

Première Partie

Principes de Base de la Sécurité de l'Information

Quatre Principes

1. Connaître le système à défendre
2. Moindre privilège
3. Défense en couches
4. Prévention souhaitable / Détection obligatoire

Connaître son système

- « Connais ton ennemi et **connais-toi toi-même**; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.
- Si tu ignores ton ennemi et que **tu te connais toi-même**, tes chances de perdre et de gagner seront égales.
- Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites. »

Sun Tzu « L'Art de la Guerre »

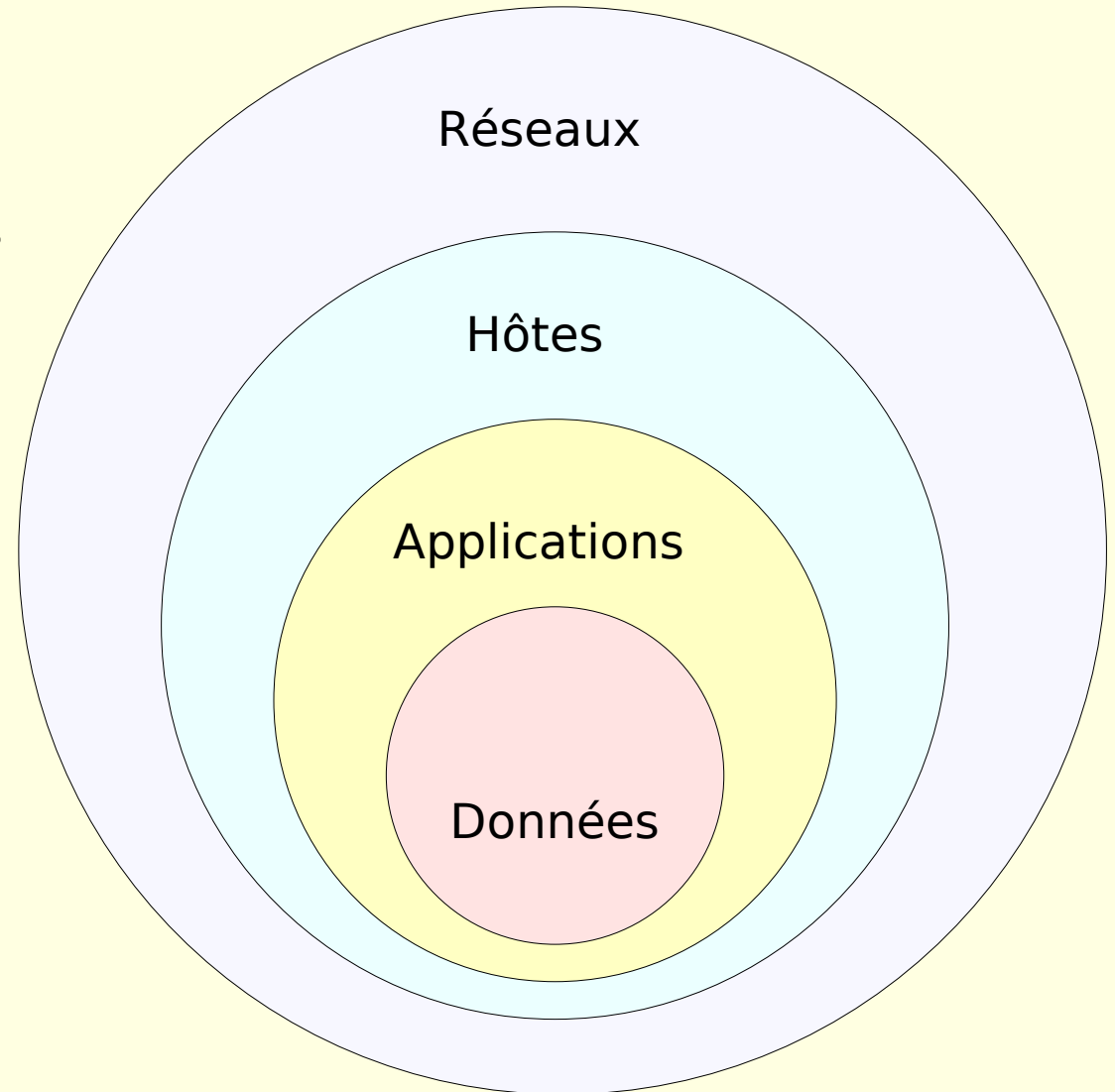
(Article III - Des propositions de la victoire et de la défaite)

