Sécurité des Systèmes d'Information

(introduction)

université d'Alger 1 -
Benyoucef Benkhedda

Introduction:

La sécurité informatique est très importante

Introduction:

Les fonctionalités d'un système d'information:

- ✓ **Collecte d'informations:** permet le recueil des différentes informations **internes** (des entités du systèmes) ou **externes** (clients, fournisseurs, etc…).
- ✓ **Mémorisation d'information:** permet l'organisation et le stockage des informations collectées (papier, bases de données, magnétiques ou optiques.
- ✓ **Traitement de l'information:** consiste de la recherche, extraction, modification et consolidation des informations.
- ✓ **Diffusion de l'information:** à travers différents supports (papiers, orales ou numériques)

Définitions:

sécurité informatique:

- ✓ ensemble des **actions** et **décisions** permettant la conception, dévelopement et élaboration des différentes techniques afin d'assurer une protection des **biens** dans un systèmes d'information

- ✓ la stratégie de protection est décidée selon l'objectif voulu.

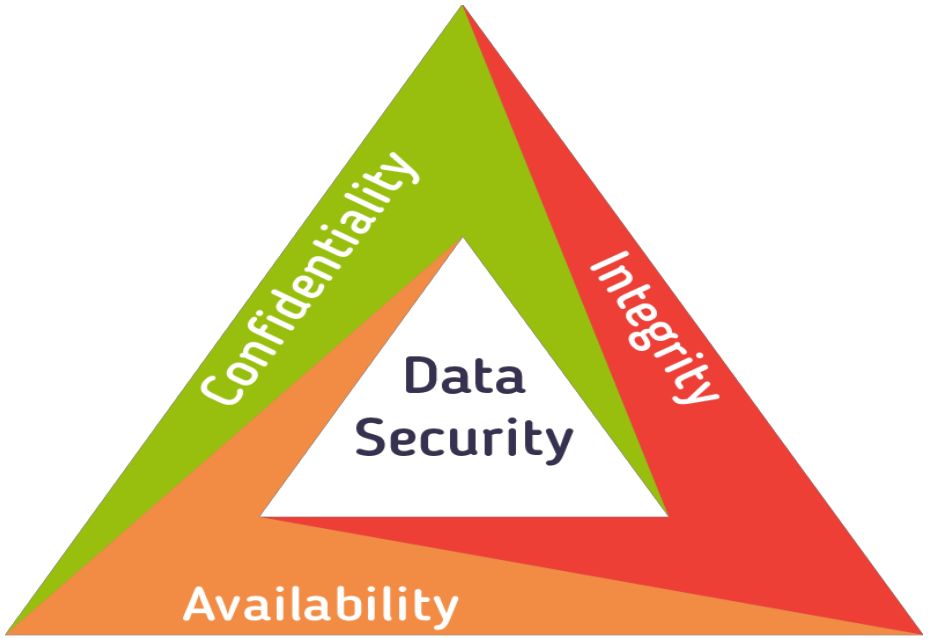
Définitions:

Protection de quoi (biens)?

- ✓Protection des équipements physiques
- ✓Qualité de l'environnement
- ✓Fiabilité des systèmes et tolérance de pannes
- ✓Systèmes de secours, sauvegardes, maintenance
- ✓Qualité de base des logiciels
- ✓Confidentialité, intégrité, disponibilité

