RES101

Invariants fonctionnels

6. SÉCURITÉ

Authentification

- L'authentification est le mécanisme par lequel une entité prouve qu'elle est bien celle qu'elle prétend être

- Clés
  - Clé secrète / clé publique
  - Clé secrète partagée entre les 2 entités communicantes

- Permet de
  - Authentifier de toutes les parties prenantes à la communication
  - Limiter l'accès à un réseau aux seuls utilisateurs vérifiés

Chiffrement

- Le chiffrement est le mécanisme par lequel des données peuvent être cachées pendant leur transmission sur le réseau
- Il s'effectue grâce à une clé de chiffrement et un algorithme de chiffrement
- Un algorithme de chiffrement n'est pas fiable si on peut retrouver la clé à partir de la lecture de plusieurs messages chiffrés
- Il faut que l'émetteur soit capable de chiffrer et le récepteur de déchiffrer

Intégrité

- La protection d'intégrité sert à vérifier qu'un message n'a pas été altéré au cours de la transmission
- C'est un mécanisme de détection d'erreur
- Attention si quelqu'un est capable de modifier le contenu d'un message, il peut être capable de recalculer les bits de redondance
- Une séquence de hachage (hash) envoyée séparément du fichier permet d'éviter ce problème

Quelques attaques

- **Exemples** :
  - Espionnage
    - L'entité malveillante peut se connecter au réseau
    - Et lit les données qui circulent sur le réseau
    - Soit directement si elles ne sont pas chiffrées, soit après avoir obtenu la clé de chiffrement
  - Man in the middle
    - L'entité malveillante se fait passer pour un fournisseur de services
    - Et intercepte les messages et les retransmet au fournisseur réel de services pour garder l'illusion
    - L'utilisateur lui fournit ses informations délibérément
  - Denial of Service (DoS)
    - L'entité malveillante ou les entités malveillantes peuvent se connecter au réseau
    - Et inondent un fournisseur de service de requêtes
    - Jusqu'à ce que celui-ci soit incapable de répondre aux requêtes des utilisateurs légitimes