Cours Sécurité des Systèmes Informatique Support de Cours pour Sécurité des Systèmes d'Informations

Abderrahim Sebri

Cours Sécurité des Systèmes Informatique

Support de Cours pour Sécurité des Systèmes d'Informations

Année Universitaire 2022-2023

Dr. SEBRI Abderrahim
Université de SAVOIE - FRANCE

SOMMAIRE

A propos du Document

Utilisation du document	
Un historique des versions de ce document est conservé en cas de modifications importantes de la portée nécessitant des mises à jour ou des modifications.	
Détaille	
Dernière Mise à Jour	Cours **Sécurité des Systèmes Informatique & Systèmes d'Informations**
Version du document :	Final
Contact	**Dr. SEBRI Abderrahim**
Description du Document	

Le document intitulé «**Sécurité des Systèmes Informatique & Systèmes d'Informations** », proposé aux étudiants de 3éme année Licences Spécialité Ingénierie des Systèmes Informatique, Système Informatique et Informatique de Gestion comportant deux Sections ayant pour objectif de :

Section Cours : Comprendre les notions du **Sécurité des Systèmes Informatique & Systèmes d'Informations** :

- Concept de **Sécurité des Systèmes Informatique & Systèmes d'Informations**
- Méthodologies de **Sécurité des Systèmes Informatique**
- Méthodologies de **Sécurité des Systèmes d'Informations**,
- Niveaux de **Sécurité des Systèmes Informatique & Systèmes d'Informations**,
- Comprendre les Outils de la mise en place de le Méthodologies de **Sécurité des Systèmes Informatique & Systèmes d'Informations**, et les différents types d'outils de Framework utilisées

Préambule

Ce présent cours décrit la Sécurité informatique comme étant l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information, des systèmes et ressources informatiques contre les menaces atteignant leur confidentialité, intégrité, et disponibilité.

Les systèmes d'information sont basés sur des infrastructures informatiques et de télécommunication. Par suite, la vulnérabilité des infrastructures implique la vulnérabilité des systèmes d'information. Dont Les dangers qui guettent les SI sont présentes dans des différents niveaux de l'infrastructure hardware et software du système informatique et du SI.

On distingue 2 dangers majeurs guettent ces derniers :

- **Perte de données** dont les causes courantes sont :
  - **« Les accidents imprévu »** (?) : Feu, inondations, tremblements de terre, guerres, émeutes, rats, ….
  - **les erreurs matérielles ou logicielles** : Fonctionnement défectueux du processeur, disques et bandes illisibles, erreurs de télécommunication, bogues dans les programmes, …
  - **les erreurs humaines** : Saisie de données erronées, utilisation d'un mauvais disque, mauvaise exécution d'un programme, perte d'une disquette,…

  La solution universelle à ces problèmes : la sauvegarde et la mise en place d'un système de back-up

- **Fuite de données et intrusions** dont les causes courantes sont :
  - Indiscrétion des utilisateurs
  - Furetage
  - Appât du gain : modification de données, vente d'information, chantage informatique
  - Espionnage industriel ou militaire

  Les solutions sont les mécanismes de protection :

  - Identification
  - Authentification
  - Autorisation
  - Encryptage
  - Firewalls
  - Audit
  - Logiciels anti-virus
  - Programmes de tests de vulnérabilité et d'erreurs de configuration
  - Détection d'intrusion

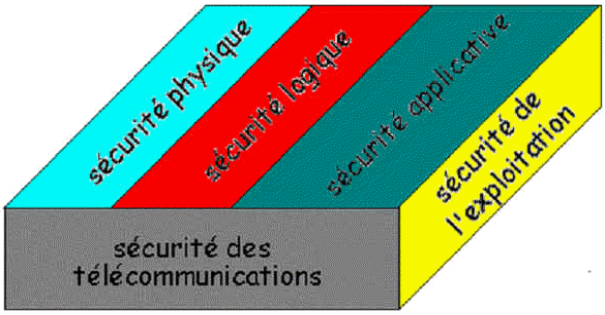
Chapitre I : Sécurité des Systèmes Informatiques

1. Définitions - Les Aspects de la Sécurité Informatique

Dans la suite nous détaillons les objectifs de la sécurité informatique qui sont présentées en deux objectives :

- **Réduire les risques technologiques**
- **Réduire les risques informationnels dans l'utilisation des systèmes d'information**

Il existe plusieurs domaines de sécurité à mettre en œuvre selon la figure suivante :



Sécurité physique : Aspects liés aux systèmes matériels Aspects liés à l'environnement : locaux, alimentation électrique, climatisation,… ; nécessitante la prises des différents mesures de sécurité : Respect de normes de sécurité, Protections diverses, Traçabilité des entrées, Gestion des accès, Redondance physique, Marquage de matériels

