

Méthodologie de la sécurité informatique

(introduction et rappels)

université d'Alger 1 -
Benyoucef Benkhedda

mais avant...

le master!!!

Objective du module:

Comprendre les attaques pour mieux se défendre

Contenu du module:

- ✓ **Chapitre 1:** introduction à la sécurité informatique
rappel sur les notions de bases de la sécurité informatique
- ✓ **Chapitre 2:** management de la sécurité informatique (SMSI)
présentation de la partie théorique dans le processus de développement des systèmes de sécurité
- ✓ **Chapitre 3:** Méthodes d'attaques et menaces informatiques
présentation des différentes attaques informatiques et la méthode de **fonctionnement** et non pas de leur **utilisation**
- ✓ **Chapitre 4:** Mécanismes d'implémentation de la sécurité informatique
comprendre le fonctionnement des différentes techniques de protection des données

Contenu du module:

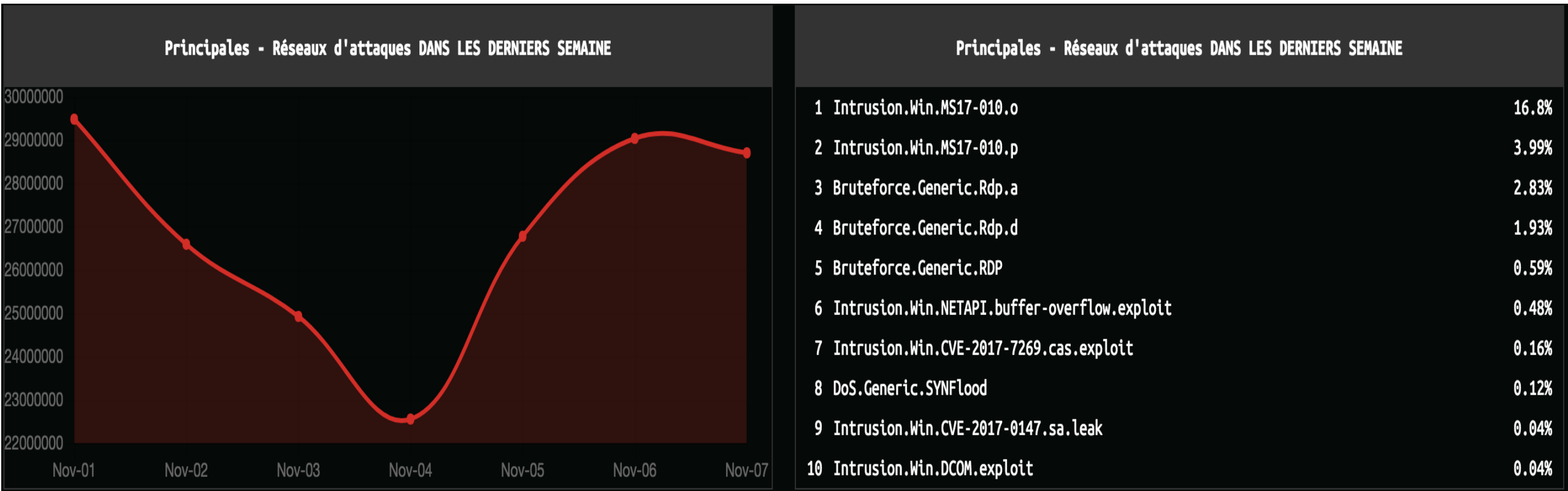
- ✓ **Chapitre 5:** Concepts de la préservation de la vie privée
comprendre le domaine de la préservation de la vie privée et sa relation à la sécurité informatique
- ✓ **Chapitre 7:** Audit de sécurité informatique et gestion des risques
comprendre le principe d'audit et les différents mécanismes d'audit et d'analyse de risques
- ✓ **Chapitre 8:** Sécurité des applications web
étudier les différents protocoles de sécurité des applications web

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 (3ème 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

Introduction:

✓ Attaques dans le monde



Introduction:

