Services de Sécurité

- **Confidentialité**

  Les données ne sont connues que des tiers autorisés

- **Authentification**

  L'identité des communicants est vérifiée

- **Intégrité**

  Les données n'ont pas été modifiées ou altérées

- **Non-répudiation**

  Les parties impliquées ne peuvent nier leur participation

- **Disponibilité**

  Garantir que les services et ressources demandés restent accessibles

Mécanismes de défense (1)

- **Chiffrement (Cryptage)**

Procédé grâce auquel on souhaite rendre la compréhension de données (chiffrées) impossible à toute personne qui n'a pas le droit (Confidentialité).

- **Signature numérique**

Mécanisme permettant de garantir l'intégrité d'un document électronique et l'authentification de l'auteur ou l'émetteur (par analogie avec la signature manuscrite d'un document papier).

- **Bourrage de trafic**

Données supplémentaires ajoutées à la charge utile (*payload*) pour la confidentialité des données: volume et contenu de la charge utile masquée par le bourrage.

Mécanismes de défense (2)

- **Contrôle d'accès**

Vérifier si une entité (une personne, une machine …) demandant d'accéder à une ressource a les droits requis pour le faire.

- **Notarisation**

La notarisation électronique permet la vérification et l'archivage des preuves d'échanges et d'archivage électroniques par un tiers de confiance agréé (à la manière d'un notaire).

- **Authentification**

Authentifier un nœud : mot de passe, carte à puce, biométrie (empreinte digitale, oculaire ou vocale)…

Mécanismes de défense (3)

- **Protection physique**

Protéger les nœuds physiquement contre tout accès frauduleux. Peut fournir une protection totale mais en risquant d'isoler le nœud.

- **Contrôle du routage**

Sécuriser les routes, les équipements d'interconnexion: routeurs, hub, …… ainsi que les software en relation (protocoles de routage, tables de routage, …)

- **Horodatage (timestamping)**

Mécanisme qui consiste à associer une date et une heure à un événement, une information ou une donnée informatique pour enregistrer l'instant auquel une opération a été effectuée. Très efficace pour la Non-répudiation.

Mécanismes de défense (4)

- **Antivirus**

Une application censée protéger la machine contre des codes néfastes (voir TD1).

- **Pare-feu (Firewall)**

Logiciel ou matériel informatique qui contrôle la politique de sécurité et les accès autorisés ou pas au sein du réseau. Protège des attaques externes et aide à gérer la politique suivie .

- **Détection d'intrusion**

Repère et détecte les activités suspectes sur le réseau et les signale à l'administrateur (dernière partie du cours sera consacrée aux Systèmes de Détection d'Intrusion).

Mécanismes de défense (5)

- **Distribution de clés**

Distribution sécurisée des clés entre les entités concernées et qui nécessite une gestion judicieuse. (Cours crypto avec Alice et Bob :))

- **Certification**

Certificat électronique ou numérique: carte d'identité numérique, utilisé pour identifier et authentifier une personne physique ou morale et pour chiffrer des échanges.

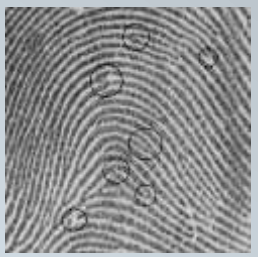
- **VPN (Virtual Private Network) et tunnels**

Mécanisme qui consiste à relier deux réseaux ou sous-réseaux par un tunnel sécurisé.

Mécanismes de défense (6)

un exemple d'authentification: La Biométrie

- **La biométrie**
  - **empreinte digitales**: unique et différentes pour chaque individu



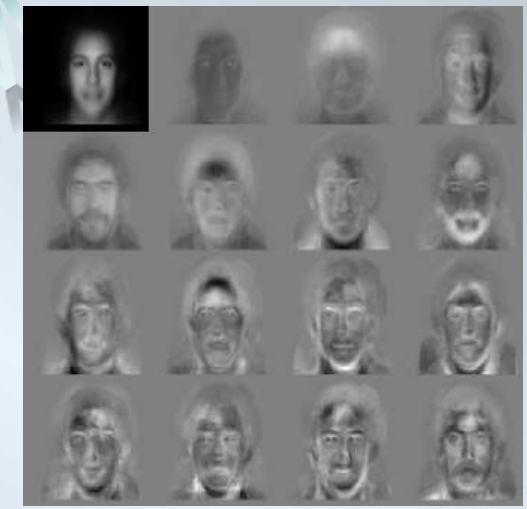
  - **test ADN**: considéré comme intrusion dans la vie privée
  - **géométrie de la main**: forme, longueur, largeur, forme articulations…
    - par imagerie infra-rouge, mais pas complètement infaillible entre jumeaux ou quelques membres de la même famille
  - **Iris (iris-scan):** différents même entre jumeaux et même entre œil gauche et droit

    - nécessite un éclairage restreint et maîtrisé
    - l'œil doit être très proche du capteur pour ne pas induire des erreurs de calculs

Mécanismes de défense (7)

un exemple d'authentification: La Biométrie

- **reconnaissance faciale**
  - plusieurs photos concernant différentes zones du visage (coins de la bouche, haut des joues, distances entre yeux, …)



- **système et configuration des veines**
  - analyser le dessin formé par le réseau des veines sur une partie du corps (en générale la main)
  - peut être combiné avec d'autres solutions biométriques

Mécanismes de défense (8)

(un exemple d'authentification: La Biométrie)

- caractéristiques comportementales
  - **Dynamique de frappe au clavier** (durée entre 2 frappes, taux erreurs, …)
    - méthode très statistique et dépendante de beaucoup de facteurs (type texte, état de l'individu, peut s'habituer à la frappe au travail ce qui augmente la vitesse de frappe…)
      - ⊆ pas très fiable
  - **Reconnaissance vocale**
  - **Dynamique des signatures** (durée, accélération, pression, …)
- techniques en cours de développement
  - géométrie de l'oreille, odeurs, les pores de la peau…
- **inconvénients:** peuvent changer avec le temps (ex: blessure au doigt peut changer l'empreinte digitale)