Sécurité logique : admettant plusieurs prises de mesures dans :

- Mécanismes logiciels de sécurité
- Contrôle d'accès logique : identification, authentification, autorisation
- Protection des données : cryptage, anti-virus, sauvegarde

Sécurité applicative : l'objectif est d'éviter les « bugs » : Méthodologie de développement par la Mise en place des :

- Plans de Contrôles et tests
- Plans de migration des applications

Sécurité de l'exploitation : elle vise le bon fonctionnement des systèmes

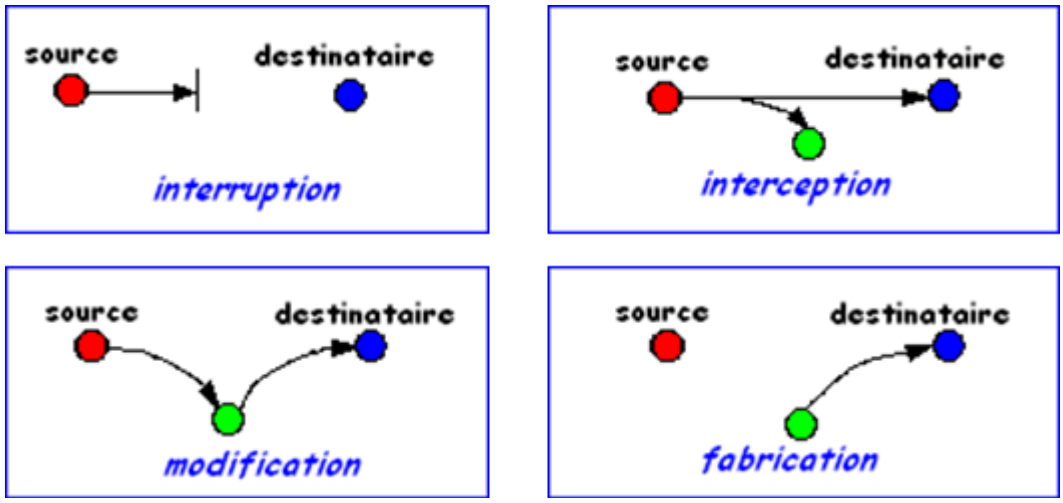
- Procédures de maintenance, de test, de diagnostic, de mise à jour
- Plan de sauvegarde Plan de secours

Sécurité des télécommunications : Nécessité d'une infrastructure réseau sécurisée

- au niveau des accès
- au niveau des protocoles

- ☐ Au niveau des systèmes d'exploitation
- ☐ Au niveau des équipements

Dans le domaine de la sécurité des systèmes informatiques et plus précisément les systèmes d'informations SI on distingue 4 problèmes principaux à résoudre (cliquez sur l'image):



2. Les propriétés (services) fondamentales de la sécurité

Les propriétés (services) fondamentales de la sécurité sont les suivantes :

- ❖ **Confidentialité** : protéger le contenu d'un message ou de données contre un espion qui écouterait les communications.
- ❖ **Intégrité** : la certification de la non-altération des données, traitements et services.
- ❖ **Disponibilité** : L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.
- ❖ **Authentification** : la vérification de l'identité de l'utilisateur et de ses autorisations (détermination de l'identité de l'interlocuteur).
- ❖ **Non-répudiation** : protection contre la négation d'une action accomplie : imputabilité, traçabilité, audibilité.
- ❖ **Authenticité** = l'authentification et l'intégrité.

3. Gestion des Risques

3.1. Définitions

La gestion de risque est défini par :

- ❖ **Risque** = (Menace x Vulnérabilité)/Contre-mesures
- ❖ **Menace** : Violation potentielle d'une propriété de sécurité.

3.2. Types de Menace

Accidentelles :

- Catastrophes naturelles ("acts of God"): feu, inondation, …
- Actes humains involontaires : mauvaise entrée de données, erreur de frappe, de configuration, …
- Performance imprévue des systèmes : Erreur de conception dans le logiciels ou matériel, Erreur de fonctionnement dans le matériel,…

Délibérées :

- Vol de systèmes
- Attaque de dénis de service
- Vol d'informations (atteinte à la confidentialité)
- Modification non-autorisée des systèmes.

Vulnérabilité : faiblesse / faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système.

Attaque : tentative volontaire de violer une ou plusieurs propriétés de sécurité.

Intrusion : violation effective de la politique de sécurité.

3.3. Contre-Mesures

Contre-mesures est l'ensemble des actions mises en œuvre en prévention de la menace.

