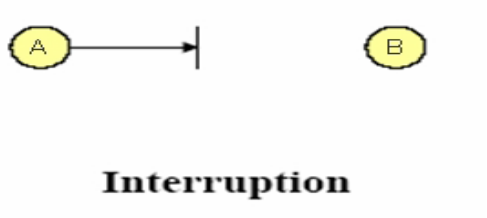
Il existe deux types d'attaques : Attaque Passive et Attaque active.

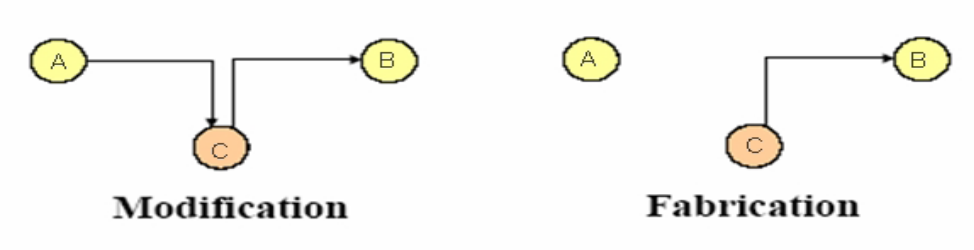
Dans l'attaque passe les informations et services ne sont pas modifiés ou supprimés. Il s'agit d'une écoute et peut être un détournement d'une copie de l'information recherché.



Dans l'attaque active les informations et services sont altérés et engendre des dégâts qui pourraient être irréversibles. A titre d'exemple :

- Formater un disque
- Supprimer des données
- Modifier le profil d'un utilisateur
- Divulguer sur le réseau des informations secrètes.





a- Les Systèmes de détection d'intrusions

Les intrusions dans les systèmes informatiques sont des attaques qui peuvent être passives ou actives. La solution à ces attaques est le développement des IDS « Intrusion Detection Systems).

Ces systèmes aident l'administrateur du réseau ou des applications et leurs bases de données à surveiller les utilisateurs et détecter les utilisateurs non autorisés.
Ils sont basés sur des méthodes d'analyse de composante principales et les « Users List », « Share List » implémentées dans les serveurs d'applications.
Grace aux journaux de l'activité effectuée sur les applications et les journaux des trafics sur les réseaux, l'administrateur est alerté pour mettre fin à l'intrusion.

b- Déni de service (Dos)

Il représente une attaque d'un serveur informatique destinée à l'empêcher de remplir sa fonction.
Exemple 1: envoi au serveur des requêtes généralement mal formées à dessein pour entraîner une réponse anormale et paralysante. L'attaque utilise très souvent une multitude de "PC zombies" travaillant de concert, infectés par chevaux de Troie, et mobilisables à distance.
Exemple 2 : Il est aussi possible de bloquer à distance **des routeurs** en tirant parti de failles de leur software (algorithme de routage).

Une des solutions est limiter le nombre maximal des requêtes adressées au serveur et limiter le nombre maximal les paquets de trafic sur le routeur.

7. Techniques de sécurités appliquées

1. **Signature numérique:** données ajoutées pour vérifier l'intégrité ou l'origine des données.
2. **Notarisation :** utilisation d'un tiers de confiance pour assurer certains services de sécurité.
3. **Contrôle d'accès :** vérifie les droits d'accès d'un acteur aux données ou aux systèmes.

4. **Bourrage de trafic :** données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
5. **IDS :** Système de détection d'intrusion.
6. **Chiffrement :** Algorithme généralement basé sur des clés et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clés.

7.1 Signatures numérique/électronique

La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur. La figure ci-dessous donne le rôle de la signature électronique. La signature numerique peut appartenir à une personne physique ou une organisation morale :

Personne physique : Auteur, Aréateur,…

Organisation morale : Université, Mairie, Entreprise,…..

