Sécurité Informatique

Chapitre 1 : Introduction à la sécurité

F.Z. Filali

Janvier 21, 2018

Plan

Objectifs du Chapitre

- Comprendre la sécurité de l'information et ses différents concepts.
- Comprendre les termes clés et les concepts critiques de la sécurité de l'information.
- Comprendre la motivation de la sécurité informatique et son évolution.
- Décrire les critères et besoins en sécurité.
- Comprendre les différents domaines d'applications de la sécurité informatique.

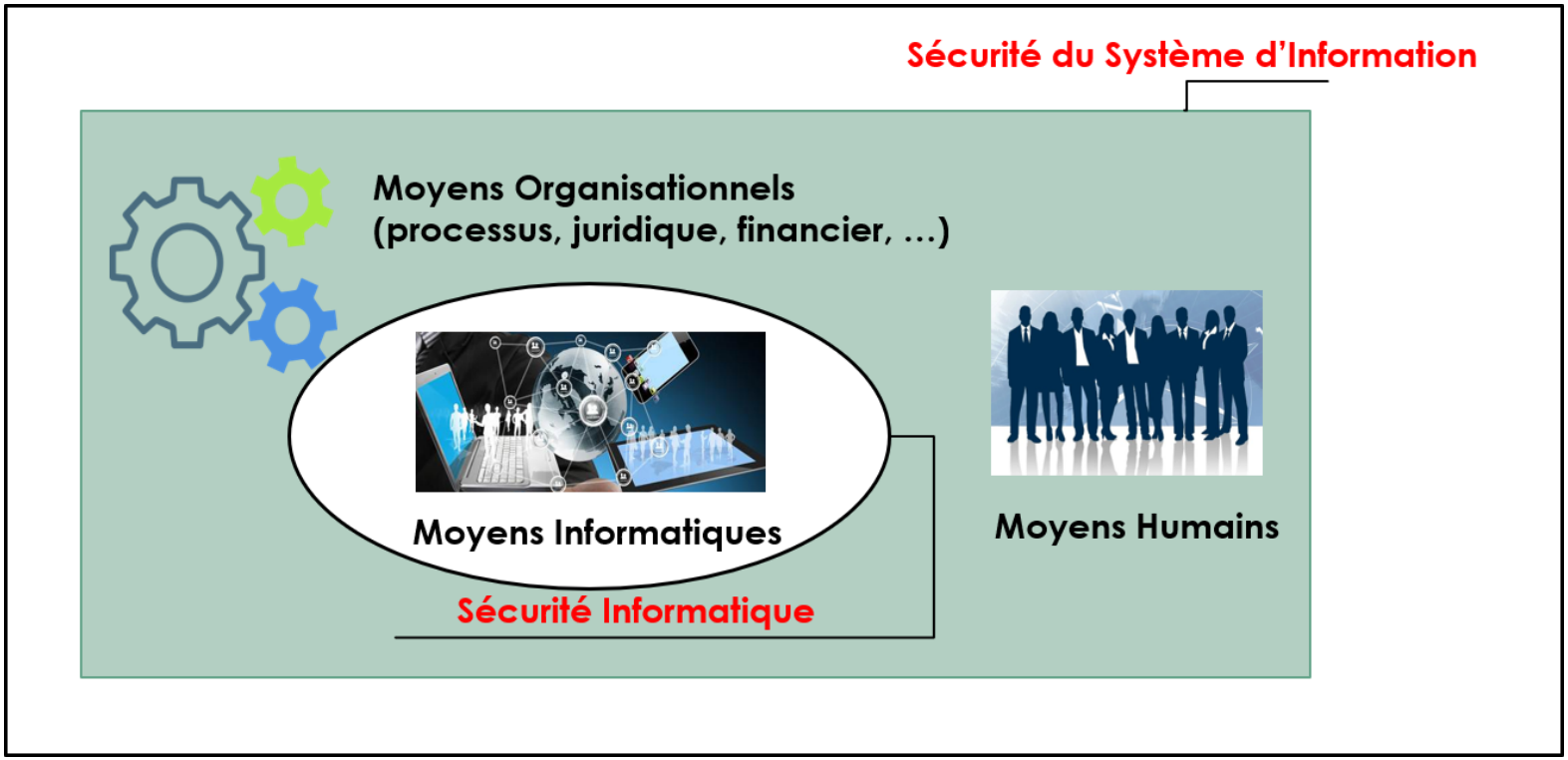
Sécurité Informatique

