Sécurité Informatique

Protection et mesures de sécurité

F.Z. Filali

Février 25, 2018

Plan

Rappel

- Vulnérabilité : c'est une faiblesse dans la sécurité d'un système informatique qui permet à un utilisateur de faire une action malveillante.
- Menace : c'est une violation d'une ou plusieurs propriétés de sécurité.
- Attaque : c'est une tentative volontaire de violer une ou plusieurs propriétés de sécurité.

Rappel

Menaces :

- Virus
- Ver Informatique
- Trojan
- Spyware, keylogger, sniffer
- Rootkit, backdoor
- Bombe logique
- spam, Hoax, phishing
- ...

Définitions

- Mécanisme de sécurité : un moyen ou méthode de sécurité conçu pour détecter, prévenir et lutter contre une attaque de sécurité.
- Service de sécurité : un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.
  - Confidentialité
  - Disponibilité
  - Intégrité
  - Authentification
  - Non-répudiation

Typologies des mécanismes de sécurité

- Prévention
- Détection
- Recouvrement

Prévention

- Consiste à prévenir l'arrivée des attaques.
- Son objectif étant de faire échouer les attaques.
- Mécanismes :
  - Surêté de fonctionnement : renforcer la qualité du logiciel (méthods formelles, analyse statique, ...).
  - Authentification et contrôle d'accès.
  - Chiffrement et cryptographie.

Détection

- Consiste à détecter l'arrivée des attaques ou des intrusions.
- Mécanismes :
  - Journalisation et audit.
  - Détection d'intrusion.
  - Supervision de sécurité.
  - Contrôle d'intégrité.

Recouvrement

- Consiste à récupérer après l'arrivée d'une attaque.
- Mécanismes :
  - Antivirus
  - Détection d'intrusion avec sauvegarde.

Domaines d'applications des mécanismes de sécurité

Les mécanismes de sécurité peuvent être regoupés selon les domaines suivants :

- Sécurité d'entreprise : gestion des risques et politiques de sécurité.
- Sécurité d'accès : contrôle d'accès, authentification, autorisation, ...
- Sécurité logicielle : anti-virus, pare-feux, IDS, ...
- Sécurité des données : cryptographie.
- Autres.

Sécurité d'entreprise

- Analyse de risques
  - Identifier les ressources à protéger.
  - Identifier les menaces qui pèsent sur ces ressources.
  - Evaluer l'occurence de ces menaces.
- Définition de politiques de sécurité
  - Qui est autorisé à utiliser la ressource et comment?
  - Qui est autorisé à accorder des droits sur la ressource?
  - Qui possède les privilèges de l'administrateur?
- Mise en oeuvre de politiques de sécurité
  - Choix de l'ensemble des mécanismes de sécurité permettant de protéger les ressources de la manière la plus efficace et pour un coût acceptable.

Notions de risques

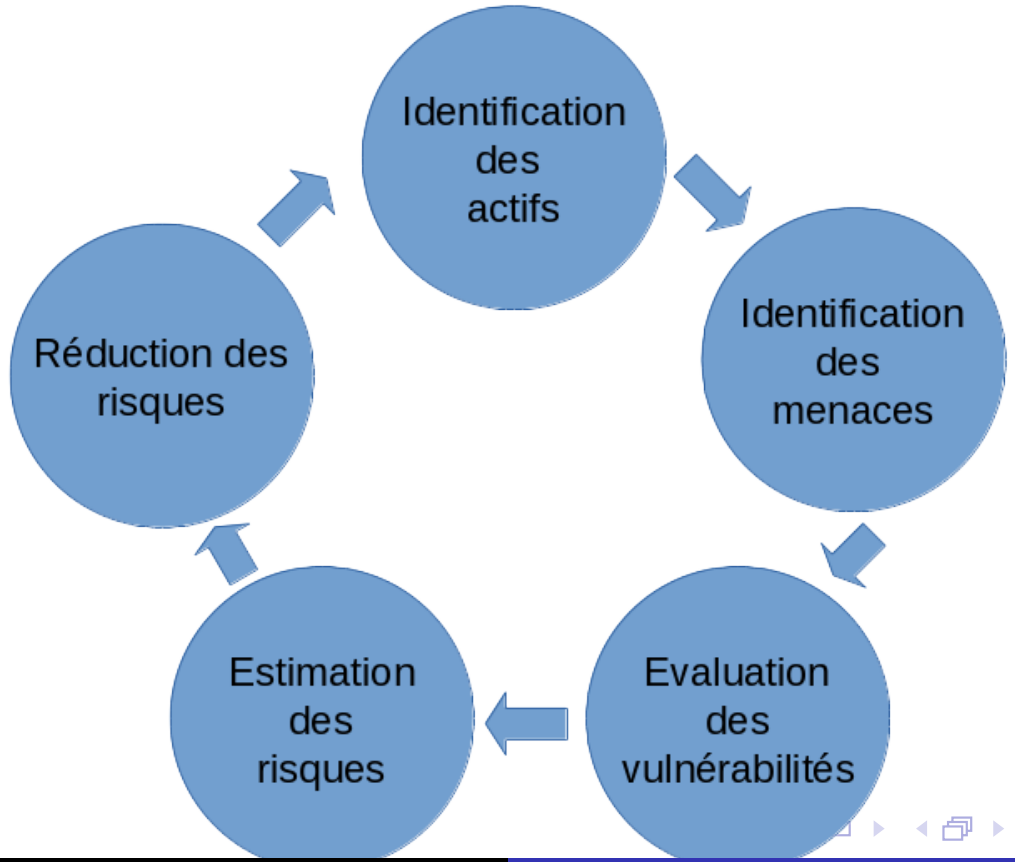
- **Risque** : probabilité qu'une menace exploite une vulnérabilité.
- **Contre-mesure** : Ensemble de moyens et actions mis en oeuvre afin de prévenir les menaces et réduire le risque.
- **Protection** : concevoir, mettre en oeuvre et maintenir des contre-mesures.