- Encryptage des données
- Contrôles au niveau des logiciels
- Partie du système d'exploitation,
- Contrôle du développement des logiciels
- Contrôles du matériel
- Contrôle de l'accès au matériel : identification et authentification.
- Contrôles physiques : serrures, caméras de surveillance, gardiens, etc…

3.4. Logiciels Malveillants

La définition d'un logiciel malveillant est un programme qui infecte un système informatique :

- **Virus :** Tout programme capable d'infecter un autre programme en le modifiant de façon à ce qu'il puisse se reproduire. **Qui infecte : Programmes, documents, secteurs de boot.**
  - **Les macro-virus,**
  - **Les virus résidents**
  - **Les virus de boot**
  - **Les virus lents**
  - **Les virus défensifs ou rétrovirus**
  - **Les virus furtifs**
- **Ver (Worm):** Programme autonome qui se reproduit et se propage à travers le réseau.

- **Cheval de Troie:** Programme à l'apparence utile mais cachant du code pour créer une faille dans le système (back-door).
- **le logiciel espion (spyware) :** fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation. Ces informations sont ensuite transmises à une société en général pour du profilage.
- **Les courriels (spamming) :** consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres pour la faire saturer.

3.5. La Mise en œuvre d'une politique de sécurité

Les moyens de la Mise en œuvre d'une politique de sécurité sont :

- moyens organisationnels et procéduraux : ensemble de règles qui doivent être mises en place et respectées
- moyens informatiques : Cryptographie, cryptanalyse.
- moyens matériels ou physiques : architecture des entreprises,

3.6. Les systèmes de contrôle d'accès et Contrôles d'accès

Les systèmes de contrôle d'accès et Contrôles d'accès sont Un ensemble de méthodes informatique a pour rôle de :

- **Administrer l'accès aux ressources (Administration).**
- **Contrôler les droits d'accès. (Identification et authentification).**
- **Identifier les utilisateurs autorisés ou non (autorisation).**

Les Contrôles d'accès gouvernent et contrôlent l'accès d'un sujet à des objets. Les étapes de processus : l'administration, l'identification, l'authentification et l'autorisation.

Administration des contrôles d'accès contient :

- La gestion des comptes utilisateur.
- Le suivi des activités.
- L'identification est le processus par lequel un sujet prétend avoir une identité et donc une responsabilité (non répudiation) est engagée. Un utilisateur fournissant un nom d'utilisateur, un ID de connexion, un numéro d'identification personnel (NIP), ou une carte à puce représente le processus d'identification. Une fois le sujet s'est identifié, l'identité de ce sujet est tenue responsable pour toutes les actions de ce sujet.
- Les systèmes de suivi (log et les fichiers journaux) permettent de garder les traces des usagers par leurs identités.
- L'identité permet au système de faire la distinction entre tous les utilisateurs de ce système.

Authentification - Facteur d'authentification de type 3 représente quelque chose de nous-même :

- Empreintes digitales,
- Géométrie de la main,
- Reconnaissance du visage,
- Reconnaissance de l'iris,

- Reconnaissance de la rétine,
- La reconnaissance vocale, dynamique des signatures (signature-scan),…

L'Autorisation : Une fois un sujet est authentifié, l'accès doit être autorisé :

Le processus d'autorisation garantit que l'accès à l'activité ou à l'objet demandé est possible compte tenu des droits et des privilèges accordés à ce sujet authentifié.

Dans la plupart des cas, le système évalue une matrice de contrôle d'accès, qui compare le sujet, l'objet, et l'activité. Si l'action spécifique est permise, le sujet est autorisé. Si l'action spécifique est interdite, le sujet n'est pas autorisé.

Important : gardez à l'esprit que juste parce qu'un objet a été identifié et authentifié ne signifie pas automatiquement qu'il a été autorisé.

3.7. Les catégories de contrôle d'accès et Contrôles d'accès

Les contrôles d'accès sont classés en trois catégories :

- **Préventifs** : Sont déployés pour stopper une activité non autorisée de se produire.
- **Détectés** : Sont déployés pour détecter (découvrir) une activité non autorisée.
- **Correctifs** : Sont déployés pour restaurer les systèmes à un état normal après qu'une activité non autorisée ou non désirée soit produite.

L'implémentation des systèmes de contrôle d'accès peut être divisée en trois parties :

- ***CA* administratifs** : représentent un ensemble de politiques et de procédures pour mettre en œuvre et appliquer un contrôle d'accès global.
- ***CA* logiques et techniques** : représentent un ensemble de logiciels et de matériels capables de gérer et de protéger l'accès aux ressources demandées.
- ***CA* physiques** : représentent les barrières physiques déployées pour éviter le contact direct avec les systèmes.