- La notion de sécurité informatique couvre l'ensemble des **moyens**, **outils**, **techniques** et **méthodes** pour garantir que seules les personnes ou autres systèmes **autorisés** interviennent sur le système et ont **accès aux données**, sensibles ou non :
  - Autoriser l'utilisation prévue.
  - Prévenir l'utilisation non intentionnelle.
- La sécurité informatique, d'une manière générale, consiste à **assurer** que les ressources **matérielles ou logicielles** d'une organisation sont uniquement **utilisées dans le cadre prévu**.

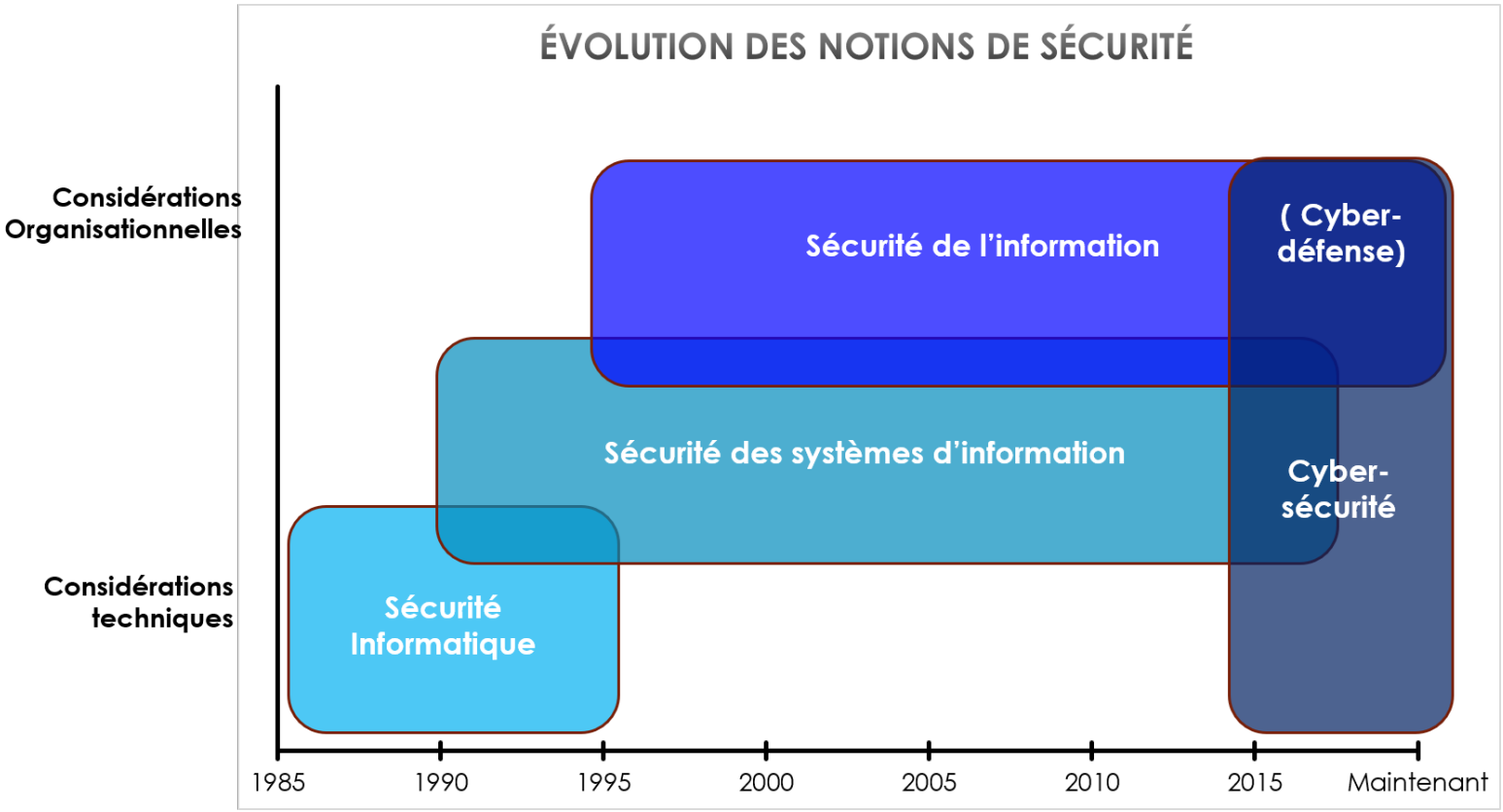
Système d'information et système informatique