Notions de risques

Calcul du risque :

- Basé sur les menaces et vulnérabilités
  - $Risque = \frac{Menaces\ x\ Vulnerabilites}{Contre-mesures}$
  - Conséquences :
    - $+$ *Contremesures* $\rightarrow$ $-$ *risque*.
    - $+$ *Vulnerablites* $\rightarrow$ $+$ *risque*.
- Basé sur l'occurrence de menaces
  - *Risque* = *criteres de securite x occurrence de menaces*
  - Pour le CIA :
    - *Risque* = *Max*(*Confidentialite*, *Integrite*, *Disponibilite*) *x Menace*.

Gestion des risques



Gestion des risques

1. Identification des actifs
2. Identification des menaces
3. Evaluation des vulnérabilités
4. Estimation des risques
5. Réduction des risques

Gestion des risques : Identification des actifs

- Actif : tout ce qui peut représenter une valeur ou un enjeu pour l'entreprise.
  - Actifs primaires : processus, activités, informations, données, ...
  - Actifs de supports : matériel, logiciel, réseaux, personnel, ...
- Faire l'inventaire de tous les actifs dans le périmètre de l'entreprise.
- Donner une valeur à chaque actif répertorié (niveau de sécurié) $\rightarrow$ Valorisation.

Gestion des risques : Identification des menaces

- Les menaces peuvent être :
  - Intentionnelle ou accidentelle.
  - Provenant de l'intérieur ou de l'extérieur.
- Cette étape consiste à enumérer les menaces pouvant affecter les actifs répertoriés
- Se base essentiellement sur l'utilisation d'un modèle de sécurité (CIA, AAA, Parkerian Hexad, ...)

Gestion des risques : Identification des menaces

Exemple :

- Actif : Application qui traîte les paiements de carte de crédit.
- En utilisant le modèle de sécurité Parkerian Hexad :
  - Confidentialité : Si les données sont exposées de manière inappropriée.
  - Intégrité : Si les données sont corrompues, les paiements peuvent être traités de façon incorrecte.
  - Disponibilité : Si l'application tombe en panne, les paiements ne peuvent pas être traités.
  - Possession : S'il y'a une perte des disques de sauvegarde.
  - Authenticité : informations clients non authentiques $\rightarrow$ transaction frauduleuse.
  - Utilitaire : Si des données invalides ou incorrectes sont collectés $\rightarrow$ utilité limitée.

Gestion des risques : Evaluation des vulnérabilités

- Consiste à évaluer et déterminer les vulnérabilités de l'actif selon les menaces identifiées.
- Réduction des menaces répertoriées en examinant les menaces potentielles.