Principe du moindre privilège

- Tout ce qui n'est pas explicitement autorisé est interdit
- Autoriser uniquement ce qui est utile et justifié
- Cependant :
 - attention à ne pas trop gêner les utilisateurs
 - ✓ ergonomie
- Exemple
 - pare-feu : ports fermés par défaut
ouverts uniquement si nécessaires

Défense en couches

- **Defence in Depth**
(Défense en profondeur)
 - multiplication des lignes de défenses
 - répartition à tous les niveaux
 - redondances
- Exemple :
 - antivirus sur le firewall **et** sur chaque station



Prévention / Détection

- Prévention
 - souhaitable
 - IPS (Intrusion Prévention System)
- **Détection**
 - **Obligatoire**
 - le plus rapidement possible
 - alertes
 - traçabilité / log
 - IDS (Intrusion Detection System)
 - honey pots

Trois concepts de base

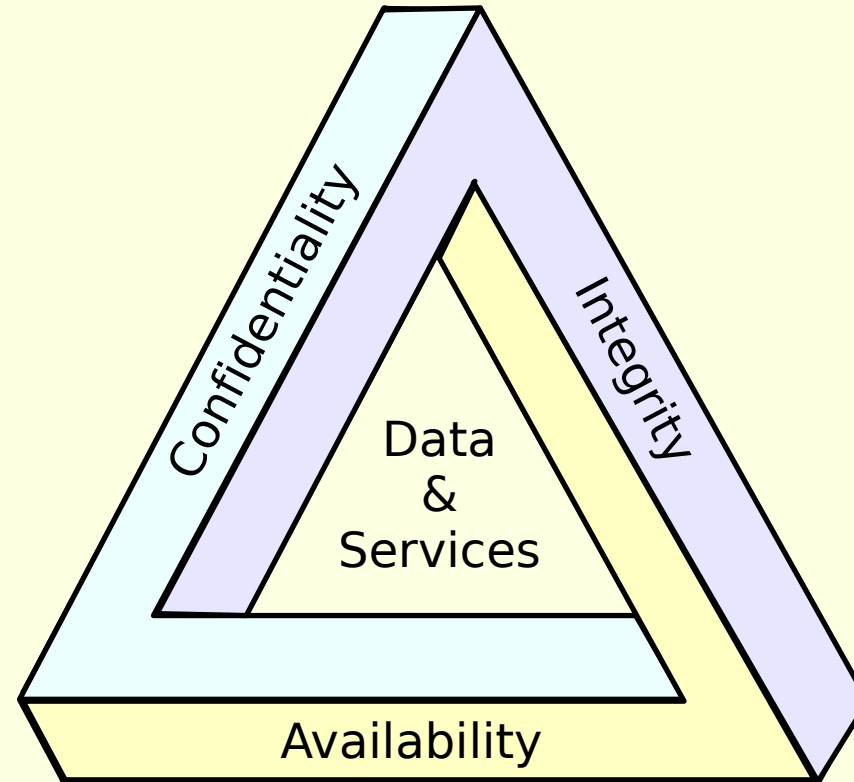
1. Confidentialité

2. Intégrité

3. Disponibilité

CIA triangle

- CIA Triad :
 - Confidentiality
 - Intégrity
 - Availability



Confidentialité

- Une information confidentielle
 - peut être :
 - ✓ accédée, utilisée, copiée ou divulguée
 - uniquement par:
 - ✓ des personnes autorisées,
 - ✓ des systèmes qui ont reçus les droits pour le faire