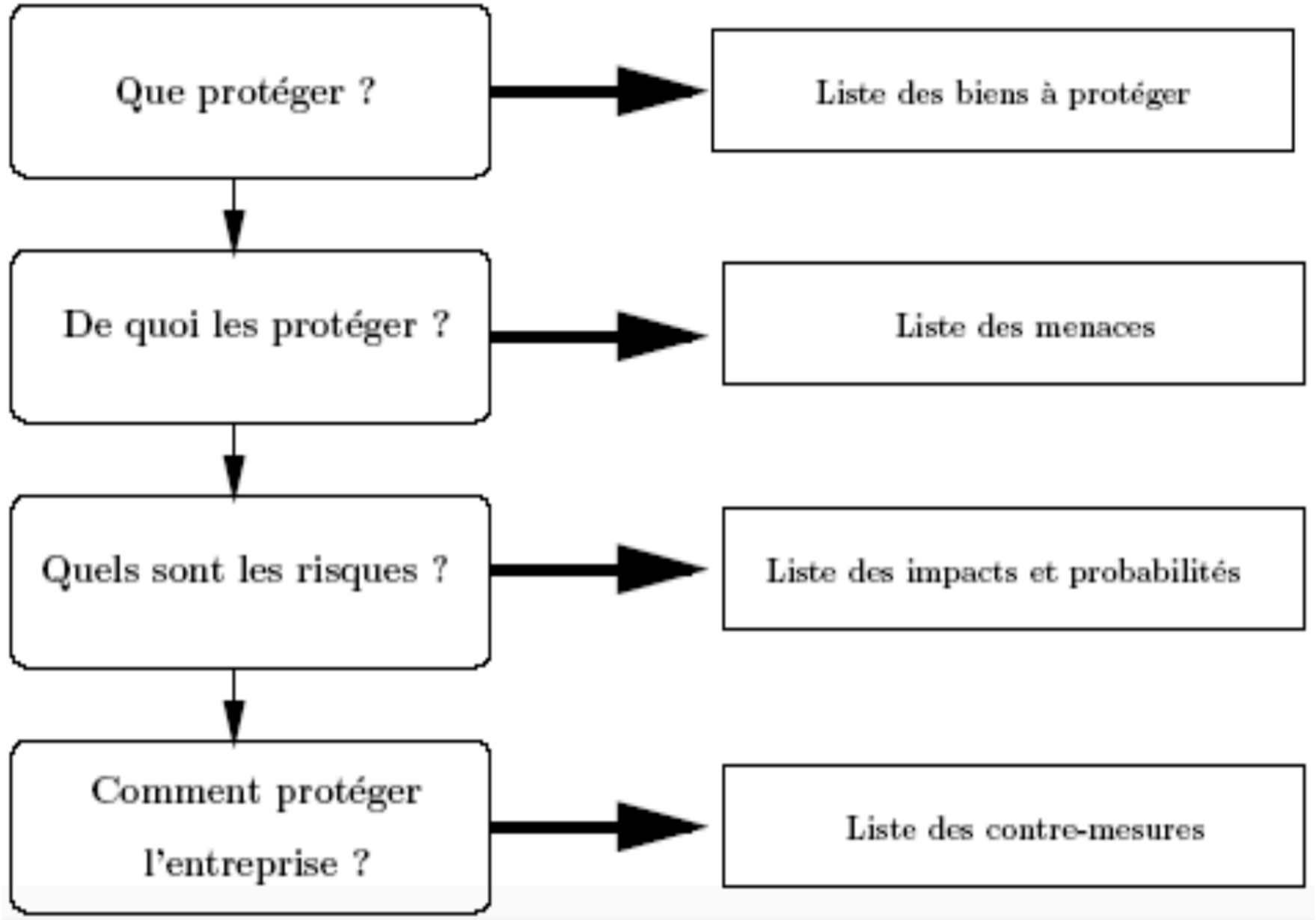
Protection contre quoi?

- ✓intrusion réseau
- ✓Virus, piratage, · · ·
- ✓Protection contre les accidents



Définitions:

La sécurité d'un tel système



Définitions:

La sécurité informatique consiste à la protection:

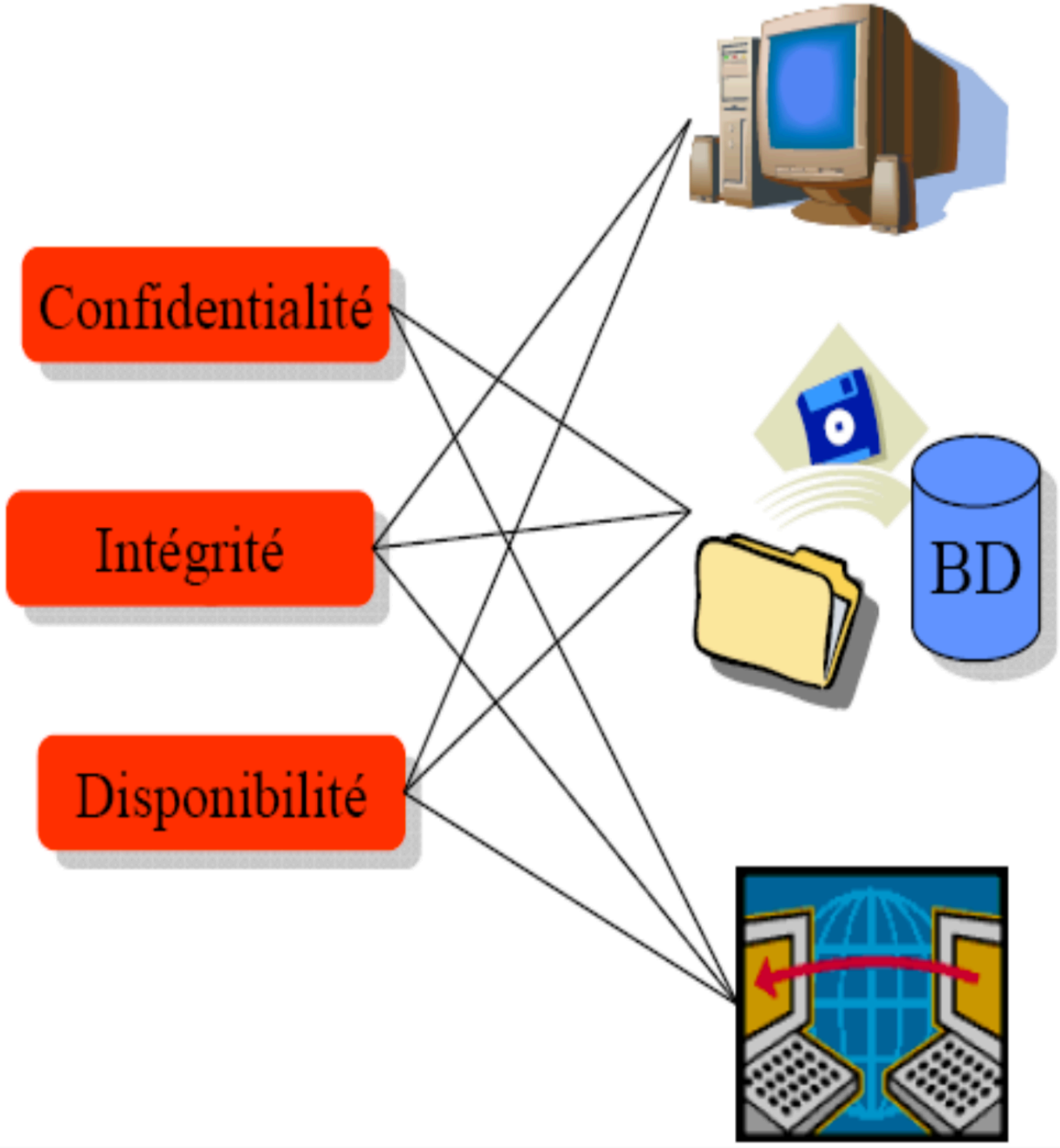
- ✓Systèmes
- ✓Information
- ✓Services et matériaux