Gestion des risques : Evaluation des vulnérabilités

Exemple :

- Confidentialité : chiffrement des données sensibles. Tests réguliers de l'application par une société externe de tests de pénétration.
- Intégrité : validation avec soin que les données de paiement sont correctes dans le cadre du processus de traitement. Les données invalides entraînent une transaction rejetée.
- Disponibilité : il n'y a pas redondance pour la base de données sur le back-end du système de traitement des paiements.
- Possession : le support de sauvegarde est crypté et transporté à la main par un courrier.
- Authenticité : aucun moyen de garantir que le paiement valide et les informations client appartiennent réellement à l'individu qui effectue la transaction.
- Utilitaire : vérification des numéros de cartes de crédit.

Gestion des risques : Estimation des risques

- Consiste à estimer le risque global en fonctions des menaces et vulnérabilités pour un actif donné,
- Exemple :
  - Actif : Application qui traîte les paiements de carte de crédit
  - Menaces : Intérruption (Disponibilité) : Si l'application tombe en panne, les paiements ne peuvent pas être traités
  - Evaluation des vulnérabilités : il n'y a pas redondance pour la base de données sur le back-end du système de traitement des paiements.
  - Risque estimé : la perte de capacité à traiter les paiements par carte de crédit en raison d'un point de défaillance sur le back-end (base de données) de l'application.

Gestion des risques : Réduction des risques

- Consiste à mettre en place des mesures pour veiller à ce qu'un type de menace soit pris en compte.
- Ces mesures sont appelées contrôles.
- Les contrôles sont divisés en trois catégories:
  - Physique : contrôles qui protègent l'environnement physique dans lequel se trouvent les actifs ou l'endroit où les données sont stockées.
  - Logique et technique : protègent les systèmes, les réseaux et les environnements qui traitent, transmettent et stockent les données. Ils peuvent inclure des éléments tels que les mots de passe, le chiffrement, les contrôles d'accès logique, les pare-feu, les IDS, ...
  - Administrative : sont basés sur des règles, des lois, des politiques, des procédures, des lignes directrices et d'autres éléments de nature "papier".

Politiques de sécurité

- Après évaluation des risques → politiques de sécurité
- Une politique de sécurité exprime la volonté de protéger les valeurs informationnelles et le ressources informatiques de l'entreprise.
- Elle spécifie les moyens (ressources, procédures, outils, ...)

Politiques de sécurité

Cette protection peut être assurée par :

- Des règles: classification de l'information,
- Des outils: chiffrement, firewall, ...,
- Des contrats: clauses, obligations, ...,
- Enregistrement, identification, tatouage, marquage, ...,
- Le dépôt de marques, brevets et protection de droit d'auteur.

Politiques de sécurité

Une politique de sécurité comprend :

- l'organisation de la sécurité.
- l'inventaire des risques relatifs aux actifs
- la définition d'une architecture de sécurité
- l'établissement d'un plan de continuité

Politiques de sécurité

Les domaines à définir dans les politiques de sécurité :

- Politique de Confidentialité,
- Politique de contrôle d'accès: gestion des identités, des profils, ...
- Politique de protection: virus, intrusions, vulnérabilités,
- Politique de réaction: gestion des crises, des sinistres, ...
- Politique de suivi: audit, évaluation, optimisation, ...

Sécurité d'accès

- Définit la mécanismes de sécurité pour l'accès aux données, informations et ressources, ...
- Mécanismes :
  - Contrôle d'accès,
  - Authentification,
  - Autorisation.

Sécurité d'accès : Contrôle d'accès

- Règles et politiques qui restreignent l'accès aux informations confidentielles.
- L'information peut être consultée par ceux qui ont besoin de savoir.

Sécurité d'accès : Authentification

- Moyens pour déterminer l'identité ou le rôle de quelqu'un.
- Authentification = identification + vérification
  - **Identification** = présentation de l'identité. Information non secrète, différente pour chaque utilisateur (nom, numéro, ...), connue (au moins) de l'utilisateur et du système informatique.
  - **Vérification** : vérification de l'identité. L'utilisateur doit présenter :
    - Quelque chose qu'il sait : mot de passe, la date de son anniversaire, son numéro de téléphone, . . .
    - Quelque chose qu'il possède : carte à puce, badge, clé, ...
    - Quelque chose qu'il est : empreinte digitale, iris, voix, . . .

