Sécurité du réseau

La sécurité

- La sécurité consiste à assurer que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.
- Les principaux objectifs sont :
  - l'intégrité : c'est à dire garantir que les données sont bien celles que l'on croit être ;
  - la confidentialité : seules les personnes autorisées ont accès aux ressources ;
  - la fiabilité : permettant de maintenir le bon fonctionnement du système informatique ;
  - non répudiation, permettant de garantir qu'une transaction ne peut être niée
  - authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressource

- La confidentialité et l'intégrité font appel aux techniques de la cryptographie

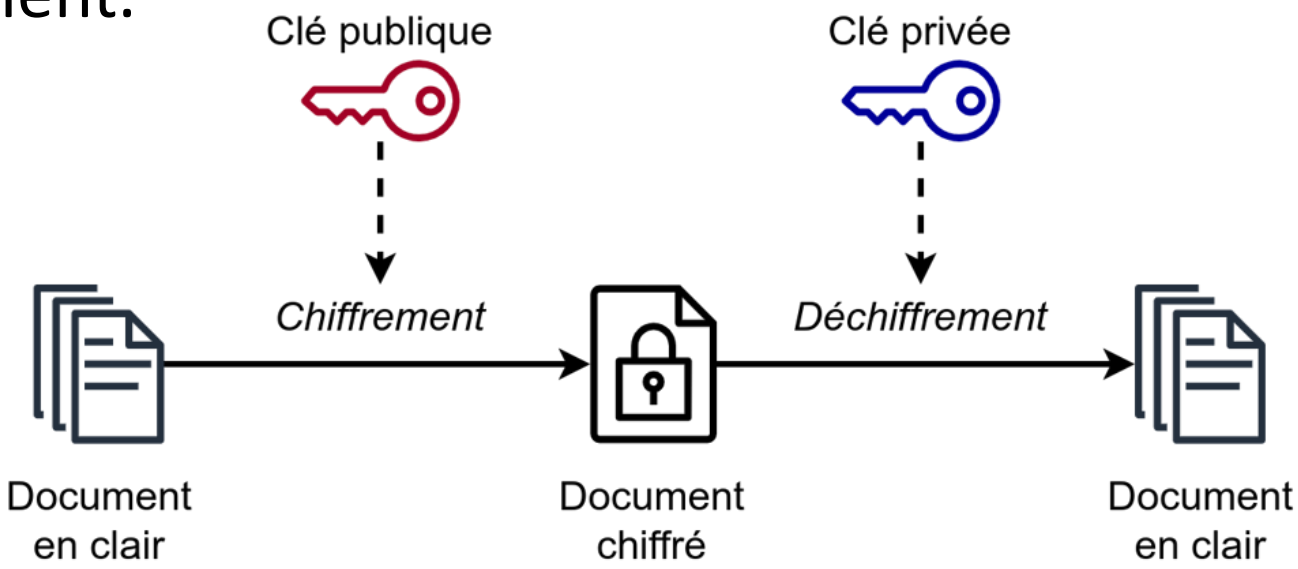
Le rôle de la cryptographie

La **cryptographie** est au cœur de la confidentialité et de l'intégrité :

- **Chiffrement** : protège les données contre la lecture non autorisée (ex. TLS pour sécuriser les communications web).
- **Signature numérique** : garantit l'intégrité et l'authenticité des données.
- **Fonctions de hachage** : permettent de vérifier qu'un fichier n'a pas été altéré.
- **Certificats numériques** : assurent la confiance entre les parties (PKI, SSL/TLS).

Cryptologie, cryptographie, cryptanalyse, quelle est la différence?

- La cryptologie est la science du secret (du grecc kruptos qui signifie. caché).
- Cryptologie = cryptographie + cryptanalyse
- La cryptologie est le domaine global qui regroupe chiffrement et déchiffrement.



