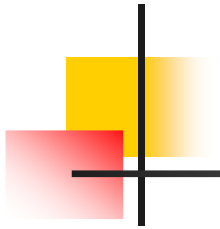
Mastère Pro ASRI

Chapitre 1 :

Présentation générale

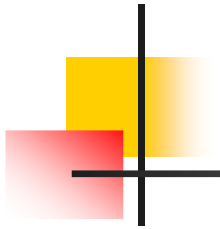
de la terminologie, des besoins, des services et des mécanismes de sécurité

Imen Khamassi



Plan

- Pourquoi, objectif de la sécurité
- Terminologie, menace, attaque, vulnirabilité, …
- Services de sécurité
- Attaques actives et passives
- Mécanismes de sécurité
- Domaine de sécurité : de confiance, de non confiance
- Gestion de risque
- Politique de sécurité



Pourquoi la sécurité ?

- L'information est une ressource stratégique.
- Une grande partie du budget d'une organisation est dépensée dans la gestion de l'information.
- Plusieurs types d'informations et plusieurs objectifs de sécurité pour chaque information.
- Insécurité dans les technologies de communications:
  - L'Ethernet est *promiscuous (confuse)*
  - TCP/IP envoi des données en clair (les données peuvent être visualisées) et les applications doivent sécuriser les données, etc.
  - L'adresse IP de la source peut être *usurpée*.

Pourquoi la sécurité ?

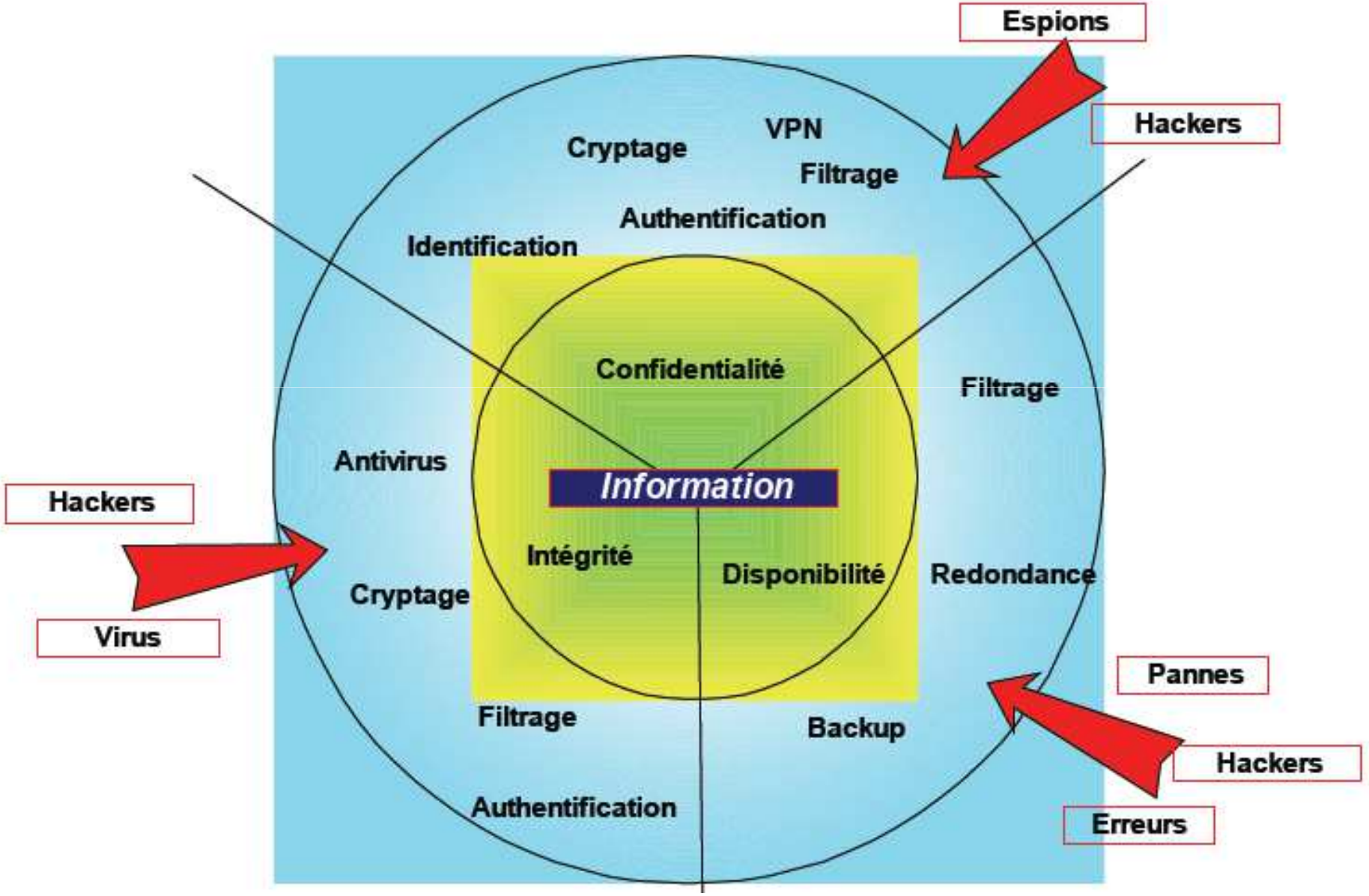
- Un système d'information représente un patrimoine essentiel de l'entreprise