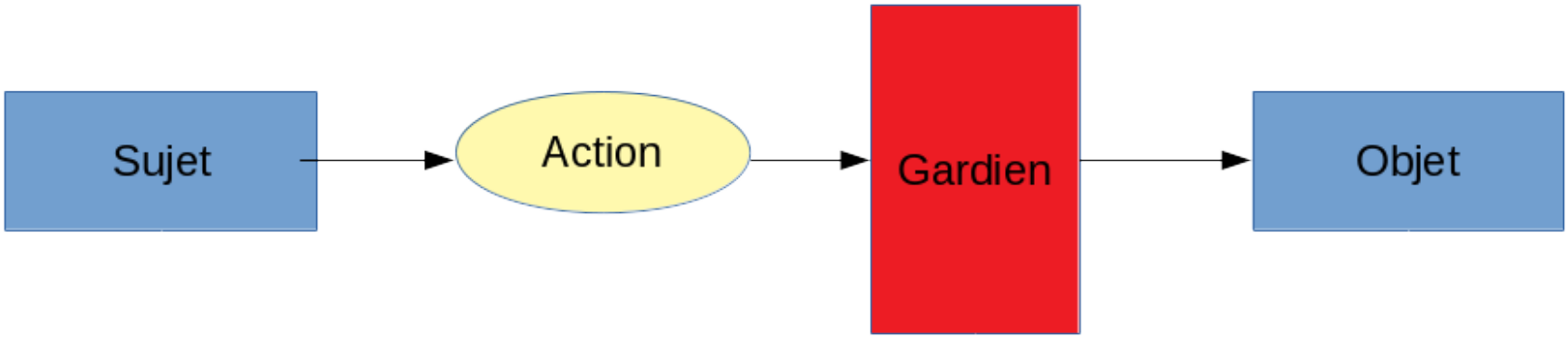
Sécurité d'accès : Autorisation

- Déterminer si une personne / un système est autorisé à accéder à une ressource.
- L'autorisation est basée sur une politique de contrôle d'accès.
- L'autorisation empêche un pirate de tromper le système pour lui permettre d'accéder à une ressource protégée.

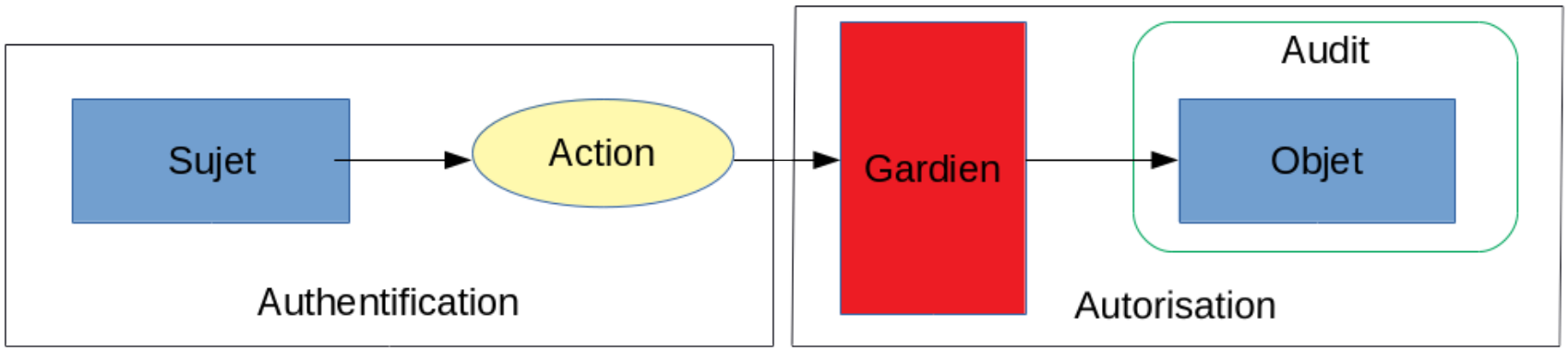
Modèle de Lampson

- Modèle qui met en évidence les relations entre les entités d'un système d'accès aux données :
- Les entités :
  - Sujet : entité pouvant éffectuée des actions (processus, humain, machine, ...)
  - Objet : ressource nécéssitant un contrôle d'accès (données, fichier, dossier, ...)
  - Action : opération effectuée par le sujet afin d'accéder à l'objet
  - Gardien : entité contrôlant l'accès

Modèle de Lampson



Modèle de Lampson



Méthodes de contrôle d'accès

- la caractéristique commune à tous ces modèles de contrôles d'accès est qu'ils se base sur le modèle de Lampson :
  - l'ensemble des sujets S
  - l'ensemble des objets O
  - l'ensemble des droits d'accès R des sujets sur les objets.
- Un modèle de contrôle d'accès sera basé sur l'ensemble des relations sur $S \times O \times R$
- Les différences qui existent entre ces modèles portent sur :
  - les **droits d'accès**,
  - la façon de grouper les sujets/objets et donc les **relations sujets-droits-objets**.

