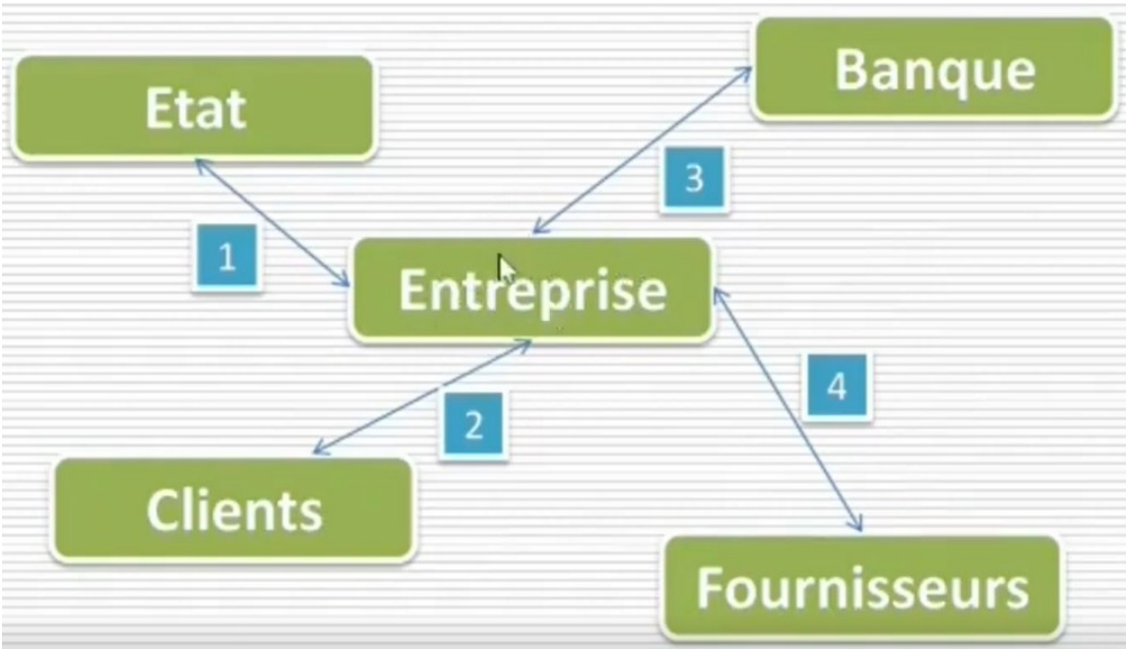
Koudou Z. Y-Serge

Sécurité informatique et cybersécurité

I- Introduction à la Sécurité informatique

Lorsqu'on parle de sécurité informatique, l'objectif visé n'est pas la sécurisation des ordinateurs eux-mêmes ou des matériels en réseau, mais c'est beaucoup plus de protéger un système d'information d'une organisation en général (ministères, entreprises, écoles, ….). Tout ce qui est traitement d'une information : acquisition, stockage, transformation, diffusion, exploitation , gestion des informations. Cela correspond à plusieurs poste de travail. Les systèmes d'information sont de natures différentes : information financières, données médicales des patients, des données techniques ou des données personnelles. La protection des données personnelles concerne des particuliers beaucoup plus. Ces données constituent les biens des personnes et des entreprises et peuvent être très convoitées, elles sont les principales cibles des pirates. Ces données étant très importantes pour l'entreprise, elle est dans l'obligation de les protéger. Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser un système informatique. Les systèmes informatiques sont devenus la cible de ceux qui convoitent l'information. L'ordinateur est au cœur de ce système informatique. Donc assurer la sécurité de l'information, c'est assurer la sécurité des systèmes informatiques. Les

entreprises font face à plusieurs défis: état, clients, fournisseurs, banques. Leur système d'information doit rester ouvert avec ces partenaires pour échanger des données.