Atteinte à la confidentialité

- Exemples :
 - ✓ divulgation d'adresse mail, de numéro de téléphone
 - ✓ publication du salaire d'un employé
 - ✓ publication sur le WEB des coordonnées personnelles des étudiants, des profs...
 - ✓ divulgation de secrets
 - ◆ médical, industriels, militaires...
 - ✓ espionnage du comportement d'un internaute
 - ◆ site visités,
 - ◆ contenu des mails
 - ✓ keylogging

Protection de la confidentialité

- Accès physiques restreints
 - sécurité des bâtiments
 - badge
 - utilisation de la biométrie
- Cryptographie
 - science du secret
 - portail Wikipedia
 - http://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Portail_Cryptologie
 - Ars cryptographica
 - <http://www.apprendre-en-ligne.net/crypto/menu/index.html>

Intégrité

- Les informations
 - peuvent être :
 - ✓ créées, modifiées ou détruites
 - uniquement par:
 - ✓ des personnes ou des systèmes qui ont reçus les droits pour le faire

Atteinte à l'intégrité (exemples 1/2)

- Origine humaine :
 - Malversations:
 - ✓ Virus
 - ✓ Modification du portail d'un site web (defacing)
 - ✓ Modification crapuleuse d'une transaction bancaire
 - ✓ Modification des notes obtenues à un examen
 - Mauvaises manipulations:
 - ✓ Effacement non voulu de données
 - ✓ Incohérence entre bases de données

Atteinte à l'intégrité (exemples 2/2)

- Origine matérielle :
 - ✓ Pannes
 - ◆ disque dur
 - ◆ perturbations électromagnétiques
 - ◆ coupure de courant
 - ◆ pendant une mise à jour de données
 - ✓ Sinistres
 - ◆ inondation
 - ◆ incendie
 - ◆ vol
 - ◆ gobelet de café renversé

Protection de l'intégrité

- Signature
 - md5 (Message Digest 5)
 - CRC (Cycle Redundancy Check – Contrôle de redondance cyclique)
 - ECC (Error-Correcting Code – Code correcteur)
 - FCS (Frame Check Sequence – Contrôle de trame)
- Duplication, sauvegarde
- Protections physiques
 - Locaux protégés
 - Coffre-fort

Disponibilité

- Accès garanti à :
 - un service,
 - des ressources
 - des informations

dans un délai maximal déterminé.

Atteinte à la disponibilité

- **DoS** : **D**enial **o**f **S**ervice
 - par saturation
 - ✓ flooding (inondation)
 - ✓ mail bombing
 - ✓ nombre de requêtes hors norme
 - par exploitation de vulnérabilité
 - etc.
- **DdoS** : **D**istributed **D**enial **o**f **S**ervice
 - attaque par reflexion

CIA Triad (extensions)

- Parkerian Hexad (Donn B. Parker) :
 - Six attributs caractérisant l'information de façon granulaire, indépendants et sans recouvrement :
 - ✓ *Confidentialité*
 - ✓ Possession ou Contrôle
 - ✓ *Intégrité*
 - ✓ Authenticité
 - ✓ *Disponibilité*
 - ✓ Utilité
- Autres extensions :
 - Responsabilité (*Accountability*)
 - Non-Repudiation

Possession

- La possession ou le contrôle de l'information est distinct de la confidentialité
- Exemple :
 - une personne s'étant fait voler une serviette, avec une enveloppe scellée contenant sa carte de crédit et le code pin correspondant, a perdu le contrôle de l'information correspondante.

Authenticité

- Vérification de l'identité
 - d'une personne,
 - d'une machine,
 - d'un programme
- Exemple :
 - une personne peut envoyer un message en se faisant passer pour quelqu'un d'autre

Utilité

- Exemple :
 - Des données cryptées dont la clé de déchiffrement a été perdue satisfont aux cinq autres critères de sécurité mais ne sont plus d'aucune utilité.