- L'informatique ou le système informatique (incluant les réseaux et télécommunications) : concerne l'ensemble des **matériels**, **logiciels** et moyens de **télécommunication** visant à automatiser les fonctions et les informations ; il est la partie automatisée du système d'information. (Exemple : ordinateur, routeur, logiciel ou serveur, etc.)
- Le système d'information : est tridimensionnel et comprends l'ensemble des moyens **informatiques**, **organisationnels**, et **humains**, permettant le traitement, la modification, la création, le stockage et la diffusion de l'information.

Système d'information et système informatique



Évolution


ÉVOLUTION DES NOTIONS DE SÉCURITÉ
Considérations Organisationnelles
Considérations techniques
Sécurité de l'information
(Cyber-défense)
Sécurité des systèmes d'information
Cyber-sécurité
Sécurité Informatique
1985
1990
1995
2000
2005
2010
2015
Maintenant

Sécurité des Systèmes d'Information (IT Security)

- Ensemble des mesures **techniques** et **non techniques** de protection permettant à un système d'information de résister à des événements susceptibles de compromettre des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Sécurité de l'Information (Information Security)

- Mesures qui permettent d'implémenter et d'assurer la sécurité des systèmes d'information incluant le système informatique (Computers Systems).
- La sécurité de l'information se focalise sur la protection de **l'information**. Elle dépasse la champ de la sécurité informatique en s'intéressant aux actifs informationnels selon une approche par le risque.

Cybersécurité (Cybersecurity)

- État recherché pour un système d'information lui permettant de résister à des événements issus du **cyberespace** susceptibles de compromettre la sécurité des données stockées, traitées ou **transmises** et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.
- La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la **cybercriminalité** et sur la mise en place d'une cyberdéfense.

Sécurité et Sûreté

- **Sûreté (safety)** : La sûreté correspond à la démarche, ainsi qu'aux méthodes et dispositions, visant à limiter les risques de nature **accidentelle** (sans malveillance), étant susceptibles d'avoir des répercutions sur l'environnement du système.
- **Sécurité (security)** : La sécurité correspond à la démarche, méthodes et dispositions, visant à limiter les risques de nature **malveillante** (provenant d'une entité voulant nuire).

Besoins en Sécurité

- Matériels informatique omniprésent
- Prix abordable du matériel
- Simplicité des logiciels
- Utilisation des réseaux et Internet