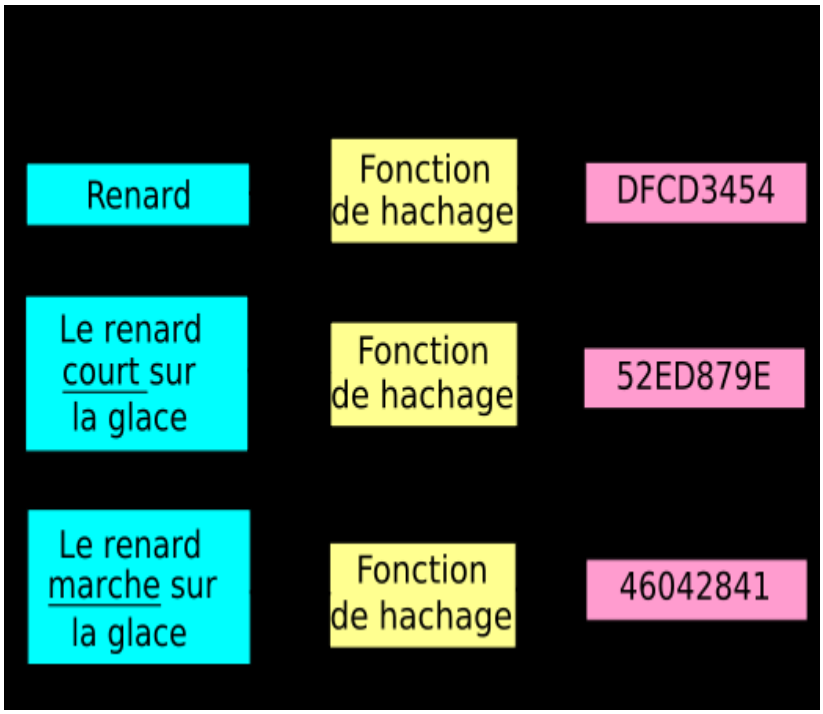
La signature est un « digest » ou un condensé tiré par une technique du document à signer ; dès que le contenu du document change la valeur du « Digest » change.

Elle est appliquée à tout type d'information : Texte, Voix, Vidéo, Image.

Signature = Fonction (document)

Les fonctions les plus utilisées sont : MD5, SHA1, SHA2. Elles sont des fonctions de Hachage. Elles produisent des Digest uniques.

Exemples :



Définition (Fonction de Hachage)

Une fonction de hachage **H** est une application facilement calculable qui transforme une chaine binaire de taille quelconque **t** en une chaine binaire de taille **n**; appelée empreinte de hachage.

X'<> X et H(x') <> H(x)

a- Horodatage des données signées

Il est utile pour assurer une capacité de vérification de la signature électronique dans le temps, si le besoin métier existe. Elle permet aussi de vérifier la durée de vie de la signature.

En effet, l'horodatage d'une information signée permet de fixer un référentiel temps, intégré à la signature électronique sur le plan technique, et permettant ultérieurement de savoir précisément à quelle date (et heure) le signataire a utilisé sa signature. Cette disposition permet ainsi de vérifier la validité de la signature (non expiré / non révoqué) à l'instant de la signature, potentiellement très longtemps après.

b- **Coffres Forts électroniques**

C'est un système d'archivages qui garanti la conservation des signatures et des signatures elles-mêmes

7.2 La Notarisation électronique.

La **notarisation électronique** est la certification des différentes étapes de l'évolution d'un document numérique ou une transaction en vue :

- de permettre lors d'un échange entre deux parties de garantir le contenu, l'origine, la date et la destination du message
- de sauvegarder de façon sécurisée des documents numériques

Elle est représentée par une Autorité de Certification notée (AC). Cette autorité produit :

1. Des signatures électroniques
2. Des clés de cryptographie
3. Des certificats électroniques

a- Les certificats électroniques

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat électronique est en quelque sorte la carte d'identité numérique de la clé publique, dont l'objet est d'identifier une entité physique ou non physique. Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique (Virtuel), délivré par un organisme appelé autorité de certification (souvent notée CA pour Certification Authority).

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

L'Autorité de Certification atteste la véracité des informations contenues, en particulier l'identité de son détenteur. (Elle atteste du lien entre l'identité physique et l'entité numérique).

b-Description du certificat

Un certificat électronique est un document regroupant un certain nombre d'informations décrivant et identifiant de façon sûre une personne physique ou morale, à la manière d'une carte d'identité.