Responsabilité

- Assurance de la traçabilité des événements permettant de remonter jusqu'à une personne ou un processus à l'origine d'une action.

Non répudiation

- Vérification que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message
- Non répudiation de l'origine :
 - prouve que les données ont été envoyées
 - Ex : Signature
- Non répudiation de l'arrivée :
 - prouve que les données ont été reçues
 - Ex : accusé de réception

Management du Risque (1/2)

- Risque :
probabilité que se produise un événement mettant en cause l'intégrité ou la confidentialité d'une information ou la possibilité d'y accéder

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$

Management du Risque (2/2)

- Menace :
type d'action susceptible de nuire dans l'absolu
Ex : virus
- Vulnérabilité :
niveau d'exposition face à la menace dans un
contexte particulier
Ex : fatigue, port ouvert
- Contre-mesure :
ensemble des actions mises en œuvre en
prévention de la menace
Ex : médicaments, pare-feu

Sécurité adéquate

- Compromis entre le coût de :
 - la valeur à protéger
 - le coût de la protection
 - le coût de l'acte de piratage
- Coût de la protection $<$ valeur à protéger
- Coût de l'acte de piratage $>$ valeur à protéger

Vulnérabilité (*Vulnerability*)

- Vulnérabilité informatique :
 - faiblesse dans un système, permettant de mettre en cause la sécurité d'une information ou d'un système d'information.
- Synonymes :
 - faille, brèche, trou de sécurité
- Exploit :
 - programme permettant à un individu d'exploiter une faille de sécurité informatique

Menace (*Threat*)

- Action (volontaire ou non) susceptible de nuire
- Synonyme : nuisance

Menaces humaines

- Hackers
 - White hat hackers
 - Black hat hackers
 - Malicious hackers
 - ✓ Script Kiddies
 - ✓ Crackers
- Espionnage industriels
- Crime organisé
- Terroristes
- 3-letters agencies (CIA, FBI, NSA, ...)

Hackers niveau 1

- Script kiddies
 - Jeune
 - Niveau technique
 - ✓ amateur
 - Utilisateurs d'outils disponibles « prêt à pirater »
 - Motivation
 - ✓ Jeu
 - ✓ Gloire, renommée
 - Ressources
 - ✓ Beaucoup de temps disponible

Hackers niveau 2

- Activistes
 - Individu ou organisation militante
 - Niveau technique
 - ✓ comparable aux script kiddies
 - Motivation
 - ✓ porter la bonne parole
 - ✓ ridiculiser leurs adversaires
 - ♦ ex : portail web defacing
 - ✓ dénoncer ce qui est contraire à leur idéologie
 - Ressources
 - ✓ coordination entre les groupes de même obédience

Hackers niveau 3

- Criminels
 - Seul ou organisé (mafia)
 - Niveau technique
 - ✓ variable (souvent important pour les équipes mafieuses)
 - Motivation
 - ✓ l'argent
 - Ressources
 - ✓ adaptées aux objectifs
 - ✓ équipes gérées par la mafia
 - ◆ vol de cartes de crédit
 - ◆ raquette de sites commerciaux

Hackers niveau 4

- Cyber-terroristes / Cyber-hooligans
 - Niveau technique
 - ✓ variable
 - Motivation
 - ✓ désorganiser
 - ✓ détruire
 - ✓ provoquer la panique
 - ✓ faire passer un message
 - Ressources
 - ✓ variables

Hackers niveau 5

- Industriel malhonnêtes
 - Motivation
 - ✓ Espionnage industriel et commercial
 - ✓ Sabotage
 - Niveau technique
 - ✓ Élevé
 - Ressources
 - ✓ Importantes

Hackers niveau 6

- Agences gouvernementales
 - 3-letters agencies
 - Militaires
 - Police
 - Motivation
 - ✓ Espionnage
 - ✓ Sécurité
 - ✓ Lutte contre la cyber-criminalité
 - Niveau technique
 - ✓ Maximal
 - Ressources
 - ✓ très grandes