Niveaux de sécurité

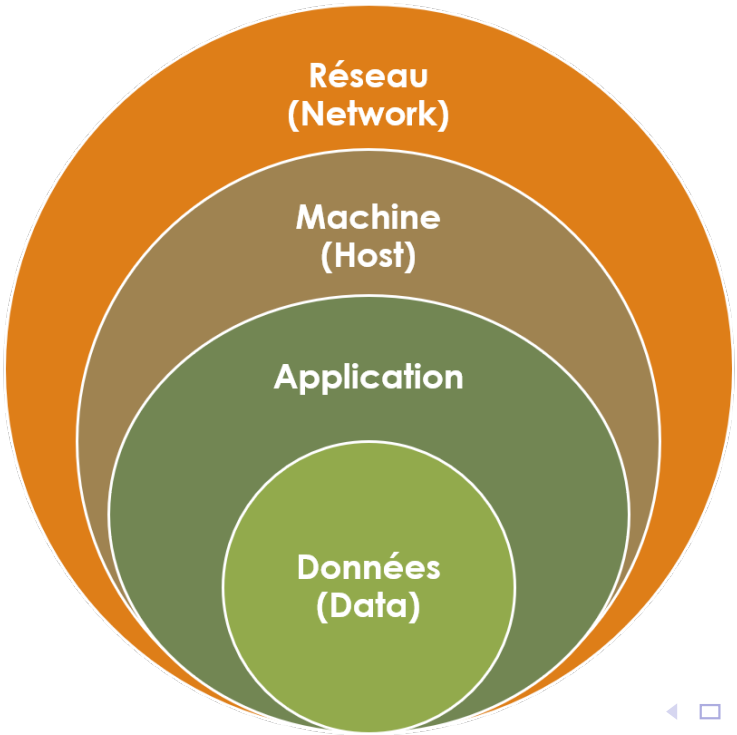
La sécurité existe à plusieurs niveaux :

- La portée de l'information.
- Durée de vie de l'information.

Portée de l'information

La sécurité existe à plusieurs niveaux :

- **La portée de l'information.**
- Durée de vie de l'information.



Durée de vie de l'information

La sécurité existe à plusieurs niveaux :

- La portée de l'information.
- **Durée de vie de l'information.**

Objectifs de Sécurité

- Confidentialité (Confidentiality)
- Intégrité (Integrity)
- Disponibilité (Availability)
- Authentification (Authentication)
- Non-répudiation (Non-repudiation)

Confidentialité

- La confidentialité est le maintien du secret des informations.
- Dans le cadre d'un système informatique ou système d'information, cela peut être vu comme une protection des données contre une **divulgation** non autorisée.
  - Limiter leur accès par un mécanisme de **contrôle d'accès**.
  - Transformer les données par des procédures de **chiffrement**.

Disponibilité

- La disponibilité est fortement liée à l'accessibilité. Une ressource doit être accessible, avec un temps de réponse acceptable.
- La disponibilité des services, systèmes et données est obtenue :
  - par un dimensionnement approprié.
  - par une gestion opérationnelle des ressources et des services.
- Un service doit aussi être assuré avec le minimum d'interruption en respect avec l'engagement établi.
- De plus des pertes de données sont possibles si l'enregistrement et le stockage ne sont pas gérés correctement, d'où l'importance d'une haute disponibilité d'un système et de la mise en place d'une politique de **sauvegarde**.

Intégrité

- L'intégrité permet de certifier que les données, les traitements ou les services n'ont pas été **modifiés, altérés ou détruits** tant de façon intentionnelle ou accidentelle.
- L'altération est principalement occasionnée par le média de transmission mais peut provenir du système d'informations.