Types de clés cryptographiques

Les clés sont utilisées pour chiffrer/déchiffrer les données :

- **Clés symétriques** : une seule clé sert au chiffrement et au déchiffrement (ex. **AES**).
  - Rapides mais nécessitent un partage sécurisé de la clé.
- **Clés asymétriques** : une paire clé publique / clé privée (ex. **RSA, ECC, Ed25519**).
  - La clé publique chiffre, la clé privée déchiffre.
- **Clés de hachage** : utilisées pour vérifier l'intégrité (ex. **SHA-256, MD5**).
  - Ne permettent pas de déchiffrement, mais garantissent que les données n'ont pas été modifiées.
- **Clés de session** : générées temporairement pour une communication sécurisée (ex. **TLS**).
  - Utilisées uniquement pendant la durée de la connexion.

SSH (sécurisation des accès)

•Secure Shell (SSH) est un protocole réseau cryptographique permettant d'exploiter des services réseau en toute sécurité sur un réseau non sécurisé.
•Protocole de couche transport largement utilisé, SSH permet de sécuriser les connexions entre clients et serveurs.
• SSH a été conçu pour remplacer Telnet et les protocoles shell distants non sécurisés qui transmettent des informations critiques, telles que des mots de passe, au format texte brut et sont susceptibles d'être interceptés et
•Le chiffrement utilisé par SSH garantit la confidentialité et l'intégrité des données sur un réseau non sécurisé, comme Internet.

Sécurisation SSH sous Linux

- **Modifier la connexion root** → réduit les risques d'attaque directe sur le compte le plus puissant.
- **Modifier la connexion par mot de passe** → élimine les attaques par dictionnaire ou brute force.
- Modifier /etc/ssh/sshd_config :
  - PermitRootLogin no
  - PasswordAuthentication no
- **Connexion par clé SSH** → sécurité renforcée, car la clé privée reste sur la machine et seule la clé publique est sur le serveur.
- Redémarrer SSH :
  - sudo systemctl restart ssh

Sécurisation SSH sous Linux

- **Générer une clé RSA 3072 bits**
- ssh-keygen -t rsa -b 3072
  - -t rsa → type de clé
  - -b 3072 → taille en bits
- **Générer une clé Ed25519**
- ssh-keygen -t ed25519
  - Plus rapide et plus sécurisé que RSA.
  - Taille fixe (255 bits), mais niveau de sécurité équivalent à RSA 3072/4096.
  - Les clés seront stockées par défaut dans ~/.ssh/id_rsa ou ~/.ssh/id_ed25519

Sécurisation SSH sous Windows

- **Créer une paire de clés**
- ssh-keygen
  - Par défaut, la clé est enregistrée dans :
    C:\Users\<NomUtilisateur>\.ssh\id_rsa (clé privée)
    C:\Users\<NomUtilisateur>\.ssh\id_rsa.pub (clé publique).
- **Protéger la clé privée**
- Ne jamais partager id_rsa.
- La clé publique (id_rsa.pub) peut être copiée sur le serveur distant.

Sécurisation SSH sous Windows

- **Générer une clé RSA 3072 bits**
- ssh-keygen -t rsa -b 3072
- **Générer une clé Ed25519**
- ssh-keygen -t ed25519

Les formes d’intrusions / attaques

- **Spyware**
- Logiciel qui transmet des informations généralement à des annonceurs publicitaires sur l’utilisateur ou ses habitudes sans son autorisation.
- **Spam ou pourriel**
- Courrier non désiré. Il fait l’objet d’envois massifs à des fins commerciales mais aussi d’escroquerie.
- **Malware (logiciels malveillants)**
- Virus, vers, chevaux de Troie, spyware infectent un système pour voler, détruire ou manipuler des données.
- **Phishing**
- Faux emails ou sites imitant des services légitimes trompant l’utilisateur pour obtenir ses identifiants ou données bancaires.
- **Ransomware**
- Logiciel qui chiffre les données et exige une rançon pour les déverrouiller.
- **Attaques par déni de service (DoS/DDoS)**
- Saturation d’un serveur ou réseau par un flot massif de requêtes et rendre un service indisponible.
- **Injection SQL / XSS**
- Exploitation de failles dans les applications web et accéder à des bases de données ou exécuter du code malveillant.