Contre les menaces:

- ✓Accidentelles
- ✓délibérées

Atteignant leur:

- ✓Confidentialité
- ✓Intégrité
- ✓Disponibilité



Objectifs de la sécurité:

sécurité informatique (confidentialité):

- ✓Présente l'enjeux majeur de la sécurité et l'objectif le plus étudier
- ✓A été formellement utilisé pour la première fois dans le secteur militaire (chiffrement de Cesar) ensuite appliqué dans tous les secteurs (militaire et industriel)
- ✓Consiste de la dissimulation de l'information ou des ressources contre la lecture inapropriée

"Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché."

Objectifs de la sécurité:

sécurité informatique (Intégrité):

- ✓Se refére à la confiance aux données et ressources (crédibilité)
- ✓Ses mécanismes peuvent être classés en deux catégories: mécanismes de prévention, mécanismes de détection
- ✓Mécanismes de prévention permettent d'empêcher la **modification non-autorisée** et la **modification d'une façon non-autorisée**
- ✓Mécanismes de détection permettent la détection des modifications déja faites accidentellement (erreur de transmission) ou forcément (compromis de la sécurité)

Objectifs de la sécurité:

sécurité informatique (Intégrité):

- ✓Travailler avec l'intégrité, contrairement à la confidentialité, repose sur les faits d'exactitude des données ainsi que la confiance à la source des données

"Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire."

Objectifs de la sécurité:

sécurité informatique (Disponibilité):

- ✓Un système indisponible est beaucoup plus pire qu'un système inéxistant
- ✓Se refére au principe qu'un utilisateur doit avoir le service quand il a besoin **émidiatement**
- ✓Un système qui répond tard est un système indisponible
- ✓Les systèmes reposent sur des modèles statistiques expectant des scénarios les plus possibles

"Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu."

Objectifs de la sécurité:

sécurité informatique (non-répudiation):

- ✓ça revient toujours à la confiance à la source de données

“Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.”

Objectifs de la sécurité:

sécurité informatique (authentification):

“L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.”

références utils:

- ✓ Computer Security Handbook, S.Bosworth, M.E.Kabay, E. Whyne, 15/04/ 2014, 9781118127063
- ✓ Computer Security: art and science 2nd edition, Matt Bishop, 12/10/2018, 9780321712332
- ✓ Programming Windows Security, Keith Brown, 15/07/2000, 9780201604429
- ✓ Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications), D. R. Stinson, 11/01/2005, 9781584885085
- ✓ Introduction to Modern Cryptography: Principles and Protocols, J. Katz, Y. Lindell, 31/08/2007, 9781584885511
- ✓ Introduction to Cryptography with Coding Theory (2nd Edition), Wade Trappe and Lawrence C., 01/01/2006, 9788131714768
- ✓ Cryptography and Network Security: Principles and Practice, William Stallings, 24/02/2016, 9780134444284
- ✓ Cryptographie appliquée, Bruce Schneier, 08/01/2017, 9782711786763
- ✓ Sécurité informatique - Cours et exercices corrigés, G. Avoine, P. Junod, P. Oechslin, S. Pasini, 16/10/2016, 9782311401684
- ✓ Tableaux de bord de la sécurité réseau (3éme édition), C. Llorens, D. Valois, B. Morin, L. Levier, 26/08/2012, 9782212128215
- ✓ Computer System and Network Security (Computer Science & Engineering), Gregory B. White, Eric A. Fisch, Udo W. Pooch, 10/10/1995, 9780849371790