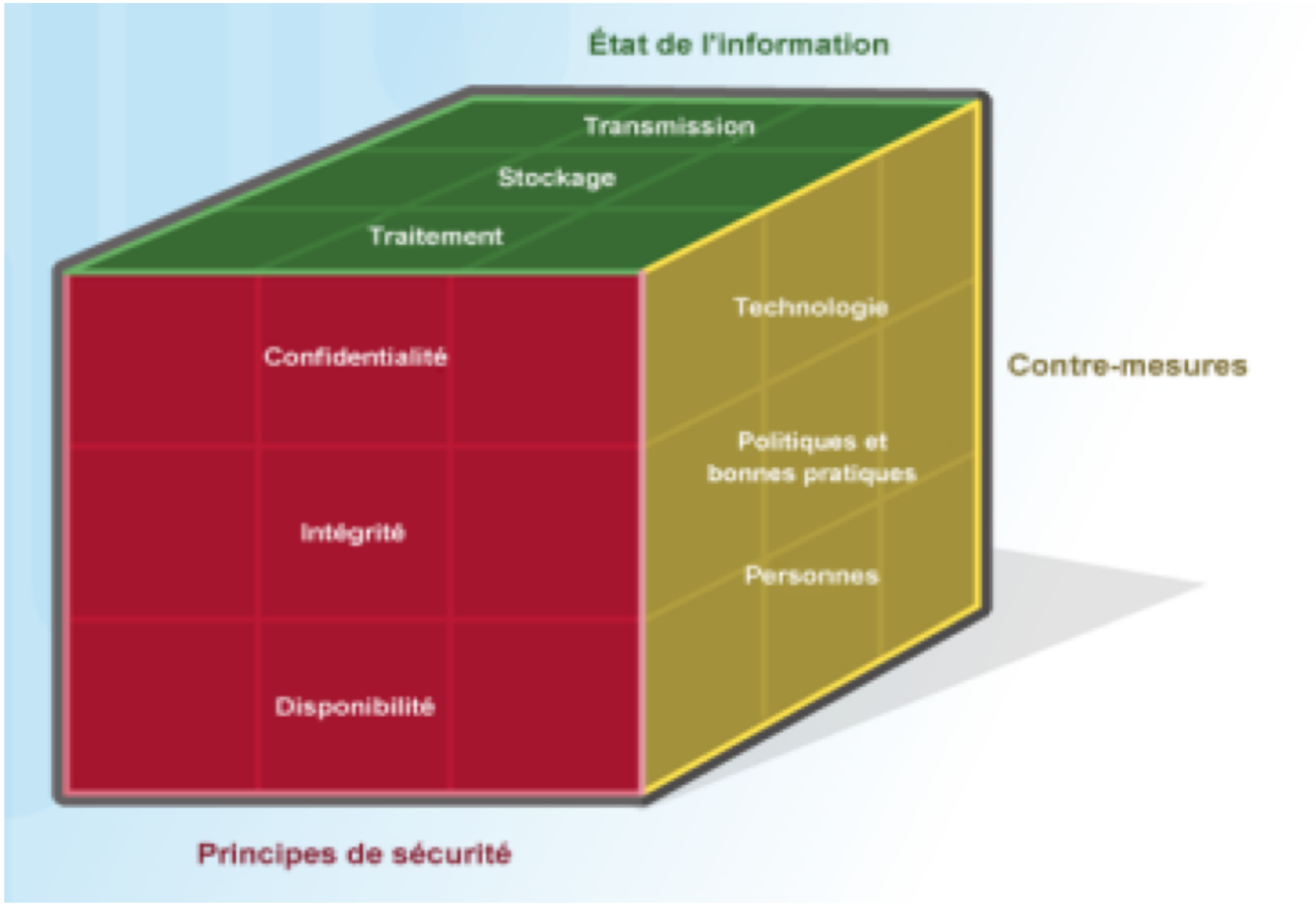
Introduction à la Sécurité

Licence 2 – Sem4
2020

Objectifs

- Comprendre les principes de sécurité pour:
  - Assurer la confidentialité des messages
  - Assurer l’Intégrité des données.
  - Assurer la Disponibilité des services

Principes de la sécurité
Cube Magique



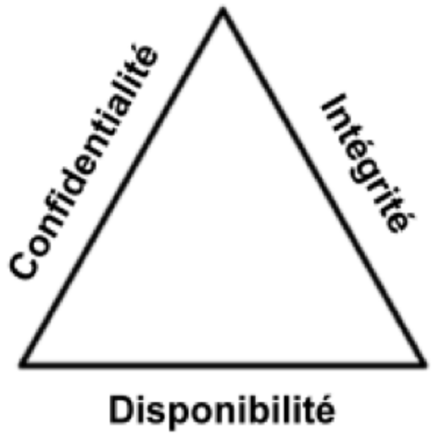
Principes de la sécurité
Cube Magique

- La **première dimension du cube magique** de la cyber sécurité identifie les objectifs à protéger sur Internet. Les objectifs identifiés dans la première dimension constituent les principes fondateurs du monde de la cyber sécurité.