4. Détection d'Intrusion

4.1. Notion d'un Système de Détection d'Intrusion IDS

La détection d'intrusions consiste à analyser les informations collectées par les mécanismes d'audit de sécurité en utilisant un système qui effectue la détection d'intrusion d'une manière automatique, ce système est appelé « **IDS: Intrusion Detection System** ».

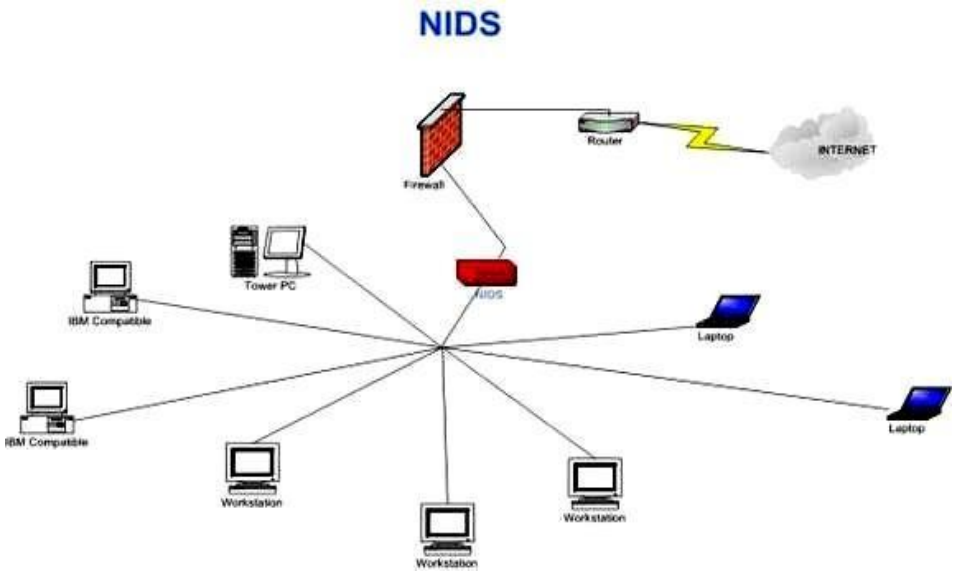
Les IDS sont des systèmes software ou hardware conçus afin de pouvoir automatiser l'inspection des fichiers journaux, d'audits et les événements produits par le système en temps réel.

Un IDS peut :

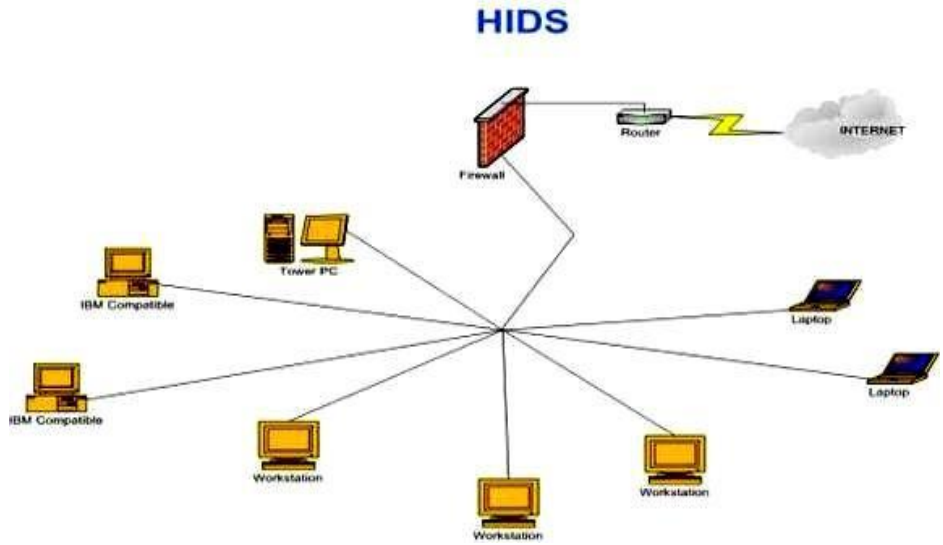
- Surveiller activement les activités suspectes.
- Mettre en évidence les vulnérabilités, identifier le point d'origine de l'intrusion.
- Reconfigurer les routeurs et les pare-feu pour empêcher les répétitions d'attaques découvertes.

4.2. Système de Détection d'Intrusion (NIDS et HIDS)

- **Les NIDS (Network-Based IDS)** sont installés sur le réseau, ils permettent de détecter les attaques ou les anomalies par le biais de la capture et de l'évaluation des paquets réseau. Certaines versions de titres IDS basé sur le réseau utilisent des agents à distance pour recueillir des données provenant de divers sous-réseaux et de faire les reports à un système de gestion centrale.