Ces partenaires constituent pour l'entreprise des pôles de vulnérabilité qu'il faut bien surveiller. Cela nous amène à la définition de la sécurité informatique :

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

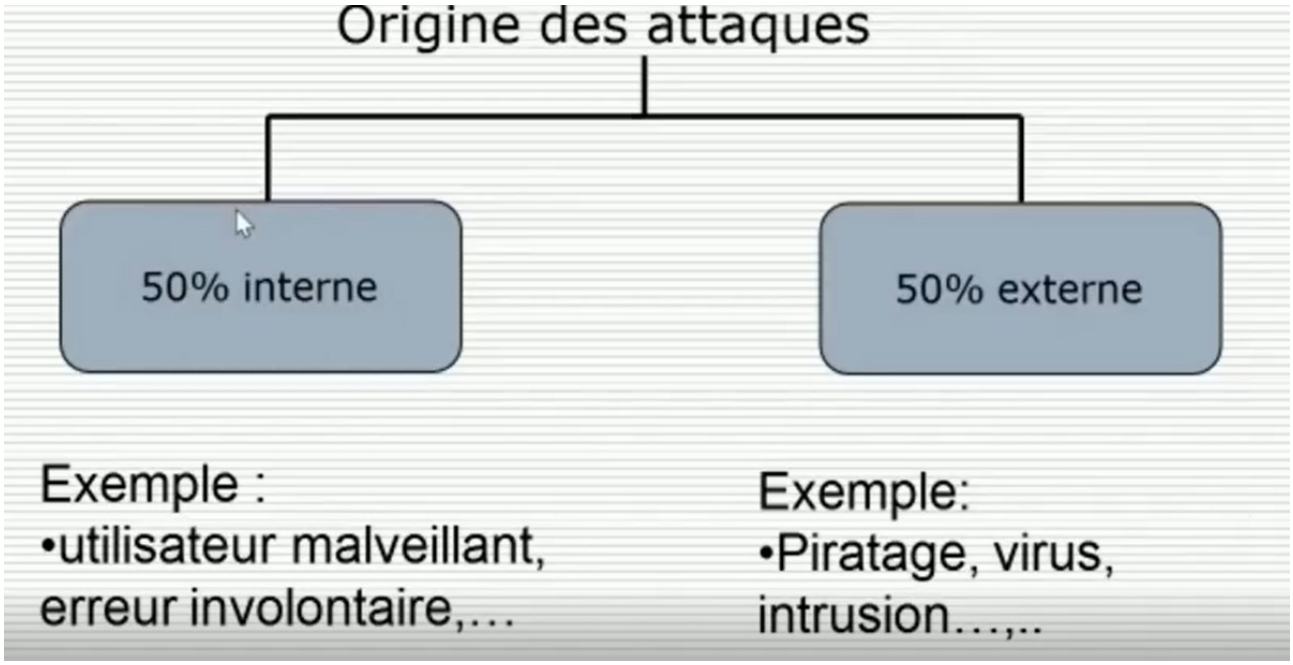
Remarque : Deux points importants dans cette définition:

1- on ne vise pas à éliminer les vulnérabilités puisqu'il y a toujours un risque, mais on vise à réduire au maximum la vulnérabilité.

2- D'un autre côté, on est face à deux types de menace :

- Des **menaces intentionnelles**, c'est-à-dire, que la personne a prémédite son acte (un pirate, un intrus, une personne de l'entreprise qui travaille pour un concurrent mal intentionné (un espion), ….)
- Des **menaces accidentelles** ça peut être un utilisateur mal formé qui peut ramener un document contaminé sur un support (clé USB, Disque, …) et l'introduire dans le système de l'entreprise, ou bien, Il ne sait pas installer des logiciels donc il télécharge des jeux ou des applications de manière automatique sur le site de l'entreprise, ce qui peut causer accidentellement des problèmes de sécurité, ou un mot de passe trop faible et pas sécurisé.