- Ces trois principes sont la **confidentialité**, **l'intégrité** et la **disponibilité**.

- Ces principes permettent au cybermagicien de cibler ses efforts et d'établir des priorités dans les mesures à prendre pour assurer la protection de ses ressources sur Internet.

- Souvenez-vous de ses principes avec les initiales CID.



Principes de la sécurité
Cube Magique

- Les états des données:

  Internet est constitué de données. La protection des données est donc la priorité des cybermagiciens

- **La Deuxième dimension du cube magique** de la cyber sécurité porte sur les problèmes liés à la protection des données sur Internet, quel que soit leur état.

- Les données peuvent se présenter sous **trois états différents** :

  1) Données enregistrées ou stockées
  2) Données en transit
  3) Données en cours de traitement

Principes de la sécurité
Cube Magique

Dispositifs de protection en cyber sécurité

- La **troisième dimension du cube magique** de la cyber sécurité définit les types d'outils utilisés pour la protection sur Internet. Le cube magique identifie trois types d'outils :
  - **Technologies** : appareils et produits disponibles pour protéger les systèmes d'information et contrer les cybercriminels.
  - **Politiques et bonnes pratiques** : procédures et directives permettant aux citoyens du monde virtuel d'être protégés et de respecter les bonnes pratiques.
  - **Personnes** : informées et qualifiées, ils connaissent leur monde virtuel et les dangers qui le menacent.

Quelques définitions

La **cryptologie**

- La cryptologie est la science du secret. Elle se divise en deux disciplines :

  - La **cryptographie** qui est l'étude des algorithmes permettant la protection d'informations (numériques). Ces algorithmes sont appelés cryptosystèmes;

  - la **cryptanalyse** qui est l'étude du niveau de sécurité des cryptosystèmes fournis par les cryptographes (attaques).

Quelques définitions

La **cryptanalyse**
Peut essentiellement se diviser en deux grandes familles d'attaques qui viseront deux cibles différentes :

- **Algorithmes** : ici l'attaquant essaie de trouver des algorithmes efficaces pour résoudre les problèmes mathématiques sur lesquels reposent les cryptosystèmes

- I**mplémentations matérielles** : ici l'attaquant utilisera les fuites d'information lors de l'exécution d'un cryptosystème pour retrouver les secrets.

Quelques définitions

La **cryptographie**

La cryptographie protège l'information de différentes manières :

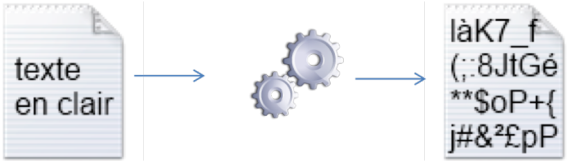
- **Confidentialité** : pour s'assurer que l'information ne soit seulement accessible qu'à ceux dont l'accès est autorisé ;
- **Intégrité** : pouvoir affirmer que les données ont ou n'ont pas été modifiées ;
- **Authenticité** : vérifier l'identité d'une personne ou d'un matériel informatique ;
- **L'authentification de l'origine** : les données proviennent d'une source prévisible.
- **La non-répudiation** : l'expéditeur peut prouver de manière irréfutable l'intégrité du message.

Ces moyens doivent reposer sur des secrets

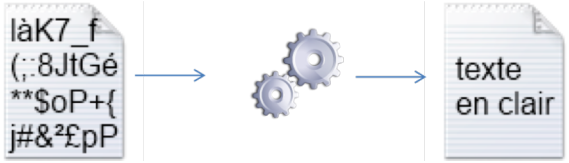
- **Clé secrète** : cryptographie symétrique ;
- **Clé publique/secrète** : cryptographie asymétrique

Quelques définitions

- **Chiffrer** : l'action de rendre un message clair **M** (plaintext) en un message **C** appelé cryptogramme ou message chiffré, illisible.



- **Déchiffrer** : Action inverse du chiffrement



- **Cryptosystème** : L'algorithme (ou le dispositif physique) permettant de chiffrer des données.

- **Attaquer, casser** : Mettre à mal la sécurité d'un cryptosystème (retrouver **M** à partir de **C** sans connaître la clé, retrouver la clé).

Quelques définitions

- **Le chiffrement** : est un algorithme composé d'une série d'étapes bien définies que vous pouvez suivre pour chiffrer et déchiffrer des messages.

Deux caractéristiques des clés de chiffrement :

- **Longueur de la clé (taille)** : la longueur en bits de la clé.
- **Espace de clé** : le nombre de valeurs possibles qui peuvent être générées par une longueur de clé spécifique.