Logiciels malveillants

- Virus (CPA : Code Auto Propageable)
 - Vers (*Worms*)
 - Cheval de Troie (*Trojan*)
 - Bombe logique
- Logiciel espion (Espionlogiciel - *spyware*)
- Rootkit
- Porte dérobée (*back door*)
- Keyloggers
- Composeur (*dialer*)

Contre-mesure (*Parade*)

- Ensemble des actions mises en œuvre en prévention d'une menace
- Trois types de contrôle
 - administratifs
 - logiques (techniques)
 - physiques

Contrôles administratifs

- Règles écrites
- Procédures
- Standard
- Recommandations

Contrôles logiques

- Moyens techniques logiciels de surveillance et de contrôle grâce à :
 - des données :
 - ✓ logon / mot de passe
 - ✓ certificats
 - des logiciels :
 - ✓ pare-feux
 - ✓ suite de sécurité : antivirus, anti-espions...
 - ✓ IDS (Intrusion Detection System)
 - ✓ IPS (Intrusion Prevention System)

-

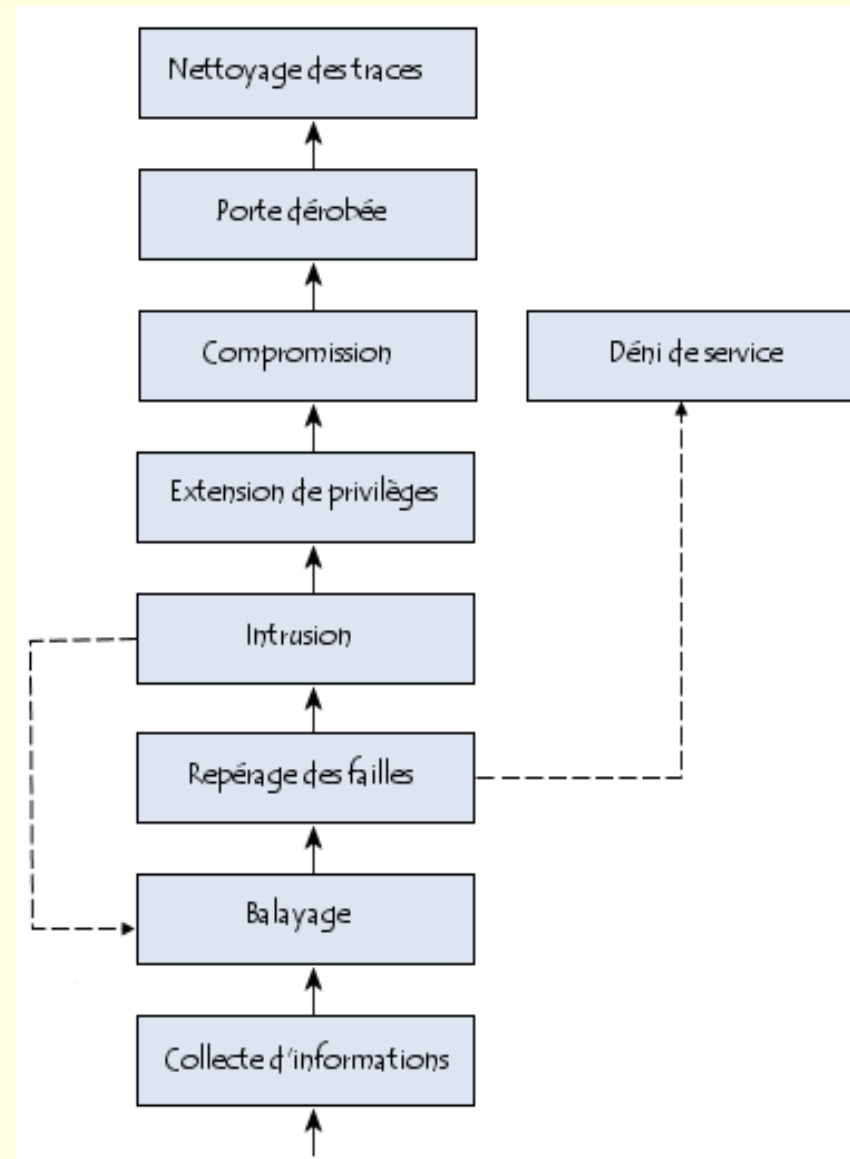
Contrôles physiques

- Moyens techniques matériels
 - machines dédiées :
 - ✓ proxy
 - ✓ routeurs / pare-feux
 - ✓ honey pots
 - ✓ onduleurs
- Protections physiques :
 - portes, badges, gardiens
 - alarmes
 - systèmes antivol
 - dispositifs anti-sinistres (anti-incendie, parfoudre...)

Principaux risques et parades

- Intrusion illégale : Authentification forte
- Vol d'informations : Encryption
- Intégrité : Authentification, firewalls
- Falsifications d'emails : Messagerie sécurisée (PGP, S/MIME)
- Denial of Service : Full scalability
- Virus : Antivirus
- Mots de passe crackés : Biométrie, puces...
- Intrusion sur le réseau : Firewall, Détection d'intrusion (IDS)

Attaque (Méthodologie)



Collecte d'informations

- Ingénierie sociale (social engineering)
 - exploitation des relations humaines
 - « L'art de la supercherie » de Kevin Mitnick
- Data bases publiques
 - www.iana.net, www.ripe.net, www.arin.net
- Moteurs de recherche
- Analyse du réseau visé
 - Adressage IP
 - noms de domaine
 - protocoles de réseau
 - services activés, types de serveurs, etc.

Balayage du réseau

- Utilisation d'un scanner pour déterminer :