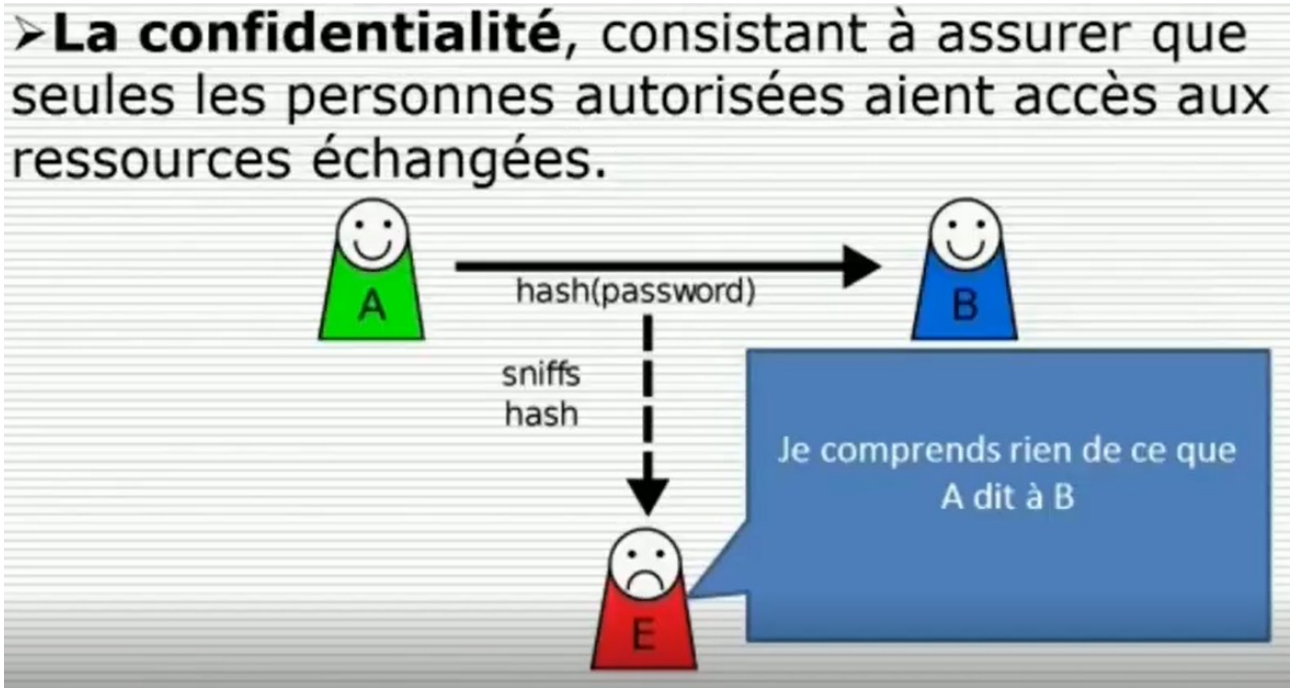
II- Les exigences fondamentales et objectifs de la sécurité informatique



Quand on fait de la sécurité informatique, il faut garder en mémoire que les attaques peuvent venir aussi bien de l'extérieur que de l'intérieur de l'entreprise.

Les exigences fondamentales et les objectifs de la sécurité informatique caractérisent ce à quoi s'attendent les utilisateurs du système informatique.