Méthodes de contrôle d'accès : Droits

- le droit de **lecture** : un sujet possédant ce droit peut récupérer l'information contenue dans un objet (par exemple lire un fichier).
- le droit d'**écriture** - un sujet possédant ce droit peut modifier ou ajouter de l'information dans un objet (par exemple écrire dans un fichier).
- le droit d'**exécution** : le droit d'exécution consiste en un droit d'accès qui n'est ni lire, ni écrire (par exemple exécution d'un processus).
- Le droit de **possession**.

Méthodes de contrôle d'accès

- Contrôle d'accès Discrétionnaire (DAC),
- Contrôle d'accès Obligatoire (MAC),
- Contrôle d'accès basé sur les Rôles (RBAC),
- Contrôle d'accès basé sur un Attribut (ABAC),
- Contrôle d'accès Multi-niveaux.

Méthodes de contrôle d'accès : 1. Contrôle d'accès Discrétionnaire (DAC)

- DAC : Discretionary Access Control
- Ce modèle considère que chaque sujet peut détenir un droit de possession sur un objet.
- Ce droit permet à son propriétaire (créateur de l'objet) d'ajouter ou soustraire des droits d'accès pour lui ou pour les autres.
- Exemple : Partage réseau dans les systèmes d'exploitation Microsoft.

Méthodes de contrôle d'accès : 1. Exemple de DAC - Matrice de contrôle d'accès

- Une matrice de contrôle d'accès est une fonction qui donne pour chaque couple (sujet, objet), l'ensemble des droits associés.
- Tout sujet peut avoir le droit de possession sur ces objets.
- Les liens entre ces entités sont capturés dans la matrice d'accès A où les objets sont les colonnes et les sujets sont les lignes.

Matrice de contrôle d'accès

	Fichier 1	Fichier 2	Fichier 3	Fichier4
Personne 1	Lecture Ecriture	lecture	Exécution	
Personne2	Exécution		Lecture	Lecture Ecriture

Méthodes de contrôle d'accès : 2. Contrôle d'accès obligatoire

- MAC : Mandatory access control
- le propriétaire de l'objet ne décide pas qui peut y accéder, mais l'accès est décidé par un groupe ou une personne ayant l'autorité pour définir l'accès aux ressources.
- Souvent implémenté dans des organisations gouvernementales, où l'accès à une ressource donnée est largement dicté par l'étiquette de sensibilité qui lui est appliquée (secret, top secret, etc.).

Méthodes de contrôle d'accès : 3. Contrôle d'accès basé sur les rôles

- RBAC : Role-Based Access Control
- **Rôle** : ensemble de privilèges
- Similaire à MAC, fonctionne sur les contrôles d'accès définis par une autorité responsable plutôt que par le propriétaire de la ressource.
- RBAC est basé sur le rôle que joue l'individu auquel l'accès est accordé.
- Exemple : Dans une application particulière, si un employé dont le seul rôle est de saisir des données, il sera autorisé uniquement à accéder à cette application.

Méthodes de contrôle d'accès : 4. Contrôle d'accès basé sur un attribut

- ABAC : Attribut-Based Access Control
- Il est, basé sur des attributs (propriétés ou caractéristiques).
- Exemple : une voiture ou camion ne doit pas dépasser 6 m pour passer sous le pont.
- Trois types d'attributs :
  - **Les attributs du sujet** : sont ceux d'un individu particulier. Exemple : captcha $\rightarrow$ doit être humain pour passer ce test.
  - **Les attributs de ressource** : sont ceux qui se rapportent à une ressource particulière, telle qu'un système d'exploitation ou une application. Exemple : application qui ne fonctionne que pour un type de navigateur.
  - **Les attributs environnementaux** : peuvent être utilisés pour activer les contrôles d'accès qui fonctionnent en fonction des conditions environnementales. Exemple : accès à une certaine heure..

Méthodes de contrôle d'accès : 5. Contrôle d'accès multi-niveaux

Utilisés lorsque les contrôle d'accès précédents ne sont pas suffisant :

- Le modèle Bell-LaPadula.
- Le modèle Brewer et Nash.