Sécurité informatique

Les moyens de protection

- **Droit d'accès** Ensemble de règles qui définissent qui peut lire, modifier ou exécuter un fichier ou un répertoire. Exemple : permissions NTFS sous Windows ou chmod sous Linux.
- **Cryptage (chiffrement)** Transformation des données lisibles en données codées, accessibles uniquement aux personnes disposant de la clé de déchiffrement. Exemple : chiffrement AES pour protéger des fichiers.
- **Pare-feu (firewall)** Outil matériel ou logiciel qui filtre les communications réseau selon des règles prédéfinies. Il contrôle les flux entrants/sortants pour protéger le réseau interne contre les intrusions.
- **Signature électronique** Mécanisme basé sur la cryptographie qui permet d'authentifier l'auteur d'un document ou d'un message électronique. Elle garantit l'identité et l'intégrité des données.
- **Charte informatique** Document officiel qui définit les règles d'utilisation des moyens informatiques et des réseaux dans une organisation. Elle encadre les droits et devoirs des salariés et protège l'entreprise.
- **Mises à jour** Correctifs logiciels qui comblent des failles de sécurité et améliorent la stabilité. Elles empêchent l'exploitation de vulnérabilités (ports ouverts, services non sécurisés).
- **Anti-virus** Programme qui détecte, bloque et supprime les logiciels malveillants (virus, trojans, ransomwares). Exemple : Windows Defender, Avast.

Analyse réseau sous Linux	Analyse réseau sous Windows (Powershell)
• Vérifier les ports ouverts : • netstat -tulnp • ss -tulnp • Lister les connexions actives : • lsof -i	• Vérifier les ports ouverts : • netstat -ano • Identifier le processus lié : • Get-Process -Id <PID>

Firewall (pare-feu)

- **Parefeu** est un dispositif logiciel ou matériel qui contrôle les flux réseau selon des règles définies.
- Sert a protéger un système ou un réseau contre les accès non autorisés.
- **Exemple** : autoriser uniquement le trafic HTTP (port 80) et HTTPS (port 443).
- Le firewall applique des règles de sécurité qui peuvent inclure :
  - Filtrage par **adresse IP** (source/destination).
  - Filtrage par **port** (TCP/UDP).
  - Filtrage par **protocole** (HTTP, SSH, ICMP…).
  - Filtrage par **état de connexion** (nouvelle, établie, invalide).

Firewall (pare-feu)

- Les pare-feu filtrent le trafic réseau selon des règles prédéfinies. On distingue :
- **Pare-feu de filtrage de paquets** : contrôle basique des adresses IP et ports.
- **Pare-feu à inspection dynamique** : analyse le contexte des connexions.
- **Pare-feu applicatif (proxy)** : filtre au niveau des applications (HTTP, FTP).
- **Pare-feu matériel** : dispositifs dédiés placés en périphérie du réseau.
- **Pare-feu logiciel** : installés sur un poste ou serveur.
- **Pare-feu basé sur l'hôte** : protège une seule machine.
- **Pare-feu périmétrique** : protège l'ensemble du réseau interne.
- **Pare-feu nouvelle génération (NGFW)** : inclut IDS/IPS, filtrage applicatif, inspection SSL

Pare-feu: Filtrer le trafic réseau

- **UFW** :
- sudo ufw enable : Active le pare-feu et commence à appliquer les règles
- sudo ufw status :Affiche les règles en cours (ports autorisés ou bloqués).
- sudo ufw allow 22/tcp : autoriser SSH
- sudo ufw deny 80/tcp : bloquer HTTP
- **iptables** :
- sudo iptables -L -n -v : Lister les règles actuelles avec détails (ports, protocoles, compteurs de paquets)
- sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT : Autoriser SSH (port 22)
- sudo iptables -A INPUT -p tcp --dport 80 -j DROP : Bloquer HTTP (port 80)

Pare-feu: Filtrer le trafic réseau

- **Pare-feu Windows**
- Vérifier l’état :Get-NetFirewallProfile
- Créer une règle :
- New-NetFirewallRule -DisplayName "Autoriser SSH" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow
  - **New-NetFirewallRule** : crée une nouvelle règle dans le pare-feu.
  - **-DisplayName "Autoriser SSH"** : nom lisible de la règle (ce qui apparaîtra dans la liste).
  - **-Direction Inbound** : la règle s’applique au trafic **entrant** (depuis l’extérieur vers ton PC).
  - **-Protocol TCP** : le protocole concerné est **TCP**.
  - **-LocalPort 22** : le port local ouvert est **22**, utilisé par le service SSH.
  - **-Action Allow** : l’action est d’**autoriser** ce trafic (au lieu de le bloquer).