 - les adresses IP actives
 - les ports ouverts
 - le système d'exploitation
- Outils
 - ping
 - nmap (scanner actif)
 - kismet (scanner passif)

Repérage des failles

- Utilisation de scanners de vulnérabilité.
 - Nessus
 - SAINT (**S**ecurity **A**dministrator's **I**ntegrated **N**etwork **T**ool)
- Consultation des bases de données répertoriant les vulnérabilités
 - ex : Insecure.org www.insecure.org
- Consulter les CERT

Intrusion

- Ingénierie sociale
 - contact des utilisateurs pour extorquer des informations
 - ✓ logon, mot de passe, etc.
- Recherche de nom d'utilisateurs valides
 - analyse d'annuaire, etc.
- Exploitation des vulnérabilités des logiciels
 - exploit
- Attaque des mots de passe (par force brute, etc.)
- Backdoor (porte dérobée)

Nettoyage des traces

- Suppression des fichiers
- Nettoyages des logs (journaux d'activité)
- Rootkits (Kits racine)
 - version modifiées des outils système
 - ✓ dissimule l'activité du pirate sous des noms de commande usuelle
 - ✓ ex : commande ls, find, etc.

Classification des informations

- Permet de mettre en place les procédures et protections appropriées.
- Doit être revue périodiquement :
 - pour vérifier si le niveau de classification d'une information est toujours nécessaire
 - si les protections correspondantes sont en place
- Exemples
 - dans les entreprises :
 - ✓ public, privé, sensible, confidentiel
 - dans les administrations :
 - ✓ non classifié, à usage interne, confidentiel, secret, top secret

Audit

- Audit interne
- Audit externe
 - sociétés spécialisées
- Méthodes
 - Marion (CLUSIF)
 - ✓ Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux
 - Mehari (CLUSIF)
 - ✓ Méthode Harmonisée d'Analyse de Risques Informatiques
 - EBIOS (DCSSI)
 - ✓ Expression des Besoins et Identification des Objectifs de Sécurité

Plan général

- Introduction
- Principes de Bases de la Sécurité de l'Information
- Cryptographie
- Sécurité des Réseaux
- Sécurité des Applications
- Politique de sécurité
- Conclusion