  ➔ Nécessité de protection du SI (Sécurité du SI).

- Menaces aux systèmes d'informations : erreurs humaines, employés malhonnêtes, accès externe, etc.

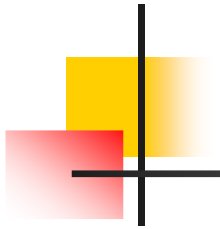
- Une intrusion à un SI peut causer des dégâts divers (vol des données confidentielles, pertes financières suite à des transactions erronées, perte de confiance des clients) et peut même menacer son existence sur le marché.

Objectifs de la sécurité



Que couvre la sécurité en général ?

- Prévention
  - Prendre des mesures afin d'empêcher les biens et les actifs d'être attaqués.
- Détection
  - Prendre des mesures afin de détecter quand, comment, par qui un actif ou un bien a été endommagé.
- Réaction
  - Prendre des mesures après un incident de sécurité afin de pouvoir restaurer les biens et les actifs, ou réduire l'impact de l'incident.



Intrus (*Intruder*) : Définition

- L'entité responsable d'une attaque de sécurité, capable de:
  - Accéder à des ressources internes propres à la cible de l'attaque de sécurité (appelée **victime**) de façon non autorisée.
  - Manipuler des données propres à la victime.
  - (Tenter de) contourner les mécanismes de sécurité mis en place.
  - Manipuler/agir sur le fonctionnement interne des machines.
  - Deviner/Décrypter les mots de passe utilisés pour protéger l'accès à des comptes utilisateurs ou à des services (type spécifique d'intrus : *cracker*).

Menace : Définition

- Une **menace** est «un signe qui laisse prévoir un danger»
- La **menace** peut être une personne, un objet, ou un événement qui peut créer un danger pour un bien (en terme de **confidentialité**, **intégrité** ou **disponibilité**).
- Une menace peut provenir de l'environnement naturel, physique ou peut être le résultat d'actions humaines.
- Exemple:
  - Un virus circule sur le réseau local.
  - Un programme installé sur la machine semble être en train d'épuiser les ressources disponibles (mémoire, CPU).

Une attaque de sécurité est la réalisation d'une menace.

Exemples de menaces/attaques

- Accès non autorisé.
- Perte de l'intégrité du système.
- Déni de service.
- Les virus.
- Coupure d'électricité.
- Panne du matériel.
- Divulgation des données confidentielles.
- Vol des données.
- Destruction des données.

Vulnérabilité : définition

- **Faille** ou **bug** pouvant être utilisé pour obtenir un **niveau d'accès illicite** à une **ressource d'information** ou des **privilèges supérieurs** à ceux considérés comme normaux pour cette ressource.

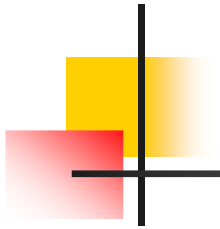
- La **vulnérabilité** caractérise les composants du système (matériel, logiciel, les règles, les procédures, personnel) susceptibles d'être attaquées avec succès.