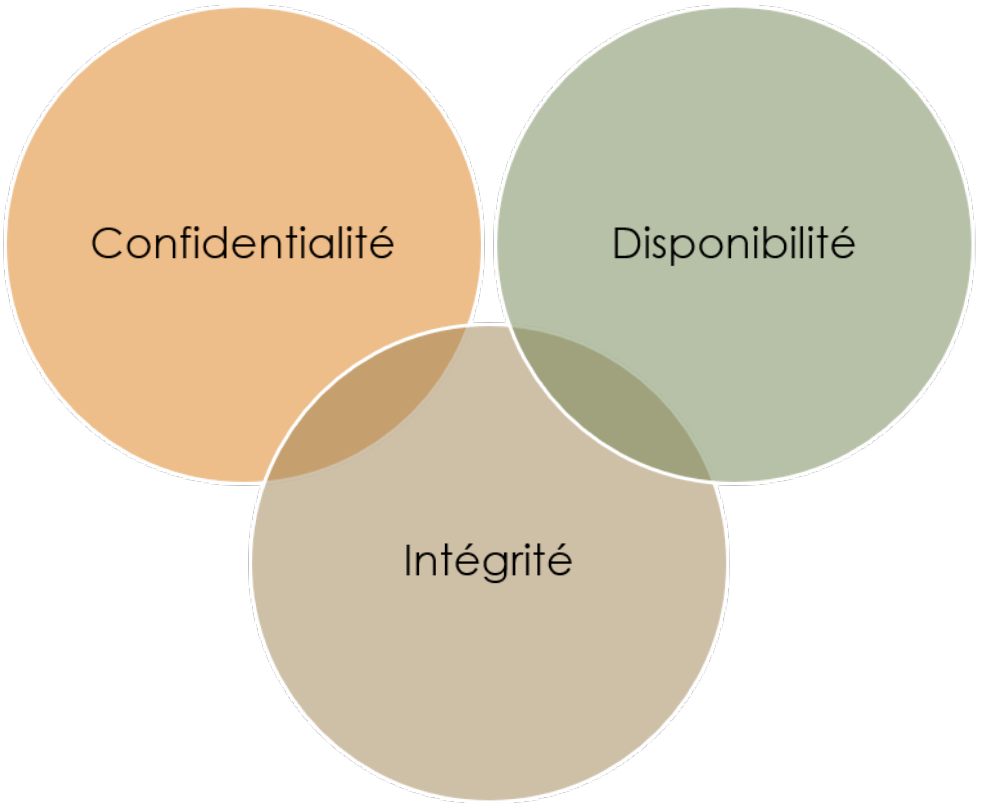
Authentification

- L'authentification consiste en l'identification de la source d'une données et la garantie de l'authenticité de la source.
- Afin d'assurer l'authentification les mesures suivantes doivent être mises en place :
  - **La confidentialité et l'intégrité** des données d'une personne.
  - **La non répudiation**, c'est à dire qu'une personne identifiée et authentifiée ne peut nier une action.
- L'identification peut être vu comme un simple login de connexion sur un système
- L'authentification peut être un mot de passe connu seulement par l'utilisateur.

Non-répudiation

- La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu.
- A cette notion sont associées :
  - **L'imputation** : une action a eu lieu et automatiquement un enregistrement, preuve de l'action, est effectué
  - **La traçabilité** : mémorisation de l'origine du message
  - **L'auditabilité**: capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement.
- L'existence de fichiers journal (log) permet de garantir l'imputation et l'audit.