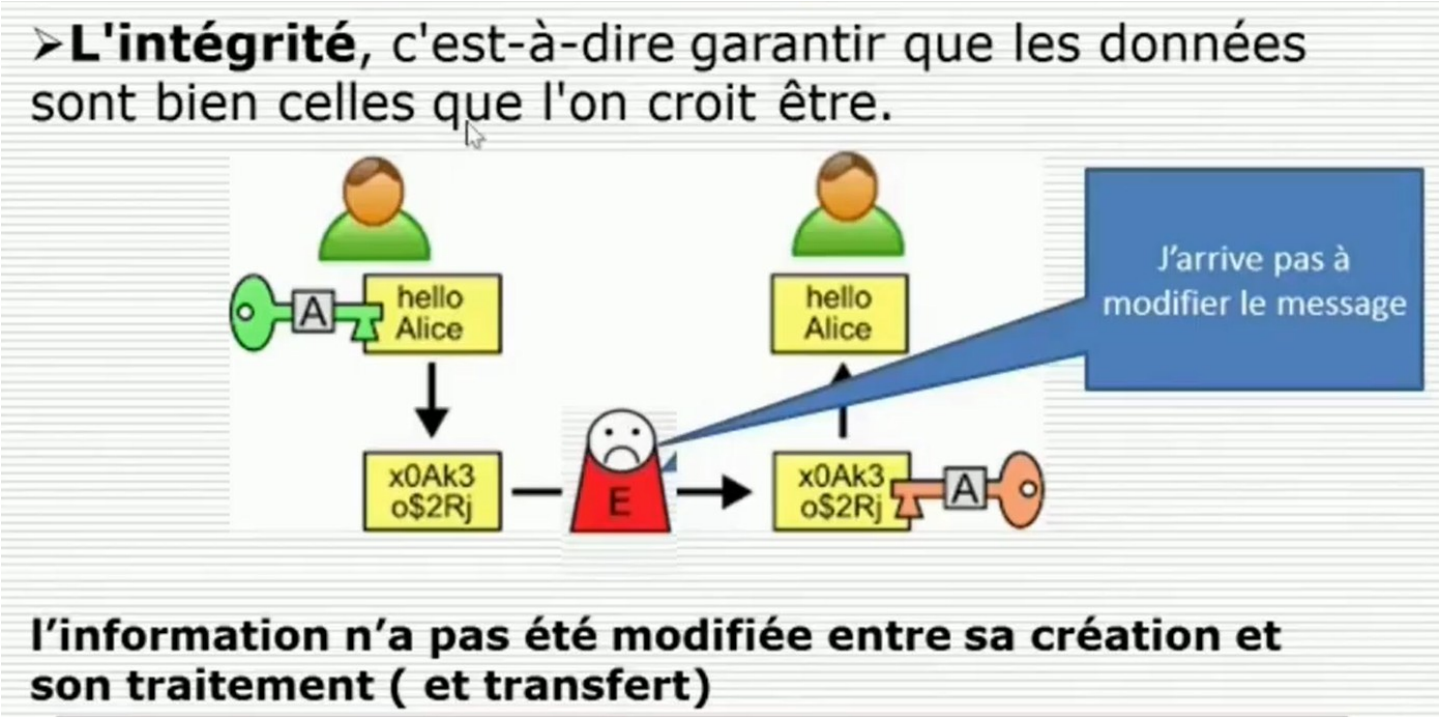
1- Autrement dit, moi un utilisateur de votre système informatique, à quoi vais-je m'attendre de votre système pour que je sois plus à l'aise ?



La confidentialité veut dire que les informations échangées entre les utilisateurs doivent rester confidentielles. Par exemple E ne doit pas savoir ce que A dit à B. Elle consiste donc à assurer que seule les personnes autorisées aient accès aux ressources échangées (données, photos, vidéos, ….) La notion de **confidentialité** est liée au maintien du **secret**, elle est réalisée par la protection des données contre une divulgation non autorisée (notion de protection en lecture). Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

• limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire ;

• les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.