Méthodes de contrôle d'accès : 5. Contrôle d'accès multi-niveaux

Utilisés lorsque les contrôle d'accès précédents ne sont pas suffisant :

- Le modèle Bell-LaPadula :
  - met en œuvre une combinaison de DAC et MAC.
  - Il est principalement concerné par la confidentialité de la ressource en question.
  - Exemple : une ressource est classée comme secrète et un utilisateur qui a un niveau de possession, lui permettant d'accéder à la ressource sous les accès autorisés par MAC.
- Le modèle Brewer et Nash.

Méthodes de contrôle d'accès : 5. Contrôle d'accès multi-niveaux

Utilisés lorsque les contrôle d'accès précédents ne sont pas suffisant :

- Le modèle Bell-LaPadula.
- Le modèle Brewer et Nash :
  - Également connu sous le nom de modèle du mur de Chine,
  - Il est conçu pour prévenir les conflits d'intérêts.
  - Trois classes de ressources principales sont considérées dans ce modèle :
    - **Objets** : ressources telles que des fichiers ou des informations, appartenant à une seule organisation.
    - **Groupes d'entreprises** : tous les objets appartenant à une organisation particulière.
    - **Classes de conflit** : tous les groupes d'objets qui concernent des parties concurrentes.

Méthodes d'authentification : Facteurs

- les facteurs de **connaissances** : quelque chose que l'utilisateur connaît.
- les facteurs de **propriété** : quelque chose que l'utilisateur possède.
- les facteurs d'**inhérence** : quelque chose que l'utilisateur est ou fait.

Méthodes d'authentification : Facteurs

- les facteurs de **connaissances** : quelque chose que l'utilisateur connaît :
  - Mot de passe
  - Code PIN (Personal Identification Number)
  - Réponse à un défi (question de calcul ou culture générale ou pattern, ...
  - Question secrète
- les facteurs de **propriété** : quelque chose que l'utilisateur possède.
- les facteurs d'**inhérence** : quelque chose que l'utilisateur est ou fait.

Méthodes d'authentification : Facteurs

- les facteurs de **connaissances** : quelque chose que l'utilisateur connaît.
- les facteurs de **propriété** : quelque chose que l'utilisateur possède
  - Carte d'identité,
  - Carte à puce,
  - Badge,
  - téléphone portable avec jeton matériel ou logiciel.
- les facteurs d'**inhérence** : quelque chose que l'utilisateur est ou fait.

Méthodes d'authentification : Facteurs

- les facteurs de **connaissances** : quelque chose que l'utilisateur connaît.
- les facteurs de **propriété** : quelque chose que l'utilisateur possède.
- les facteurs d'**inhérence** : quelque chose que l'utilisateur est ou fait
  - empreinte digitale,
  - séquence d'ADN
  - signature,
  - visage,...

Méthodes d'authentification : Authentification par mot de passe

- Mot ou une série de caractères utilisés comme moyen pour prouver son identité et qui doit être tenu secret.
- Représente un point faible car ils doit être retenu par les humains.
- Les utilisateurs choisissent des mots de passe qui sont faciles à retenir ou qu'ils écrivent sur papiers accessibles,...
- Il y au moins 4 points importants pour la sécurité des mots de passe:
  - Comment sont-ils choisis?
  - Comment les mots de passe sont-ils transmis entre l'usager et le vérificateur?
  - Comment l'usager range-t-il son mot de passe?
  - Comment le vérificateur range-t-il les mots de passe?

Méthodes d'authentification : 1. Mot de passe

Liste des 25 mots de passe les plus populaires → les moins sécurisé.

- 123456 (=)
- Password (=)
- 12345678 (+1)
- qwerty (+2)
- 12345 (-2)
- 123456789 (Nouveau)
- letmein (Nouveau)
- 1234567 (=)
- football (-4)
- iloveyou (Nouveau)
- admin (+4)
- welcome (=)
- monkey (Nouveau)
- login (-3)
- abc123 (-1)
- starwars (Nouveau)
- 123123 (Nouveau)
- dragon (+1)
- passw0rd (-1)
- master (+1)
- hello (Nouveau)
- freedom (Nouveau)
- whatever (Nouveau)
- qazwsx (Nouveau)

Méthodes d'authentification : 2. Biométrie

- Il s'agit de systèmes qui identifient une personne en fonction de ses caractéristiques biologiques.
- Ces systèmes balayent les empruntes ou/et les yeux ou/et le visage ou/et la voix :
  - Les caractéristiques physiques sont mesurées et sont ensuite converties sous formes numériques.
- Identification par :
  - Empreintes digitale,
  - Reconnaissance faciale,
  - Reconnaissance de l'iris,
  - Reconnaissance vocale,
  - Analyse comportementale, ...
- Difficulté à reconnaître les patterns et les mesures sujettes au bruit.