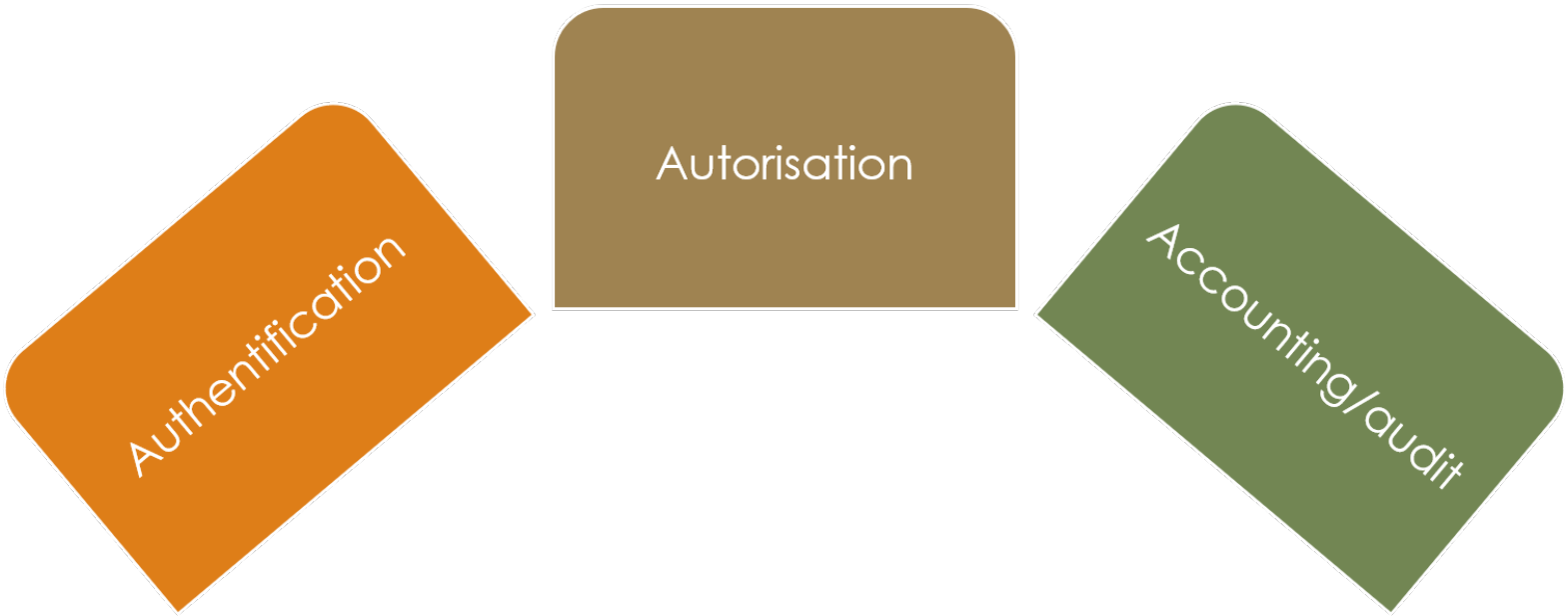
Triade CIA



Triade CIA

- Le triangle CIA (Confidentiality – Integrity – Availibility) présente les grands axes de la sécurité.
- Modèle de base pour les autres modèles.
- Le triangle opposé existe également : DAD (Disclosure – Alteration – Disruption / Divulgation - Modification - Interruption).