Firewall (filtrage IP)

- **Le filtrage IP est une fonctionnalité du firewall**
- **Sous Linux**
- Bloquer une IP spécifique sous Linux
- sudo iptables -A INPUT -s 192.168.1.50 -j DROP

- # Autoriser une IP spécifique
- sudo iptables -A INPUT -s 192.168.1.100 -j ACCEPT

- **Sous Windows**
- Bloquer une IP
- New-NetFirewallRule -DisplayName "Bloquer IP" -Direction Inbound -RemoteAddress 192.168.1.50 -Action Block

- # Autoriser une IP
- New-NetFirewallRule -DisplayName "Autoriser IP" -Direction Inbound -RemoteAddress 192.168.1.100 -Action Allow

TP1 Génération de certificat sous Windows

1. Générer un certificat auto-signé nommé TestCertificat dans le magasin CurrentUser\My

- New SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject "CN=TestCertificat" -KeyAlgorithm RSA -KeyLength 2048
  - New-SelfSignedCertificate → créer certificat auto-signé
  - CertStoreLocation → emplacement (magasin certificats)
  - CurrentUser\My → utilisateur courant, magasin personnel
  - Subject "CN=TestCertificat" → nom du certificat
  - KeyAlgorithm RSA → algorithme de clé (RSA)
  - KeyLength 2048 → taille de clé (2048 bits)

2. Lister les certificats pour récupérer le Thumbprint TTTT par ex.

- Get-ChildItem Cert:\CurrentUser\My

3. Exporter le certificat en fichier .pfx

- Export-PfxCertificate -Cert Cert:\CurrentUser\My\TTTT -FilePath C:\MonCertificat.pfx -Password (ConvertTo-SecureString -String "MotDePasseFort!" -Force -AsPlainText)
  - -Cert → chemin vers ton certificat (avec son Thumbprint).
  - -FilePath → où tu veux sauvegarder le fichier .pfx.
  - -Password → mot de passe qui protège la clé privée dans le fichier exporté.

TP1 Génération de certificat sous Windows

1. Générer un certificat auto-signé nommé TestCertificat dans le magasin CurrentUser\My

- New SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -Subject "CN=TestCertificat" -KeyAlgorithm RSA -KeyLength 2048
  - New-SelfSignedCertificate → créer certificat auto-signé
  - CertStoreLocation → emplacement (magasin certificats)
  - CurrentUser\My → utilisateur courant, magasin personnel
  - Subject "CN=TestCertificat" → nom du certificat
  - KeyAlgorithm RSA → algorithme de clé (RSA)
  - KeyLength 2048 → taille de clé (2048 bits)

2. Lister les certificats pour récupérer le Thumbprint TTTT par ex.

- Get-ChildItem Cert:\CurrentUser\My

3. Exporter le certificat en fichier .pfx

- Export-PfxCertificate -Cert Cert:\CurrentUser\My\TTTT -FilePath C:\MonCertificat.pfx -Password (ConvertTo-SecureString -String "MotDePasseFort!" -Force -AsPlainText)
  - -Cert → chemin vers ton certificat (avec son Thumbprint).
  - -FilePath → où tu veux sauvegarder le fichier .pfx.
  - -Password → mot de passe qui protège la clé privée dans le fichier exporté.

TP2 détection d'attaques sous Linux

- Créer un nouveau compte utilisateur avec mot de passe de votre choix
- Tenter de se connecter a ce compte en entrant une serie de mots de passes incorrects
- Examiner le fichier de journal d'authentification en utilisant tail avec sudo pour afficher les dernières lignes de /var/log/auth.log (où les événements les plus récents sont enregistrés).
- sudo tail /var/log/auth.log
- Rechercher toutes les lignes contenant "authentication failure"
- créer un script shell **log_monitor.sh** pour **automatiser** ce processus de surveillance