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard X.509 de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond.
- Le numéro de série du certificat.
- L'algorithme de chiffrement utilisé pour signer le certificat.
- Le nom (DN, pour Distinguished Name) de l'autorité de certification émettrice.
- La date de début de validité du certificat.
- La date de fin de validité du certificat.
- L'objet de l'utilisation de la clé publique.
- La clé publique du propriétaire du certificat.
- La signature de l'émetteur du certificat (thumbprint).

Le X.509 est le standard le plus utilisé pour la création des certificats numérique

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification. La clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

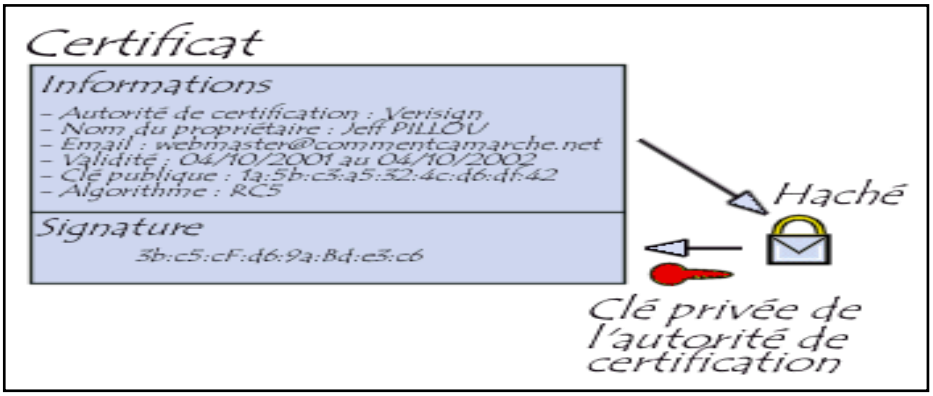


Figure 21: Structure d'un certificat

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.

Les Certificats électroniques sont basés sur des technologies complexes, l'usage d'un Certificat électronique reste toutefois extrêmement simple pour l'utilisateur.

A l'instar d'une carte d'identité traditionnelle qui établit la correspondance entre un visage, un nom et une signature manuscrite, le certificat électronique est un document sous forme électronique

attestant du lien entre les données de vérification de signature électronique (tels que des clés cryptographiques publiques) et un signataire.

c- les types de certificat

Usuellement, on distingue deux familles de certificats numériques :

- les certificats de signature, utilisés pour signer des documents ou s'authentifier sur un site web.
- les certificats de chiffrement (les gens qui vous envoient des courriels utilisent la partie publique de votre certificat pour chiffrer le contenu que vous serez seul à pouvoir déchiffrer).

On distingue différents types de certificats selon le niveau de signature :

- Les certificats auto-signés sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés.

- Les certificats signés par un organisme de certification sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.

d- Le rôle du certificat électronique

Le certificat électronique joue le rôle de pièce d'identité (passeport électronique). Le certificat sur support matériel est un outil d'authentification forte qui peut utilement remplacer tous les processus insuffisamment sécurisés à base de mot de passe.

Le certificat intervient dans les processus d'authentification de l'émetteur et de vérification de la signature. Le certificat électronique peut également servir pour l'authentification dans des fonctions de contrôle d'accès.

Les solutions basées sur le certificat permettent aussi de générer des signatures électroniques pour réaliser sur Internet des transactions sécurisées et authentifiées.

Exemple : accéder à un serveur de banque et faire une transaction.

Ainsi ils sont un outil pour assurer la Sécurité des systèmes d'information :

Les certificats électroniques peuvent être utilisés dans différentes applications informatiques dans le cadre de la sécurité des systèmes d'information pour garantir la non répudiation, l'intégrité et la confidentialité des données et l'authentification forte d'un individu ou d'une identité non physique (Web Serveur…).

Service de sécurité	Utilisation du certificat
Confidentialité	Les certificats permettent de chiffrer et déchiffrer les messages.
Intégrité	Les certificats permettent de signer un message, qui grâce à une fonction de hachage permet de s'assurer que le message n'a pas été altéré.
Authentification	L'utilisation de certificats permet d'établir l'identité de l'expéditeur, de contrôler l'accès à des applications, des sites Internet, des intranets, etc.
Non répudiation	Le certificat permet d'établir qui a participé à l'échange d'informations (serveur, application ou personne). Le dépôt du message signé et éventuellement chiffré chez un tiers notarié permet la non répudiation. Grâce à ce tiers de confiance, l'expéditeur ne peut nier avoir envoyé le message et le destinataire ne peut nier l'avoir reçu.