Le protocole AAA

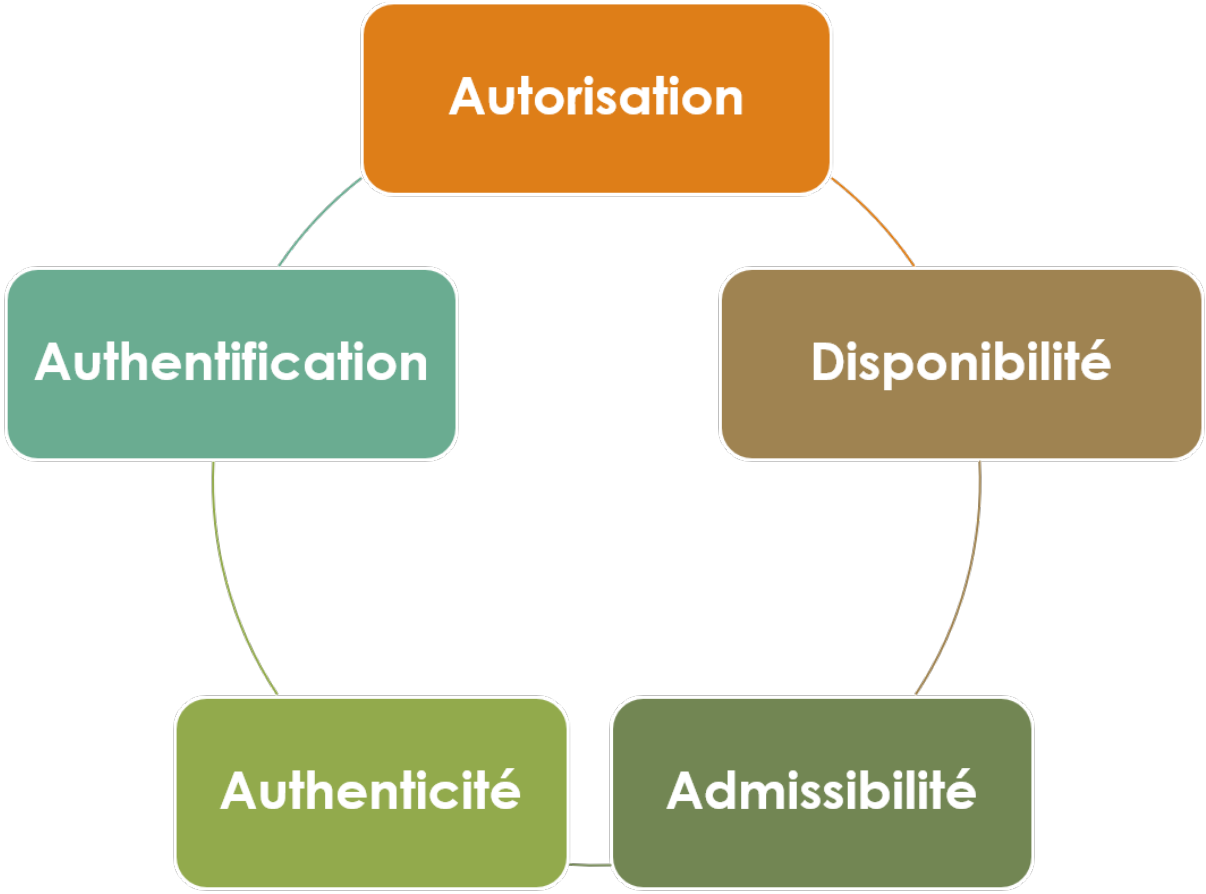


Le protocole AAA

La triangle CIA ne traite pas le contrôle d'accès → Protocole AAA (Authentication – Autorisation – Accounting & Auditing / Authentification – Autorisation – Traçabilité)

- Authentification : un processus de vérification de l'identité d'une entité afin d'autoriser l'accès.
- Autorisation : spécification des droits d'accès vers les ressources informatiques en définissant des politiques d'accès.
- Traçabilité : sauvegarde et exploitation des traces d'accès et tentatives d'accès aux éléments tracés.

Le pentagone de confiance



Le pentagone de confiance

- Défini par Piscitello en 2006.
- Ce modèle précise la notion d'accès à un système, en plus du modèle CIA. Il précise la confiance que peut/doit avoir l'utilisateur.
- On y retrouve les notions :
  - Authentification : Qui êtes vous?
  - Autorisation : Qu'est ce que vous avez le droit de faire?
  - Disponibilité : Est-ce que les données sont accessible?
  - Intégrité : Est-ce que les données n'ont pas été altérées?
  - Admissibilité : Est-ce que la machine avec laquelle nous nous connectons ou travaillons, est fiable ? Est-ce qu'on peut faire confiance à la machine cible ?