- **Les HIDS (Host-Based IDS)** sont dédiée pour identifier les fichiers et les processus compromis autorisée dans une Hôtes. Les IDS hôtes (installé sur les PCs) peuvent Détecter les intrusions locales mais pas seules des réseaux.



Les Actions d'un IDS sont :

- **Journaliser l'événement,**
- **Avertir un système ou un humain par un message,**
- **Amorcer certaines actions sur un réseau ou hôte.**

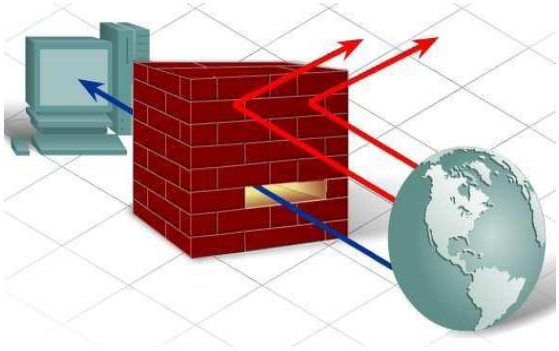
Les Points négatifs des IDS sont : Technologie complexe, Nécessite un degré d'expertise élevé, Réputer pour générer de fausses alertes, Encore immature.

5. Le Pare-feu (Firewall)

5.1. Définitions

Un pare-feu est un système physique (matériel) ou logique (logiciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3, 4 et 7 du modèle OSI.

- **Les Pare-feux (firewalls)** : est un mur qui empêche la propagation d'un incendie dans un bâtiment.
- **Pare-feu** : en informatique une protection d'un réseau contre des attaques.



Le pare-feu joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle OSI :

- déterminer le type de trafic qui sera acheminé ou bloqué
- limiter le trafic réseau et accroître les performances,
- autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau,
- Enregistrer le trafic.

5.2. Les Types de Pare-Feux (Stateless)

Pare-feux statique (Filtrage de paquets sans état) : Les pare-feux de filtrage de paquets sans état sont généralement des routeurs qui permettent d'accorder ou de refuser l'accès en fonctions des éléments suivants :

- l'adresse source,
- l'adresse destination,
- le numéro de port,
- le protocole.

Pare-feux dynamique (filtrage de paquets avec état): conserve les états des connexions : 4 types d'états:

- **NEW** : un client envoie sa première requête vers un serveur web.
- **ESTABLISHED** : connexion a déjà été initiée (après un NEW).

- **RELATED** : ce peut être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- **INVALID** : un paquet qui n'a rien à faire là-dedans.

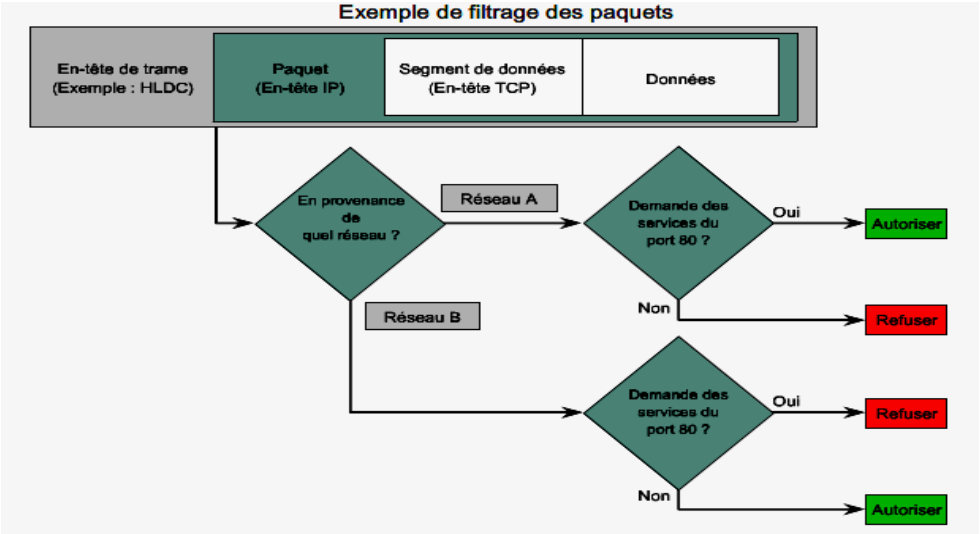
Pare-feux applicatifs (proxy): analyse du trafic échangé au niveau application (couche 7) pour appliquer une politique de sécurité spécifique de chaque application.

Ces systèmes se substituent au serveur ou au client qu'ils ont pour mission de défendre pour : Traiter les requêtes et réponses à la place du système à protéger, les transmettre, après d'éventuelles modifications ou les bloquer.

Exemple de Firewall (Filtrage de paquets) : Listes de contrôle d'accès

ACL = bout d'un pare-feu dans un routeur.