7.3. Le contrôle d'accès

Le contrôle d'accès est une technique ou ensemble de techniques de sécurité qui nous permet de demander à un utilisateur de fournir des données afin de l'autoriser à accéder à une ressource matérielle et/ou logiciel.

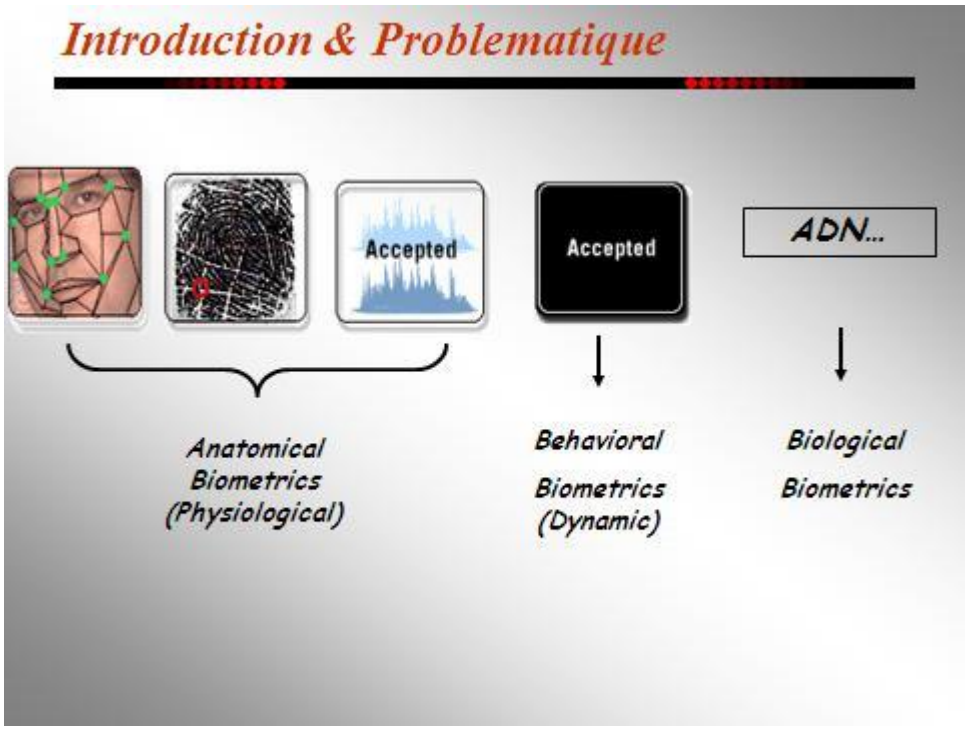
- La plus simple des méthodes est le **Nom de l'utilisateur** et le **Mot de passe**. Elle peut être appliquée à : Un PC, Un réseaux Informatique, Un Fichier, Un Serveur,…..
- **La Biométrie**

  Elle représente le fait de pouvoir mesurer toute information biologique c'est l'homme et les animaux. Elle se base sur le fait plusieurs caractéristiques chez l'homme sont uniques. A titre d'exemple :

  - L'empreinte digitale
  - L'IRIS des yeux
  - La voix humaine.
  - ADN

Elle peut être étendue à la palme de la main, des pieds et autres.

Les mesures biométriques sont exploitées dans le contrôle des accès aux systèmes informatique et autres. Elles sont aussi utilisées dans l'intégrité des données, l'identification et l'authentification.



Le Visage : l'opération consiste à trouver des points particuliers sur le visage scanné avec des méthodes intelligentes.