Méthodes d'authentification : 3. Multi-facteurs

- Appelée aussi :
  - authentification à deux facteurs dans le cas de deux facteur,
  - authentification forte.
- Elle utilise un ou plusieurs des facteurs précédents.
  - Carte bancaire + code secret
  - Chèque + signature + empreinte dégitale
- OTP (One Time Password): Utilisation d'un mot de passe à usage unique.
  - authentification avec un compte gmail avec mot de passe et OTP par SMS.

Méthodes d'authentification : 4. Authentification mutuelle

- Mécanisme d'authentification dans lequel les deux parties s'authentifient mutuellement.
- Dans l'authentification mutuelle, non seulement le client s'authentifie auprès du serveur, mais le serveur s'authentifie également auprès du client.
- Utilisation de certificats numériques $\rightarrow$ le client et le serveur disposeraient tous deux d'un certificat pour authentifier l'autre.

Méthodes d'authentification : 5. Authentification unique

- Connue sous le nom de SSO (Single Sign On)
- Méthode permettant plusieurs accès en ne procédant qu'à une seule authentification.
- Donne accès à de nombreuses ressources $\rightarrow$ les pertes peuvent être lourdes, elle doit utilisée une authentification forte.
- Exemple : Connexion à des applications mobiles à travers un compte de réseau social (google, facebook, ...)

Anti-virus

- Identifier, neutraliser et éliminer les logiciels malveillants (virus, vers, trojan, ...).
- Données analysées : mémoire, disque dur, échanges avec le réseau.
- Lorsque un anti-virus détecte un virus il va :
  - Supprimer le code malicieux du fichier infecté
  - Placer le fichier infecté en quarantaine
  - Supprimer le fichier infecté

Anti-virus : Méthodes de détection

- Le scanning des signatures.
- Contrôle d'intégrité.
- Analyse comportementale.
- Analyse Heuristique.
- Analyse dynamique.

Anti-virus : Méthodes de détection

- Le scanning des signatures :
  - Recherche et comparaison de la signature du virus à partir d'une base de signatures virales.
  - La signature doit se trouver dans la base $\rightarrow$ mise à jour régulière.
  - Robuste au polymorphisme.
- Contrôle d'intégrité.
- Analyse comportementale.
- Analyse Heuristique.
- Analyse dynamique.

Anti-virus : Méthodes de détection

- Le scanning des signatures.
- Contrôle d'intégrité :
  - L'antivirus maintienne une liste des fichiers exécutables associés à diverses informations (taille, date de création, date de modification, un CRC)
- Analyse comportementale.
- Analyse Heuristique.
- Analyse dynamique.

Anti-virus : Méthodes de détection

- Le scanning des signatures.
- Contrôle d'intégrité.
- Analyse comportementale :
  - Contrôle en continu des activités suspectes (lectures et écritures dans des fichiers exécutables, les tentatives d'écriture dans les secteurs de partitions et de boot du disque.)
- Analyse Heuristique.
- Analyse dynamique.

Anti-virus : Méthodes de détection

- Le scanning des signatures.
- Contrôle d'intégrité.
- Analyse comportementale.
- Analyse Heuristique :
  - détecter les virus avant leur exécution, en cherchant des portions de code suspectes.
- Analyse dynamique.

Anti-virus : Méthodes de détection

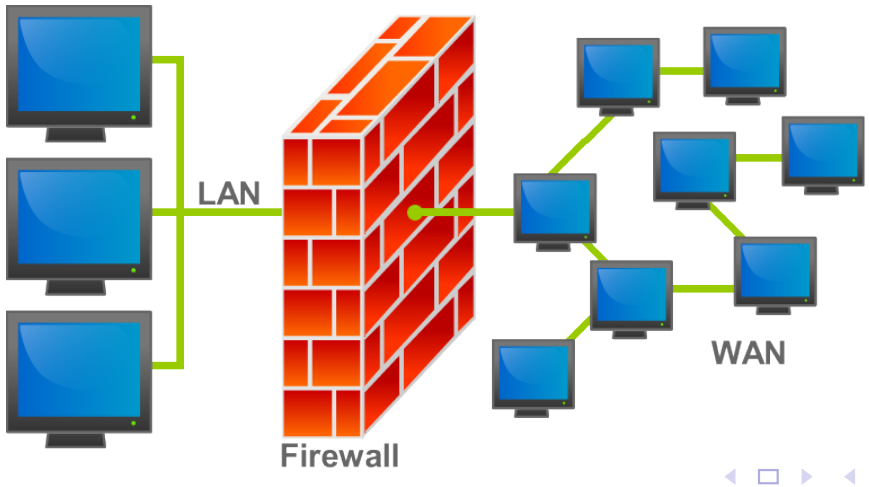
- Le scanning des signatures.
- Contrôle d'intégrité.
- Analyse comportementale.
- Analyse Heuristique.
- Analyse dynamique :
  - Le programme infecté est lancé dans un environnement virtuel (sandbox) pendant un laps de temps
  - Permet de déclencher un comportement suspect afin de détecter le virus.