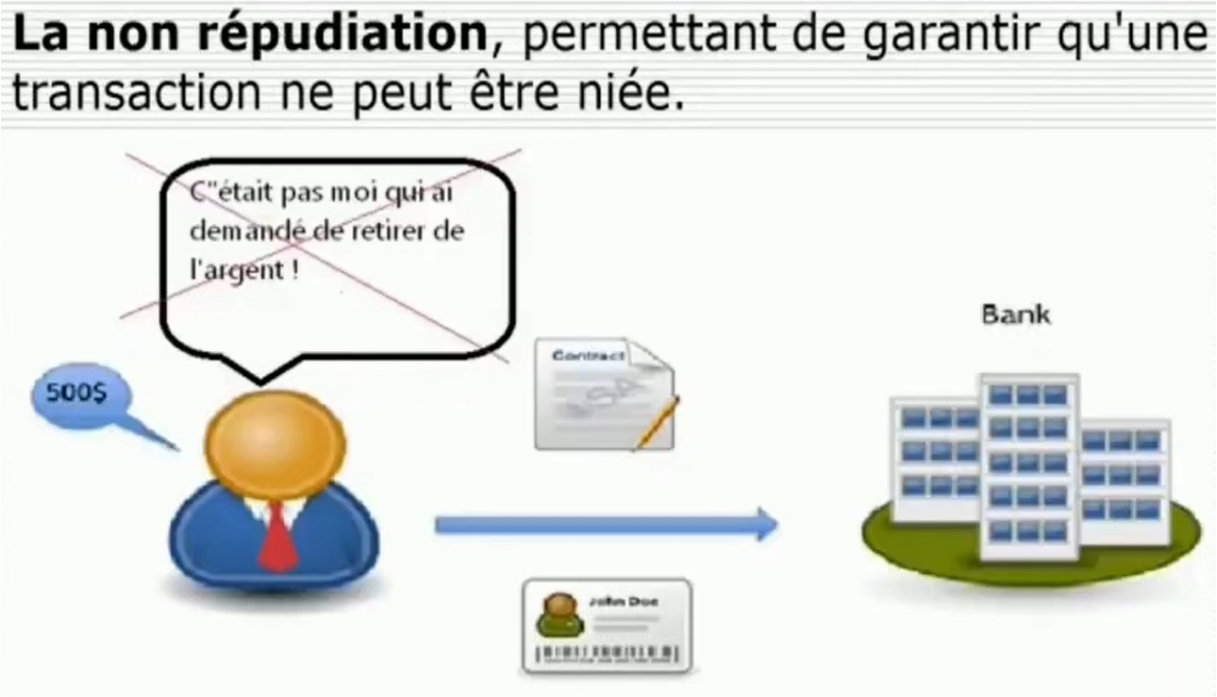
S'il y a modification, cela veut dire que le principe de l'intégrité n'a pas été respecté. Le critère d'**intégrité** des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles sont demeurées intactes, qu'elles n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires tant de manière intentionnelle, qu'accidentelle. Préserver l'intégrité des ressources et s'assurer que des ressources sont intègres sont l'objet de mesures de sécurité. Ainsi, se prémunir contre l'altération des données et avoir la certitude qu'elles n'ont pas été modifiées collabore à la qualité des prises de décision basées sur celles-ci. Si en télécommunication, l'intégrité des données relève essentiellement de problématiques liées au transfert de données, elle dépend également des aspects purement informatiques de traitement de l'information (logiciels d'application, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données). Des contrôles d'intégrité, par la mise en œuvre de mécanismes cryptographiques peuvent être effectués pour s'assurer que les données n'ont pas été modifiées lors de leur transfert par des cyberattaques.