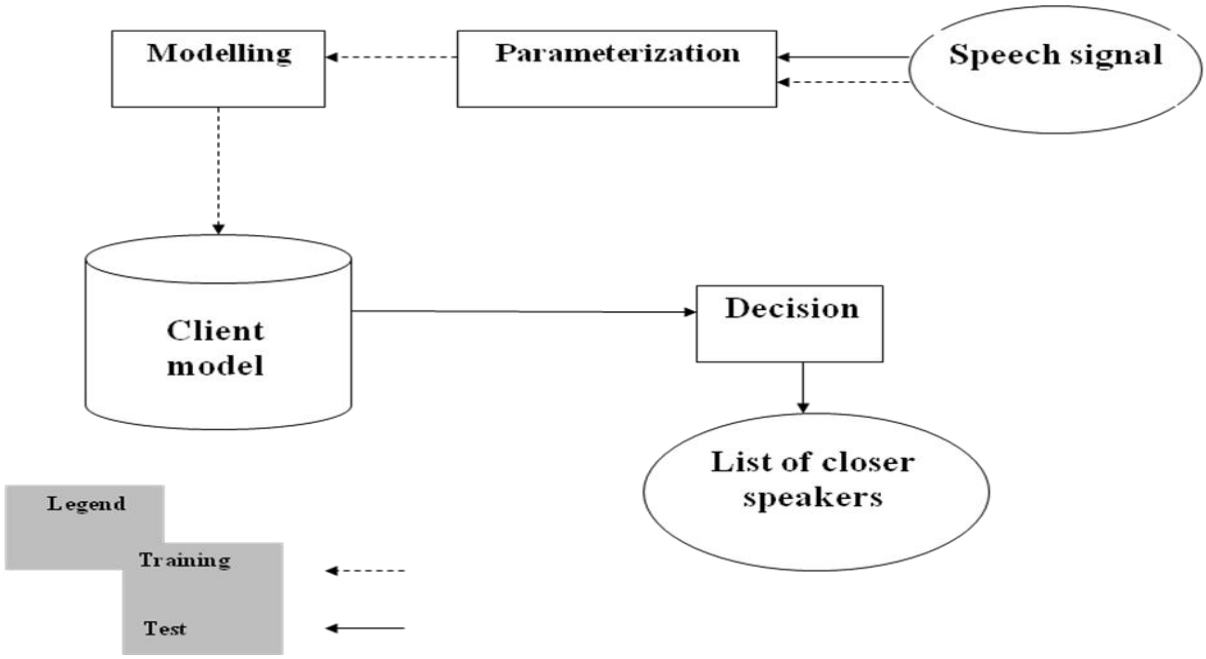
L'empreinte digitale : L'opération consiste à trouver des points particuliers pour représenter d'une manière unique l'utilisateur.

La voix : l'enregistrement de la voix est analysé pour prendre des composantes principales pour représenter l'utilisateur d'une manière unique.

Nous procédons à la représentation de la personne par un vecteur de caractéristiques qui est unique et par la suite nous construisons la base de données qui comprend l'ensemble des utilisateurs. A chaque accès un capteur est activé et le système de construction du vecteur des caractéristiques est lancé. Ainsi nous comparons avec le contenu de la base afin d'autoriser ou pas l'accès. La figure ci-dessous représente un système biométrique basé sur le signal de la voix « Speech Signal ».

La biométrie dynamique : Elle consiste analyser et prendre les composantes principales d'un comportement dynamique d'une personne.

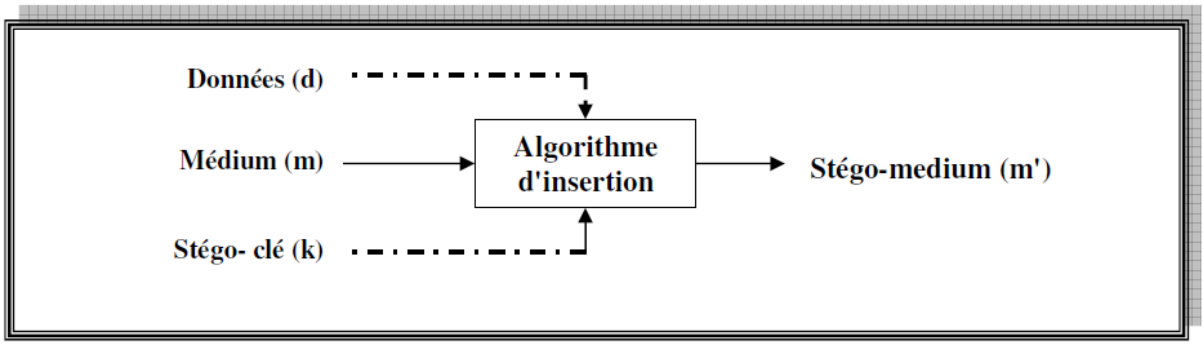
Exemple : La démarche, La posture,…



7.3. **LA STEGANOGRAPHIE**

Le mot Stéganographie vient du mot grec "steganos" qui veut dire "couvert" et du mot "graphein" pour "écriture".