LES ACL (Access Control List) : sont des Collections d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères

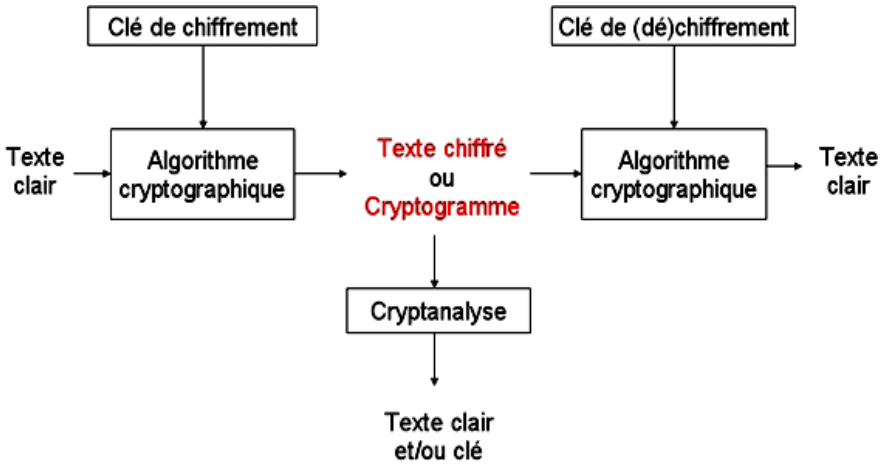


6. La Sécurité des Donnés : Cryptologie

6.1. Définitions

- **Cryptologie** : Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.
- **Cryptographie** : La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.
- **Cryptanalyse** : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en exploitant les failles des algorithmes utilisés.
- **Crypto-système** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.
- **Texte chiffré** : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

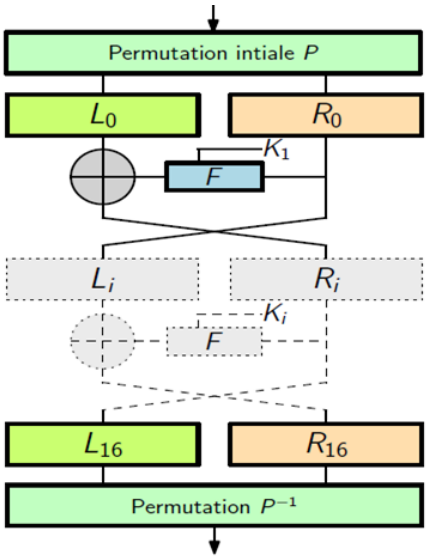
❖ **Clé** : Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement.



6.2. Algorithme Data Encryption Standard (DES)

Le DES est un algorithme de chiffrement symétrique par blocs qui permet de chiffrer des mots de 64 bits à partir d'une clef de 56 bits + 8 bits de parité.

* Le déchiffrement est identique au chiffrement, à condition de prendre les sous-clés dans l'ordre inverse.



6.3. Algorithme Advanced Encryption Standard (AES)

L'algorithme Advanced Encryption Standard (AES) est un algorithme de chiffrement par blocs à plusieurs tours similaire à DES mais avec une taille de blocs de 128 bits et de clefs supérieures et variables, choisis entre 128, 192 et 256 bits.

Algorithme de chiffrement par Traitement itératif de ces blocs en fonction de la taille de la clé secrète :

- **10 itérations pour des clés de 128 bits**
- **12 itérations (clés de 192 bits)**
- **14 itérations (clés de 256 bits)**

Initialisation :

- Le bloc de 128 bits (=16 octets) est recopie verticalement dans un tableau « d'etat » 4x4 .
- XOR avec la sous-clé numéro 0.
- Itérations (10, 12 ou 14 fois) sur le tableau d'état :
- Confusion : substitution indépendante sur chaque bloc, basée sur les inverses dans le corps fini 2^8
- Décalage des trois dernières lignes suivant un pas différent
- Diffusion : multiplication polynomiale des colonnes
- XOR avec la sous-clé numéro i
- Lecture du résultat final dans le tableau d'état.

Chapitre II : Sécurité des Systèmes d'Information

1. Introduction

Dans ce chapitre on va détailler les concepts de sécurité des systèmes d'information sont basés sur des infrastructures informatiques et de télécommunication. Par suite, la vulnérabilité des infrastructures implique la vulnérabilité des systèmes d'information. Dont Les dangers qui guettent les SI sont présentes dans des différents niveaux de l'infrastructure hardware et software du système informatique et du SI.