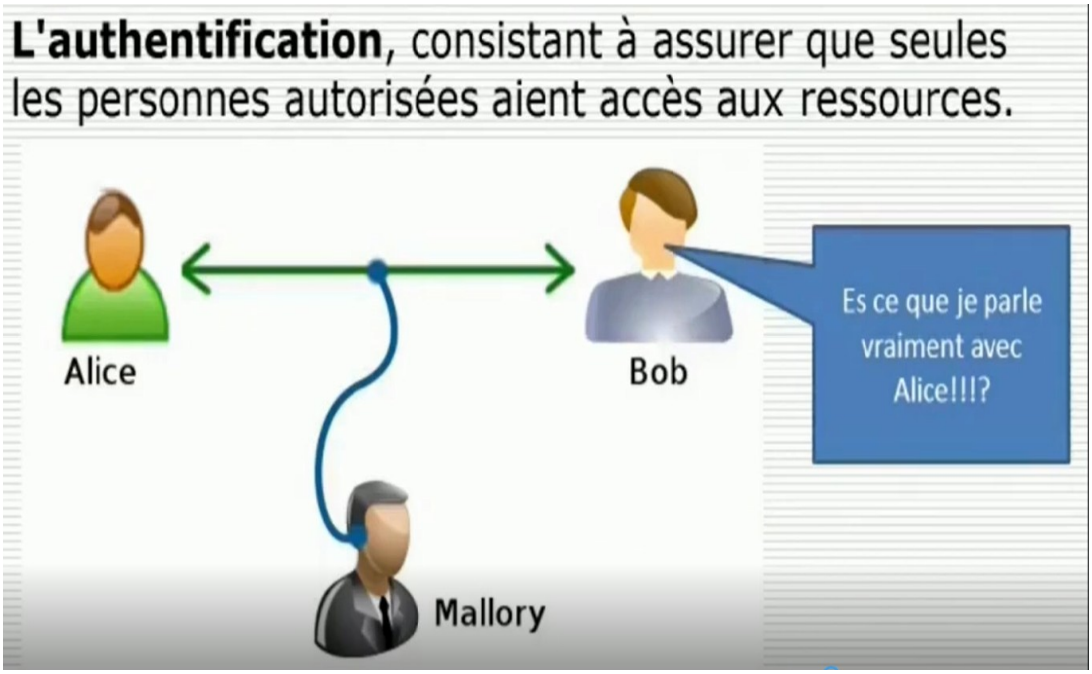
Notre système d'information doit fonctionner en permanence même s'il reçoit des attaques à l'extérieur comme à l'intérieur. Par exemple un serveur de messagerie qui permet aux utilisateurs de recevoir des mails, d'échanger des messages…Etc doit continuer de marcher quelles que soient les attaques. Pour cela il faut prévoir deux ou trois serveurs qui prennent la relève à chaque fois qu'un serveur tombe en panne. La **disponibilité** d'une ressource concerne la période de temps pendant laquelle le service qu'elle offre est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service détermine la **capacité** d'une ressource à être utilisée. Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa **disponibilité** est indissociable de sa capacité à être **accessible** par l'ensemble des ayants droit **(notion d'accessibilité)**. La disponibilité des services, systèmes et données est obtenue par un **dimensionnement approprié** et une certaine redondance ainsi que par une **gestion opérationnelle** et une **maintenance efficaces** des ressources.

La non-répudiation:

Koudou Z. Y-Serge

La non-répudiation veut dire que notre système doit garantir qu'une transaction ne peut être niée. Par exemple l'utilisateur qui retire de l'argent au guichet ou au distributeur ne doit pas dire par la suite que ce n'est pas alors que c'est lui. On assure le principe de la non-répudiation par des signatures numériques.





L’authentification, c’est s’assurer qu’on est entrain de parler à la bonne personne. La confidentialité et l’intégrité concernaient beaucoup plus les messages par la non-répudiation et l’authentification concernent beaucoup plus les personnes. Par exemple une personne qui va retirer de l’argent à un distributeur va taper son code qu’il est le seul à connaître normalement pour se faire authentifier et pour que le principe de la non-répudiation soit respecté.

Le respect de la vie privée concerne les personnes individuelles, les particuliers. Cela veut dire que moi, une personne lamda, je fais ce que je veux sur internet, sur mon portable, sur mon ordinateur et je ne veux pas que quelqu’un d’autre s’en mêle par exemple. Cela doit concerner les personnes majeures. Les mineures sont sous la tutelles des parents.

Pour résumer cette partie: on peut dire que :
La cybersécurité concerne la sécurité informatique, celle de l’information et la sécurité des réseaux, des environnements connectés à Internet. La sécurité des systèmes accessibles *via* le cyberespace et peut être mise en défaut, entre autres, par des **cyberattaques**. Ainsi, du fait de l’usage de plus en plus étendu d’Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d’importance variables, peuvent affecter les individus, les organisations ou

les États. La notion de **sécurité informatique** fait référence à des propriétés d'un système informatique qui s'expriment en termes de D**isponibilité** (D), d'I**ntégrité** (I), C**onfidentialité** (C)
Ces critères de base (critères ***DIC*****)** sont réalisés par la mise en œuvre de fonctions et services de sécurité, tels que ceux de contrôle d'accès ou de détection d'incidents par exemple. Des services de sécurité liés à **l'authentification** (notions d'authenticité et de véracité) ou encore à la **non-répudiation, à l'imputabilité**, ou à la **traçabilité** contribuent à protéger des infrastructures numériques.