La stéganographie part du principe que la perception humaine n'est pas assez évoluée pour détecter les petites modifications introduites dans les images et les fichiers et sont destinées à renfermer un message caché.

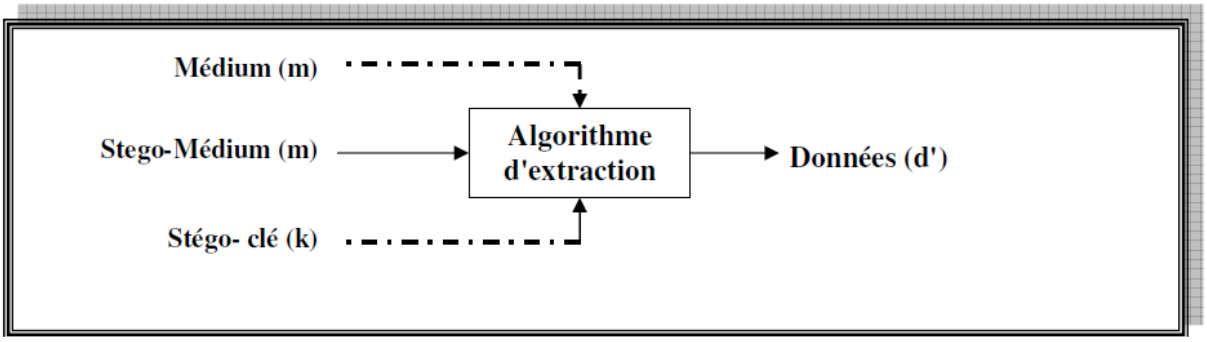


La Stéganographie

Stégano-medium: support S dans lequel le message M est dissimulé.
• Supports physiques divers (bois, peau, papier,…).
• Supports informatiques : sons, fichiers texte, vidéo, images, programmes informatiques, code source,…

Taux stéganographique est une mesure qui nous permet de cacher un message de taille inferieure à à la taille du support. Il est noté S:

S= taille en bits de M / taille en bits de Support



La Stéganalyse

Cette opération est l'opération inverse de cacher. Elle consiste à extraire le message du support.

CLASSIFICATION DES SCHEMAS DE STEGANOGRAPHIE

Le contexte dans lequel se situe un schéma de stéganographie permet de le classer dans une des catégories suivantes:

-Stéganographie à clé secrète

L'émetteur et le récepteur conviennent au préalable d'une clé qui leur sert à insérer puis extraire le message du Stégo-médium.

-Stéganographie à clé publique

L'émetteur et le récepteur possèdent deux clés K' et K. L'émetteur utilise la clé publique du récepteur lorsqu'il souhaite cacher un message dans un support. Le récepteur, pour sa part, extrait le message à l'aide de sa clé privée.

LA méthode de la SUBSTITUTION

Les méthodes classées dans ce groupe remplacent les parties redondantes de la couverture par le message. Les algorithmes sont simples à mettre en œuvre, mais sont vulnérables à des modifications les plus simples. Parmi les nombreuses méthodes de substitution, nous citons le remplacement du least significant bit (LSB-**K)** : bit de poids le plus faible, par le bit du message. La clé K prend la valeur 1, 2, 3,…

Donc :

K=1 on remplace le dernier bit
K=2 on remplace les deux derniers bits
K=3 on remplace les trois derniers bits

Exemple

Dissimulation dans une image de type BMP par la méthode LSB-1

Chaque pixel est décrit par 24 bits (trois octets). Ceci représente le médium :

(00100111 11101001 11001000) (00100111 11001000 11101001) (1100100000100111 11101001)

Pour cacher la chaîne de bits qui représente le message:

10000011

On utilise les bits de poids faibles de chaque octet.

(00100111 11101000 11001000) (00100110 11001000 11101000)
(11001001 00100111 11101001)

Les modifications de bits sont imperceptibles au niveau de l'image, du texte ou de la video.