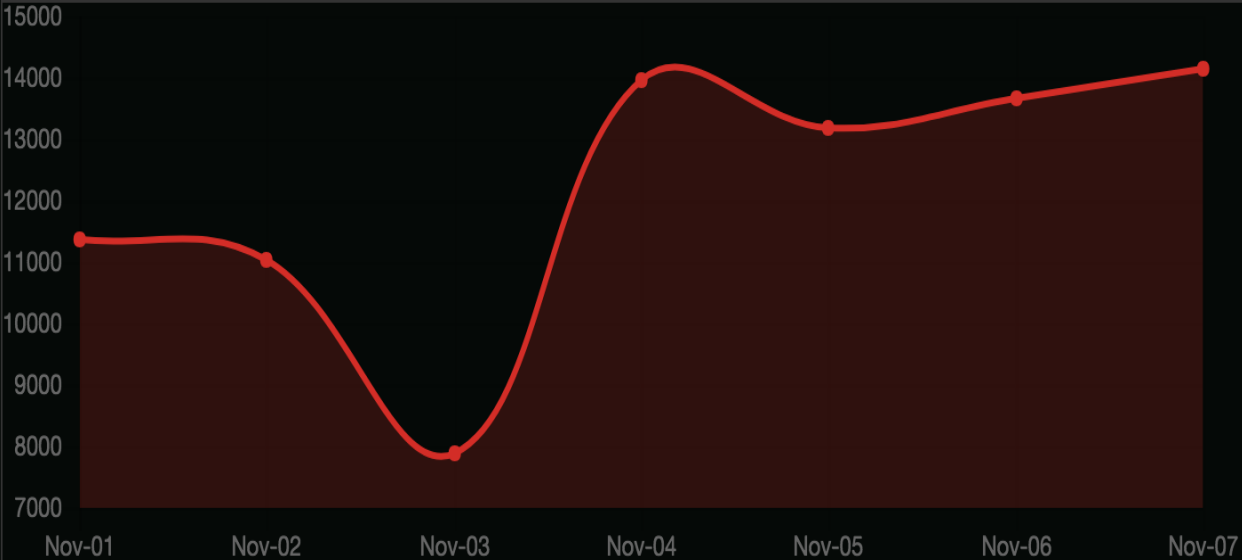
✓ Attaques dans le Algérie

Algérie

Réseaux d'attaques

PÉRIODE DE TEMPS: ☒ Dernière semaine ☐ Dernier mois

Principales - Réseaux d'attaques DANS LES DERNIERS SEMAINE



Principales - Réseaux d'attaques DANS LES DERNIERS SEMAINE

1	Intrusion.Win.MS17-010.o	27.22%
2	Intrusion.Win.NETAPI.buffer-overflow.exploit	6.39%
3	Intrusion.Generic.FTPD.PASS.buffer-overflow.attack	2.43%
4	Bruteforce.Generic.RDP	2.05%
5	Bruteforce.Generic.Rdp.a	1.98%
6	Bruteforce.Generic.Rdp.d	1.84%
7	Intrusion.Win.CVE-2017-7269.cas.exploit	0.76%
8	Intrusion.Win.MS17-010.p	0.21%
9	DoS.Generic.SYNFlood	0.19%
10	Bruteforce.Generic.Rdp.c	0.15%

Introduction:

**La sécurité informatique est
plus qu'importante**

Introduction:

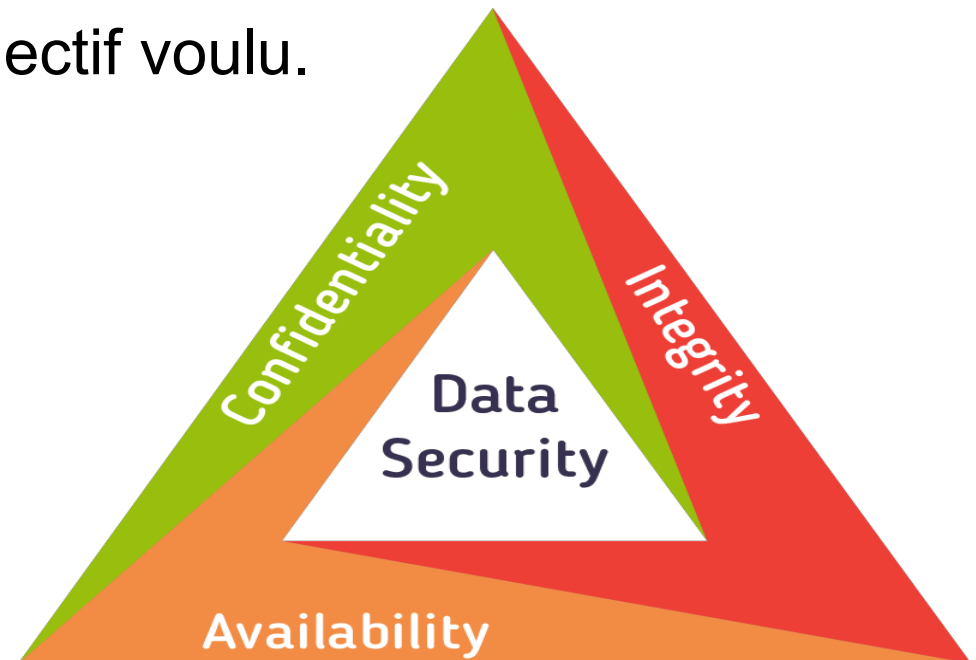
Les fonctionnalités d'un système d'information:

- ✓ **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**, **développement** 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)?