Pare-feu

- Pare-feu (firewall) : logiciel (intégré à l'OS) ou matériel dédié (serveur ou routeur).
- Il est placé à la frontière entre Internet (ou un réseau externe) et la machine (réseau interne).
- Il filtre les paquets, et si un paquet ne correspond pas aux filtres, le paquet est rejeté.

Pare-feu

- Les règles de filtrage suivent des règles dépendant de :
  - Les adresses IP (source ou destination)
  - Les ports TCP/UDP (source ou destination)
  - Les protocoles (HTTP, FTP, DNS, ...)
  - Les données (couches applicatives)

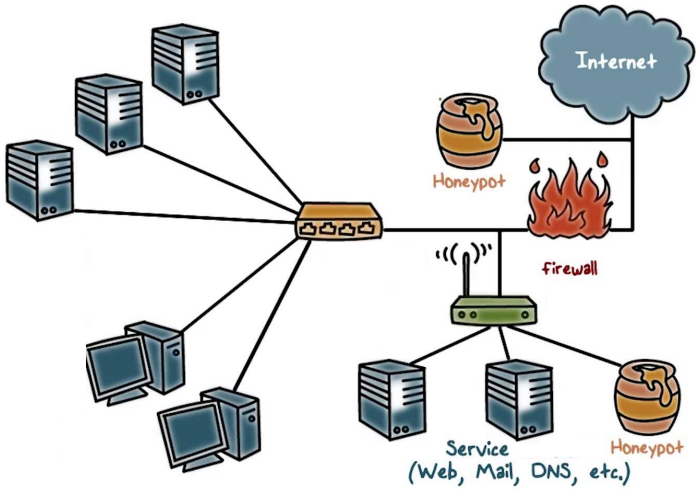


IDS

- Système de détection d'intrusion (IDS : Intrusion Detection System) : Ils sont utilisés pour écouter, et analyser le trafic d'un réseau.
- Deux techniques d'analyse de trafic :
  - Approches par scénarios ou signatures d'attaque :
    - Modèles d'attaque (bases de signature = symptômes d'attaques dans les activités observées).
    - Alerte si présence de symptômes.
  - Approche comportementale :
    - Modèles des comportements légaux.
    - Alerte si activité observée hors des comportements normaux.
- IPS : Système de prévention d'intrusion : analyse et rejet de paquets.

Honeypots

- Un honeypot "pot de miel" est un système de receuil d'informations sur les utilisations illicites et non autorisées de ce système.
- Il ne cherche pas à détecter ou prévenir une attaque particulière.
- Il sert à déterminer les méthodes d'attaques : un système accessible par les pirates, la plupart du temps dépourvue de toute protection.



VPN

- Réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN)
- Permet de se connecter de bout en bout à travers un réseau publique de façon sécurisée.
- Un VPN repose sur un protocole de tunnelisation qui permet aux données passant d'une extrémité à l'autre d'être sécurisées par des algorithmes de cryptographie.

Sécurité des donnée

Mécanismes :

- **Chiffrement** : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- **Signature numérique** : données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Distribution de clefs** : distribution sécurisée des clefs entre les entités concernées.

Autres mécanismes

- La protection physique : peut fournir une protection totale, mais qui peut être excessive (défense en profondeur)
- Bourrage de trafic : données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- Notarisation : utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- Journalisation ("logs") : Enregistrement des activités de chaque acteurs. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- Analyse des vulnérabilité ("security audit") : identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu.

Conclusion

- La sécurité à 100% n'existe pas.
- Aucun mécanisme de sécurité ne suffit par lui-même.

Questions?