2. Signature Electronique

Plusieurs questions qui traînent dans l'esprit en abordant ce suet de la signature électronique :

- **Qu'est-ce que une signature électronique ?**
- **Comment peut-on être sûr que la clé publique appartient réellement à celui qui prétend en être le propriétaire ?**

Afin d'assurer la sécurité de l'information transmise on devra assurer par une signature électronique représentant par une clé spécifique de l'information garantie par le biais des certificats :

- Intégrité du certificat garantie par signature électronique de son contenu
- Création, publication, révocation des certificats effectués exclusivement par un tiers en qui toutes les parties communicantes ont confiance

La signature électronique où on appelle PKI (Public Key Infrastucture, ou en français infrastructure à clé publique (ICP), parfois infrastructure de gestion de clés (IGC)) l'ensemble des solutions techniques basées sur la cryptographie à clé publique.

Les crypto systèmes à clés publiques permettent de s'affranchir de la nécessité d'avoir recours systématiquement à un canal sécurisé pour s'échanger les clés. En revanche, la publication de la clé publique à grande échelle doit se faire en toute confiance pour assurer que :

- **La clé publique est bien celle de son propriétaire ;**
- **Le propriétaire de la clé est digne de confiance ;**
- **La clé est toujours valide.**

Ainsi, il est nécessaire d'associer à la bi-clé (ensemble clé publique / clé privée) un certificat délivré par un tiers de confiance : l'infrastructure de gestion de clés.

Notion de tiers de confiance : Le tiers de confiance est une entité appelée communément autorité de certification (ou en anglais Certification authority, abrégé CA) chargée d'assurer la véracité des informations contenues dans le certificat de clé publique et de sa validité.

Pour ce faire, l'autorité signe le certificat de clé publique à l'aide de sa propre clé en utilisant le principe de signature numérique.

Rôle de l'infrastructure de gestion de clés : Le rôle de l'infrastructure de clés publiques est multiple et couvre notamment les champs suivants :

- enregistrer des demandes de clés en vérifiant l'identité des demandeurs ;
- générer les paires de clés (clé privée / clé publique) ;
- garantir la confidentialité des clés privées correspondant aux clés publiques ;

- certifier l'association entre chaque utilisateurs et sa clé publique ;
- révoquer des clés (en cas de perte par son propriétaire, d'expiration de sa date de validité ou de compromission).

Organisation d'une PKI : Une infrastructure à clé publique est en règle générale composée de deux entités distinctes :

- L'autorité d'enregistrement (notée AE ou RA pour Recording authority), chargée des formalités administratives telles que la vérification de l'identité des demandeurs, le suivi et la gestion des demandes, etc.) ;
- L'autorité de certification (notée AC ou CA pour Certification Authority), chargée des tâches techniques de création de certificats. L'autorité de certification est ainsi chargée de la signature des demandes de certificat (notées CSR pour Certificate Signing Request, parfois appelées PKCS#10, nom du format correspondant). L'autorité de certification a également pour mission la signature des listes de révocations (CRL pour Certificate Revocation List) ;
- L'Autorité de dépôt (Repository) dont la mission est de conserver en sécurité les certificats ;

3. La Sécurité des SI

La sécurité peut s'évaluer suivant plusieurs critères :

- **Disponibilité :** garantie que ces éléments considérés sont accessibles au moment voulu par les personnes autorisées.
- **Intégrité :** garantie que les éléments considérés sont exacts et complets.
- **Confidentialité :** garantie que seules les personnes autorisées ont accès aux éléments considérés.
- **Traçabilité (ou « Preuve ») :** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

Dans plusieurs scénario sont met en jeu :

- une méthode d'attaque (action ou événement, accidentel ou délibéré),
- les éléments menaçants (naturels ou humains, qui agissent de manière accidentelle ou délibérée) susceptibles de l'employer,
- les vulnérabilités des entités (matériels, logiciels, réseaux, organisations, personnels, locaux), qui vont pouvoir être exploitées par les éléments menaçants dans le cadre de la méthode d'attaque.

Exemple de risque décomposé :

- **Méthode d'attaque :** piégeage du logiciel (introduction d'un ver)
- **Élément menaçant :** un pirate expérimenté engagé par un concurrent
- **Entité :** réseau WiFi
- **Vulnérabilité :** possibilité d'administrer le réseau à distance
- **Opportunité jugée :** moyenne
- **Atteinte des éléments essentiels :** atteinte à la confidentialité (vol d'informations)
- **Impact sur l'organisme :** perte d'avantages concurrentiels
- **Attaque passive :** écoute

- **Attaque active** : ver informatique
- **Usurpation** : niveau envoi message, usurpation d'identité, se faire passer pour qui nous ne sommes pas
- **Répudiation** : nier être l'auteur d'un message/ document
- **Intrusion**

4. Politique de Sécurité des Systèmes d'Information (PSSI)

4.1. Définitions (PSSI)

La définition de la politique de sécurité est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.