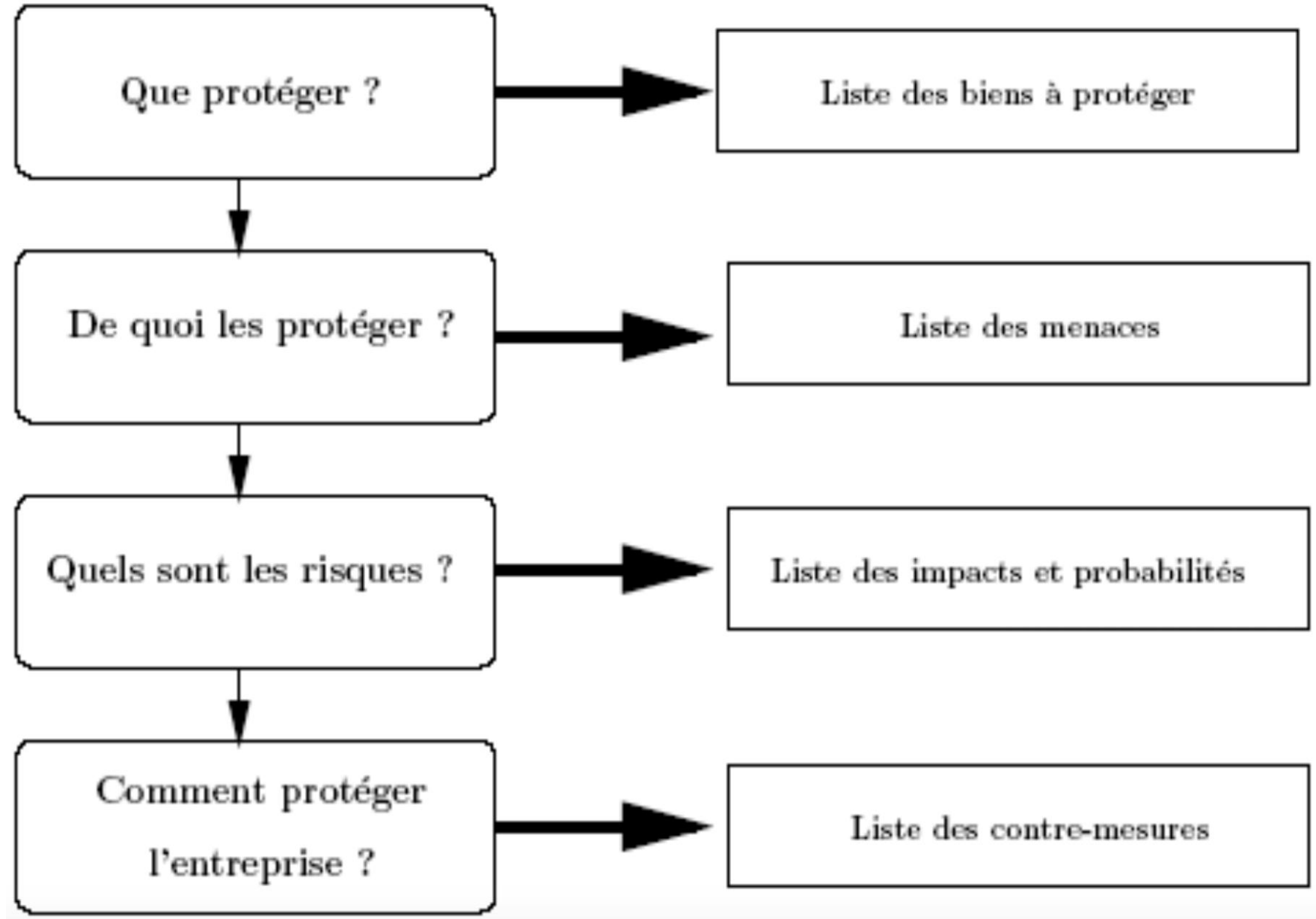
Définitions:

Protection de quoi (biens)?

- ✓ Protection contre les accidents
- ✓ Protection physique
- ✓ Qualité de l'environnement
- ✓ Fiabilité des systèmes, pannes, tolérance de pannes 
- ✓ Systèmes de secours, sauvegardes, maintenance
- ✓ Qualité de base des logiciels
- ✓ Confidentialité, intégrité, disponibilité ➤ intrusion réseau
- ✓ Virus, piratage, ...