Propriété de sécurité
La confidentialité

- C'est la propriété qui assure qu'une information ne peut être lue que par des entités habilitées (selon des contraintes précises)

  - Un mot de passe ne doit jamais pouvoir être lu par un autre que son possesseur

  - Un dossier médical ne doit pouvoir être consulté que par les malades et le personnel médical habilité

Propriété de sécurité
L’Intégrité

- C'est la propriété qui assure qu'une information n'est modifiée que par des entités habilitées (selon des contraintes précises)
- Une modification intempestive (même très temporaire) est à interdite sur une écriture comptable validée
- Le code binaires des programmes ne doit pas pouvoir être altéré
- Les messages de l’ingénieur système doivent pouvoir être lus et non modifiés

Propriété de sécurité
La Disponibilité et la Fiabilité

- **Disponibilité** : capacité de rendre un service correct à un instant donné,
- **Fiabilité** : capacité à rendre continûment un service correct
  - Relèvent de la terminologie de la sûreté de fonctionnement

On retiendra toutefois que les actions de sabotage d'un système visent justement à diminuer sa disponibilité ou sa fiabilité.

Propriété de sécurité
L’Authentification

- C'est la propriété qui assure la reconnaissance sûre de l’identité d'une entité

  L'**authentification** protège de l'usurpation d'identité.

  Signature (au sens classique) = Authentification:

- La première idée contenue dans la notion habituelle de signature est que le signataire est le seul à pouvoir réaliser le graphisme (caractérisation psychomotrice)

  Entités à authentifier:

  - une personne

  - un programme qui s’exécute (processus)

  - une machine dans un réseau

Propriété de sécurité
La Non Répudiation

- C'est la propriété qui assure que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué.
- Signature (au sens habituel) = Authentification+Non répudiation :
- La seconde idée contenue dans la notion habituelle de signature est que le signataire s'engage à honorer sa signature:

  engagement contractuel, juridique, il ne peut plus revenir en arrière.
- Deux aspects spécifiques de la non répudiation dans les transactions électroniques:

  a) La preuve d'origine

  Un message (une transaction) ne peut être nié par son émetteur.

  b) La preuve de réception

  Un récepteur ne peut ultérieurement nier avoir reçu un ordre

  s'il ne lui a pas plu de l'exécuter alors qu'il le devait juridiquement.

  Exécution d'ordre boursier, de commande, ..

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT LA CONFIDENTIALITE

Les attaques ayant pour but le vol d'information via
un réseau par **espionnage des transmissions de données**
(espion de ligne, accès aux données dans des routeurs et des serveurs Internet)

Analyse de trafic

On observe le trafic de messages échangés pour en déduire des informations sur les décisions de quelqu'un.

Exemples:
Bourse : augmentation des transactions sur une place financière.
Militaire : le début de opération entraîne un accroissement de trafic important.

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DES DONNEES

Modification de messages, de données

Une personne non autorisée, un usager ou même un agent autorisé s'attribuent des avantages illicites en modifiant un fichier, un message (le plus souvent cette modification est réalisée par programme et entre dans la catégorie suivante)
Ex modification des données sur un serveur Web

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DU FLUX DE DONNEES

Répétition ("replay")

Espionnage d'une interface, d'une voie de communication (téléphonique, réseau local) pour capter des opérations (même cryptées elles peuvent être utilisables)

Répétition de l'opération pour obtenir une fraude.

Exemple: Plusieurs fois la même opération de crédit d'un compte bancaire.

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DES PROGRAMMES

Modification des programmes

Les modifications à caractère frauduleux

Pour s'attribuer à travers le programme des avantages.
Exemple: virement des centimes sur un compte

Les modifications à caractère de sabotage

Pour détruire avec plus ou moins de motivations
des systèmes ou des données

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DES PROGRAMMES (2)

Deux types de modifications

a) Infections informatiques à caractère unique

Bombe logique ou cheval de Troie

Dans un programme normal on introduit un comportement illicite mis en action par une condition de déclenchement ou trappe
(la condition, le moment ou l'on bascule d'un comportement normal à anormal)

Exemples: licenciement de l'auteur du programme

b) Infections auto reproductrices

Il s'agit d'une infection informatique simple (du type précédent)
qui contient de plus une partie de recopie d'elle même afin d'en assurer la propagation

***Virus* :** programme ou code malveillant => corruption de fichiers système ou utilisateur

Ver : même principe que le virus avec une capacité d’auto-propagation

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT LA DISPONIBILITE
(DENI DE SERVICE)

Attaque par violation de protocole

Erreur très rare en fonctionnement normal et non supportées par le protocole

Attaque par saturation

Envoi de messages trop nombreux provoquant un écroulement des systèmes et réseaux

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’AUTHENTIFICATION

Déguisement (Mascarade)

Pour rentrer dans un système on essaye de piéger des usagers et de se faire passer pour quelqu'un d'autre:

Exemple: simulation d'interface système sur écran,
simulation de terminal à carte bancaire

Historique de la cryptographie

Stycale