La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact.

4.2. Audit

L'Audit est d'identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

- **Mise à plat des process**
- **Identification des besoins**

La phase d'identification des besoins consiste dans un premier temps à faire l'inventaire du système d'information, notamment pour les éléments suivants :

- Personnes et fonctions ;
- Matériels, serveurs et les services qu'ils délivrent ;
- Cartographie du réseau (plan d'adressage, topologie physique, topologie logique, etc.) ;
- Liste des noms de domaine de l'entreprise ;
- Infrastructure de communication (routeurs, commutateurs, etc.)
- Données sensibles.
- Analyse des risques

L'étape d'analyse des risques consiste à répertorier les différents risques encourus, d'estimer leur probabilité et enfin d'étudier leur impact.

La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait (par exemple attaque sur un serveur ou détérioration de données vitales pour l'entreprise).

Sur cette base, il peut être intéressant de dresser un tableau des risques et de leur potentialité, c'est-à-dire leur probabilité de se produire, en leur affectant des niveaux échelonné selon un barème à définir, par exemple :

- Sans objet (ou improbable) : la menace n'a pas lieu d'être ;
- Faible : la menace a peu de chance de se produire ;
- Moyenne : la menace est réelle ;
- Haute : la menace a de grandes chances de se produire

4.3. Les Démarches de la Sécurité des SI

Elaboration des règles : Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ; Rester réaliste ne pas être trop ambitieux mieux vaut partir avec des objectifs bas et tenir ses objectifs

Surveillance : Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

Actions : Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

Stratégie : PSSI doit faire partie intégrante de la stratégie de la société :

- défaut de sécurité coûte cher !
- Inclure une notion générale de la sécurité reposant sur 4 points:
- Protection des applicatifs aux métiers du SI qualifiés de sensible
- Diminution des vulnérabilités
- Sécurité proprement dite du SI
- Continuité en cas de sinistre

Normes : Qu'est-ce que les Normes de sécurité d'un système de management de la sécurité de l'information ?

- **ISO 27 001**: Approche processus (PDCA) et 133 mesures base dans l'élaboration du plan
- **ISO 17 799**: découpage par thèmes correspond aux réalités de l'organisation de l'entreprise

L'**ISO 27001** en tant que norme de management se rapproche de l'ISO 9001 par l'adoption de l'approche processus et de la démarche PDCA (Plan-Do-Check-Act) dans la mise en place et l'animation du système de management de la sécurité de l'information en insistant sur les points suivants :
- le besoin de définir une politique de sécurité de l'information par rapport à des besoins exprimés sur ce sujet,

- la mise en place opérationnelle de dispositions ou mesures de sécurité de l'information en fonction des risques pouvant peser sur l'activité commerciale de l'organisation considérée,
- la surveillance du système mis en place en termes d'efficacité,

- l'amélioration continue basée sur des vérifications objectives.

Méthodes : les étapes sont :

- Etude du contexte : éléments essentiels (ensemble d'entités de différents types)
- Expression des besoins : critères de sécurité impact
- Etude des menaces : type/cause
- Expression des objectifs de sécurité
- Détermination des exigences de sécurité

4.4. Les Méthodes de Sécurité des Systèmes SI

- **La méthode CobiT** (Control Objectives for Business and related Techonology – Contrôle de l'Information et des Technologies Associées) référentiel principal de gouvernance et d'audit des SI est le CobiT. En résumé le CobiT est un cadre de référence pour maitriser la gouvernance des SI dans le temps. Il est fondé sur ensemble de bonnes pratiques collectées auprès d'experts du SI.
- **La méthode EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI.
- **La méthode ISMS (Information Security Management System):** Il s'agit d'une démarche globale et non plus d'une démarche réactive qui fait fasse à des problèmes
  - Planifier: passer d'une posture réactive à proactive
  - Faire: développer des processus en suivant un référentiel de sécurité
  - Contrôler: audits et tests d'intrusion
  - Agir: analyse des risques des besoins et enjeux

Bibliographies

1. A. Tanenbaum : Systèmes d'exploitation (InterEditions)
2. A. Tanenbaum : Réseaux (InterEditions)
3. S. Ghernaouti-Helie : Sécurité Internet (Dunod)
4. W. Stallings : Data and Computer Communications (Prentice Hall)
5. Maekawa, Oldehoeft & Oldehoeft : Operating Systems (Benjamin)
6. Réseaux et protection numérique des documents multimédias (études INA)
7. J.P. Lovinfosse : Le piratage informatique (Marabout)
8. N.J.Yeager, R.E.McGrath : Technologie des serveurs Web (Thomson Pub.)
9. S.M.Bellowin, W.R.Cheswick : Firewalls et sécurité Internet (Addison Wesley)