Définitions:

La sécurité d'un tel système



Définitions:

La sécurité informatique consiste à la protection:

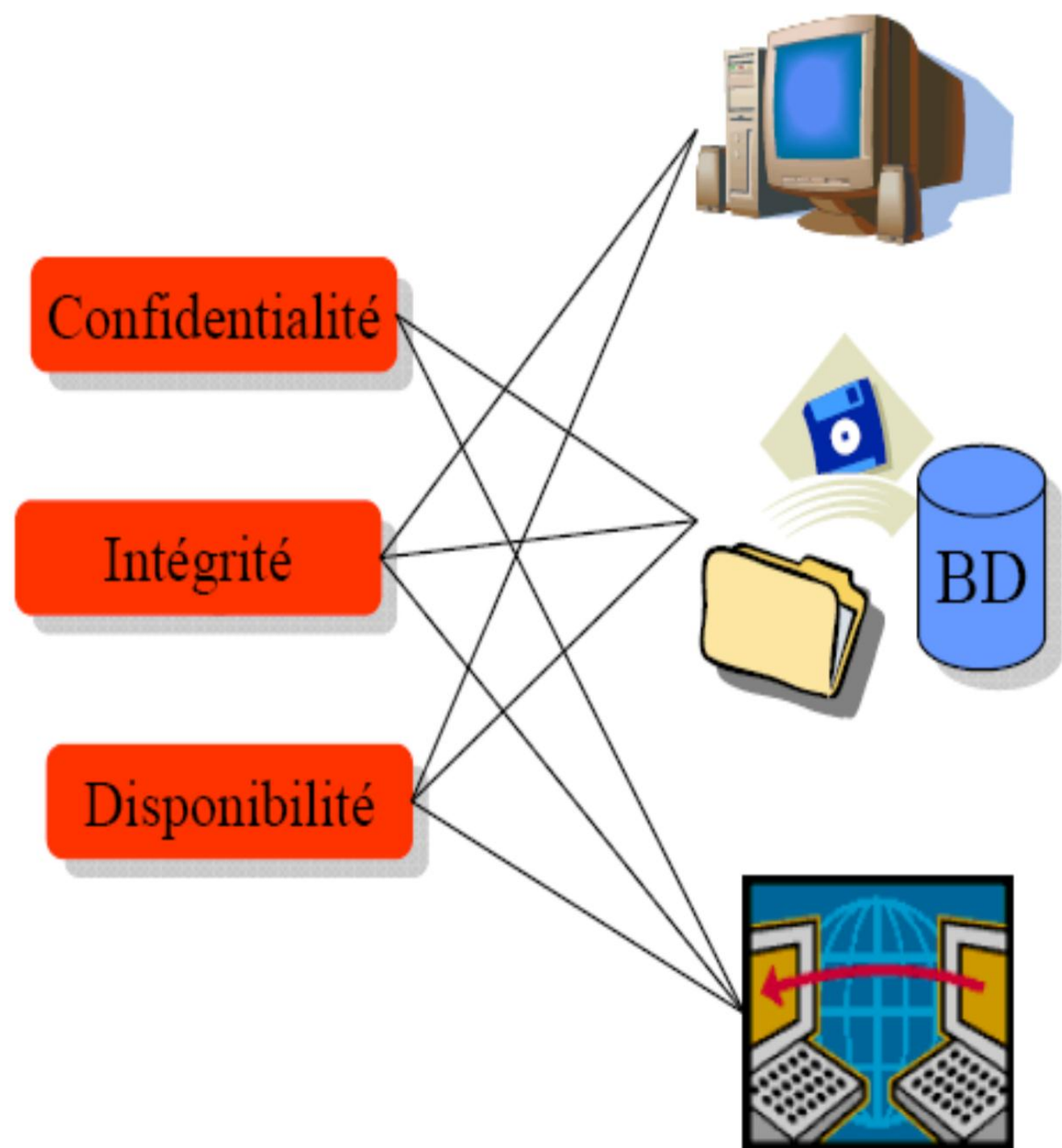
- ✓ Systèmes
- ✓ Information
- ✓ Services

Contre les menaces:

- ✓ Accidentelles
- ✓ dilébérées

Atteignant leur:

- ✓ Confidentialité
- ✓ Intégrité
- ✓ Disponibilité



Définitions:

sécurité informatique (confidentialité):

- ✓ Présente l'enjeux majeur de la sécurité et l'objectif le plus étudié
- ✓ 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 inappropriée

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

Définitions:

sécurité informatique (Intégrité):

- ✓ Se réfère 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 déjà faites accidentellement (erreur de transmission) ou forcément (compromis de la sécurité)

Définitions:

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.”

Définitions:

sécurité informatique (Disponibilité):

- ✓ Un système indisponible est beaucoup plus pire qu'un système inexistant
- ✓ Se réfère 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.”

Définitions:

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.”

Définitions:

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.”