Self Introduction to cyber Security

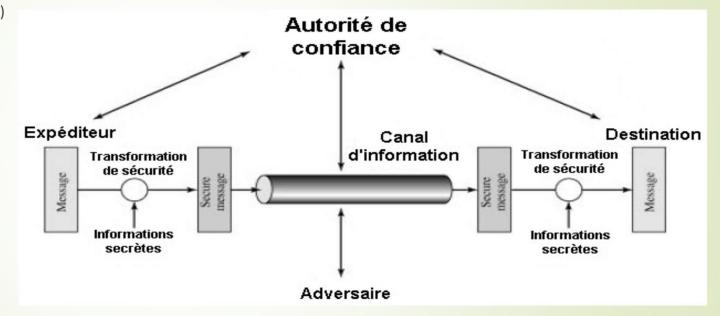
Travail à faire pour l'étudiant

Travail 1 à faire par l'étudiant

- Introduction générale
 - Qu'est que la sécurité
 - Pourquoi les systèmes sont vulnérables?
- Les enjeux de la sécurité des S.I.
 - Pourquoi les systèmes sont vulnérables
 - Pourquoi la sécurité est importante?
 - Définition de Sécurité, Protection, Dissuasion
 - Stratégie de sécurité
- Menaces de sécurité courante
- Type d'attaque d'un réseau & Techniques générales d'atténuation des risques
- Stratégie de sécurité de l'entreprise

Travail 2 à faire par l'étudiant

- L'architecture de sécurité OSI (X.800)
- Les services de sécurité
 - L'authentification
 - Le contrôle d'accès
 - La confidentialité des données
 - L'intégrité des données
 - La non répudiation
 - Le service de disponibilité
- Les mécanismes de sécurité
- Un modèle de sécurité réseau



- Documents recommandés ([RChp11]/ [RChp12]/ [RChp13]/[RChp14]
- TD à faire TD1

TD1

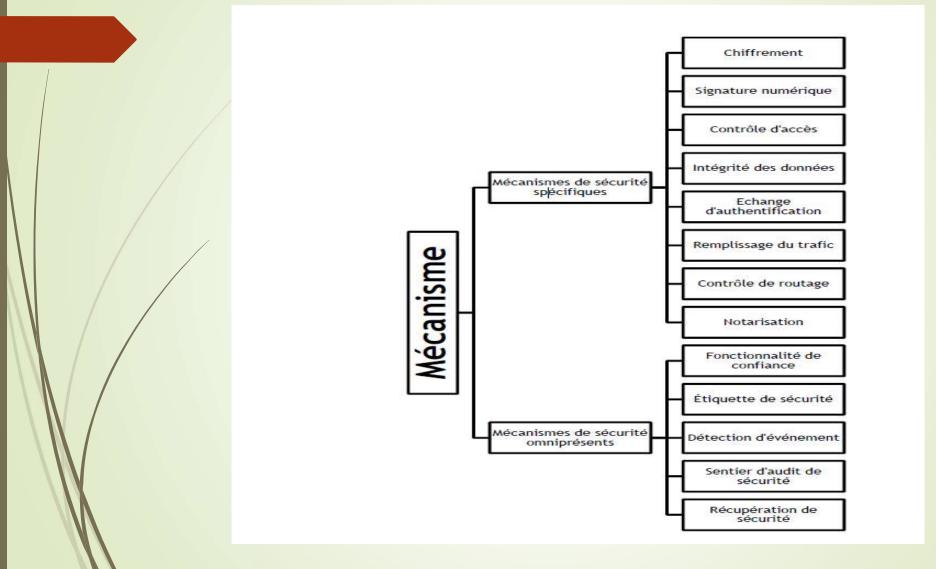
- 1. Quels sont les différents types de sécurité?
- 2. Quels sont les objectifs de la sécurité informatique?
- 3.Donner des exemples de mesures de sécurité permettant d'atteindre les objectifs que vous avez cité au dessus.
- 4.Donner une explication de la notion d'architecture de sécurité.
- 5. Identifiez les exigences fondamentales en sécurité informatique. Puis, expliquez la différence entre eux.
- 6. Présentez les mécanismes de sécurité définis dans X.800.
- 7.Donner les exigences de la sécurité informatique
- 8. Quels sont les services offerts par le contrôle d'accès ?
- 9. Donner des exemples et définir quel est la différence entre authentification, authentification à deux facteurs, et authentification à trois facteurs?

TD1: Correction

- 1. Quels sont les différents types de sécurité?
 - Sécurité Informatique
 - Sécurité du Cloud computing
 - Sécurité des mobiles
 - Sécurité des réseaux
 - Sécurité d'Internet
 - Sécurité du Web
 - ...etc
- 2. Quels sont les objectifs de la sécurité informatique?
 - Disponibilité
 - Intégrité
 - Confidentialité
 - Authentification
 - Non répudiation
- 3.Donner des exemples de mesures de sécurité permettant d'atteindre les objectifs que vous avez cité au dessus.
 - Par exemple on pourra citer :
 - Le chiffrement de données
 - Le contrôle d'accées
 - Les systèmes de détection d'intrusion
 - Pare feu
 - La redondance des infrastructures
 - La gestion des erreurs
 - La gestion des dysfonctionnements

- 4.Donner une explication de la notion d'architecture de sécurité.
 - Une architecture de sécurité est une structure qui fixe les dimensions organisationnelle, économique, technique, juridique et humaine dans lesquelles les solutions de sécurité doivent s'inscrire.
 - Définir une architecture de sécurité permet de visualiser la dimension générale de la sécurité informatique d'une entreprise et de bien identifier tous les éléments (outils, procédures mesures, réglementations, personnes ...) qui la composent. Et ceci dans le but de renforcer la cohérence et la complémentarité des solutions de sécurité retenues.
- ► 5. Identifiez les exigences fondamentales en sécurité informatique. Puis, expliquez la différence entre eux.
 - Disponibilité: Demande que l'information sur le système soit disponible aux personnes autorisées.
 - Confidentialité: Demande que l'information sur le système ne puisse être lue que par les personnes autorisées.
 - Intégrité : Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.
 - Non répudiation: Permettant de garantir qu'une transaction ne peut être niée.
 - ► Authentification: Consistant à assurer que seules les personnes autorisées aient accès aux ressources.

► 6. Présentez les mécanismes de sécurité définis dans X.800.



- 8. Quels sont les services offerts par le contrôle d'accès ?
 - Le contrôle d'accès offre 3 services essentiels:
 - Authentification (qui peut se connecter)
 - Autorisation (ce que les utilisateurs autorisés peuvent faire)
 - Responsabilisation (identifie ce qu'un utilisateur a fait)
- 9. Donner des exemples et définir quel est la différence entre authentification, authentification à deux facteurs, et authentification à trois facteurs ?
 - La différence est tout simplement dans le nombre de facteurs utilisés