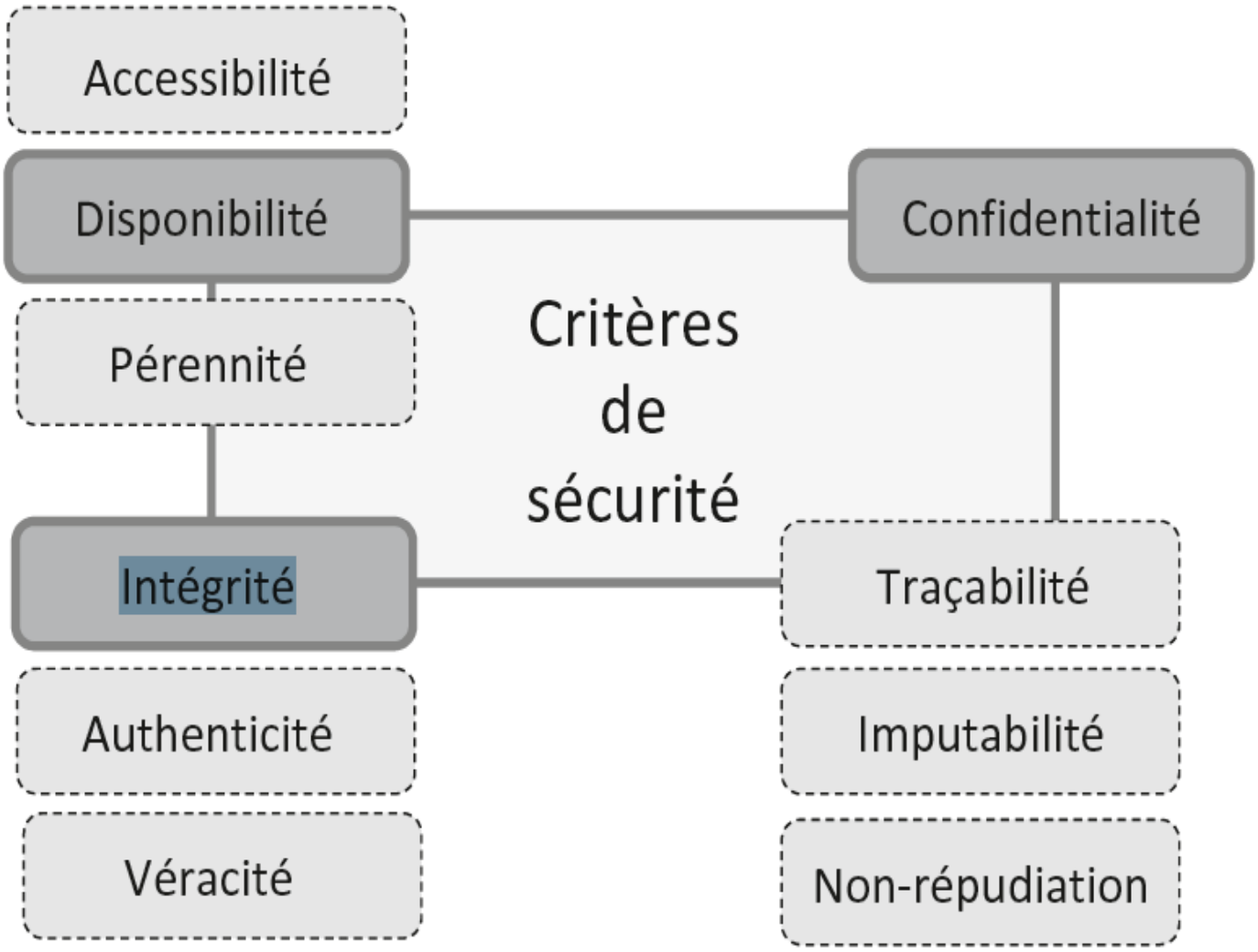


Figure 1.1 – Critères de sécurité.

Koudou Z. Y-Serge