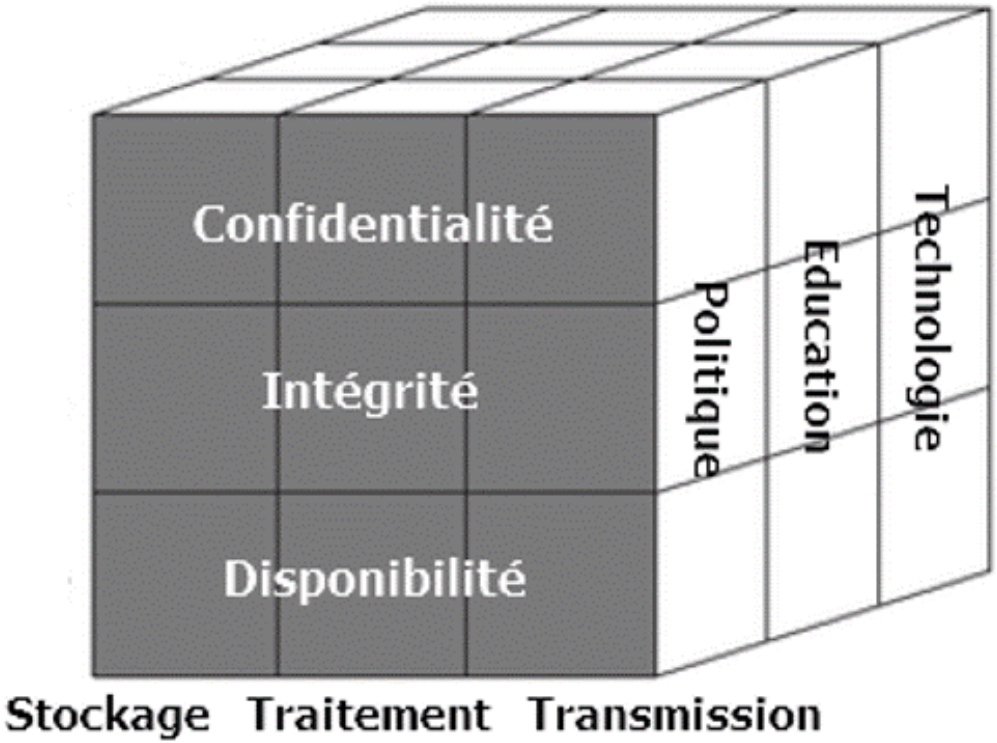
Parkerian Hexad

Parkerian Hexad

Ce modèle ajoute :

- Utilité : se réfère simplement à l'utilité (la valeur) des données.
- Contôle ou Possesion : la possibilité que des données confidentielles pouvant être possédées et contrôlées par une personne ou une partie non autorisée sans réellement violer ou enfreindre la confidentialité.

Le cube de McCumber



Le cube de McCumber

- Dans ce modèle la sécurité est décrite comme une grille cubique à trois dimensions.
- On y retrouve une dimension contenant les trois piliers de la sécurité (CIA), mais deux autres dimensions apparaissent :
  - L'état des données : le stockage, le traitement et la transmission.
  - Les méthodes : les principes et règles à adopter pour atteindre le niveau de sécurité souhaité à savoir : politiques de sécurité, éducation et apprentissage du facteur humain, et technologie représentant les solutions matérielles et logicielles.

Les domaines de sécurité

- Tous les domaines de l'informatique sont concernés par la sécurité.
- En fonction de son domaine d'application, la sécurité informatique se décline en :
  - Sécurité physique.
  - Sécurité de l'exploitation.
  - Sécurité logique.
  - Sécurité applicative.
  - Sécurité des télécommunications.

Sécurité Physique

- Concerne tous les aspects liés de l'environnement dans lequel les systèmes se trouvent.
- La sécurité physique passe donc par :
  - Des normes de sécurité.
  - Protection de l'environnement (incendie, température, humidité, ...).
  - Protection des accès.
  - Redondance physique.
  - Plan de maintenance préventive (test, ...) et corrective (pièce de rechange, ...).

Sécurité de l'exploitation

- Concerne tous ce qui touche au bon fonctionnement des systèmes d'exploitation.
- Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.

Sécurité Logique

- La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel.
- Elle repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation
- Elle repose également sur :
  - les dispositifs mis en place pour garantir la confidentialité dont la cryptographie
  - une gestion efficace des mots de passe et des procédures d'authentification
  - Des mesures antivirus et de sauvegarde des informations sensibles
- Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier leur degré de sensibilité (normale, confidentielle, top secrète, ...)

Sécurité Applicative

- Concerne le développement pertinent et son intégration harmonieusement dans les applications existantes .
- Cette sécurité repose essentiellement sur
  - Une méthodologie de développement
  - La robustesse des applications
  - Des contrôles programmés
  - Des jeux de tests
  - Un plan de migration des applications critiques
  - Un plan d'assurance sécurité ...

Sécurité des Communications

- Consiste à sécuriser le réseau afin d'offrir une connectivité fiable et de qualité.
- Il faut donc mettre un canal de communication fiable entre les correspondants, quels que soient le nombre et la nature des éléments intermédiaires.
- Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements.

Questions?