- Une **vulnérabilité** est exploitée par une menace pour engendrer une attaque.

- Exemples de vulnérabilités :
  - Utilisation des mots de passe non robustes.
  - Présence de comptes non protégés par mot de passe.

Autres définitions …

- **La protection :** Processus d'anticipation qui vise à créer un environnement aussi sécurisé que possible.
- **La détection :** Processus qui vise à déterminer les activités inappropriées.
- **La réaction :** Processus de réponse à un incident de sécurité.
- **Identification :** Moyen utilisé pour identifier un utilisateur.
- **Authentification :** Processus de validation de l'identité d'un utilisateur.
- **La disponibilité :** Une ressource est disponible s'il est possible d'utiliser une ressource lorsque c'est nécessaire.
- **Risque :**
  - La probabilité qu'une menace exploitera une **vulnérabilité** du système.
  - C'est une fonction de deux arguments : **menace** et **vulnérabilité**, et donne comme valeur une probabilité.

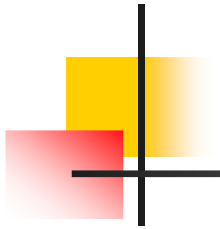


Services, mécanismes et attaques.

- Attaques de sécurité: Actions qui entraînent la compromission de la sécurité de l'information possédée par une organisation.

- Mécanismes de sécurité: Mécanismes désignés à détecter ou à empêcher ou à récupérer suite à une attaque de sécurité.

- Services de sécurité: Services améliorant la sécurité du **traitement** de données et du **transfert** d'informations. Ces services s'opposent aux attaques de sécurité et font utiliser des mécanismes de sécurité.



Services de sécurité

- **Objectif** :
  - Empêcher et détecter les attaques de sécurité.
  - Améliorer et renforcer la sécurité.
  - Répliquer les fonctions usuelles utilisées sur les documents physiques:
    - Signature, date.
    - Protection contre la divulgation, la falsification, et la destruction.
    - Certification.
    - Enregistrement.

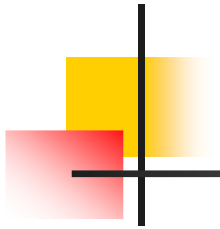
Services de sécurité (2)

- (X.800, Security architecture for OSI) regroupe les services de sécurité en 8 catégories :
  - Identification
  - Authentification
  - Contrôle d'accès
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Non répudiation
  - Non rejeu

Services de sécurité : Authentification

- S'assurer que l'origine du message soit correctement identifiée:
  - Assurer le receveur que le message émane de la source qui prétend avoir envoyé ce message.
  - Assurer l'**authenticité** des entités participantes: chacune des entités est celle qui prétende l'être.
  - Empêcher la **perturbation** de la connexion par une tierce partie qui se fait passer pour une entité **légitime** (émission ou réception non autorisée).

- **Techniques utilisées**: Cryptage, signature numérique, secret (mots de passes, PIN).



Services de sécurité: Contrôle d'accès

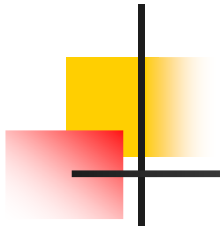
- Empêcher l'utilisation **non autorisée** d'une ressource (serveur, application, etc.)

- Le service de contrôle d'accès :
  - Définir qui a le **droit** d'accéder aux ressources ?
  - Déterminer sous qu'elles **conditions** ceci peut avoir lieu ?
  - Défini ce qu'une entité est **autorisée** de faire lors de l'accès à une ressource.

Services de sécurité: Confidentialité

Protection des données transmises contre les attaques passives, et protection des flux de données contre l'analyse.

- Préservation du secret des données transmises. Seulement les entités communicantes sont capable d'observer les données.
- Plusieurs **niveaux de confidentialité** :
  - Protection de tous les données échangées tout au long d'une connexion.
  - Protection des données contenues au niveau d'un seul bloc de donnée.
  - Protection de quelques champs des données échangées (pour une connexion ou un seul bloc de donnée).
  - Protection de l'information (source, destination, etc.) qui peut être déduite à partir de l'observation des flux de données échangés.



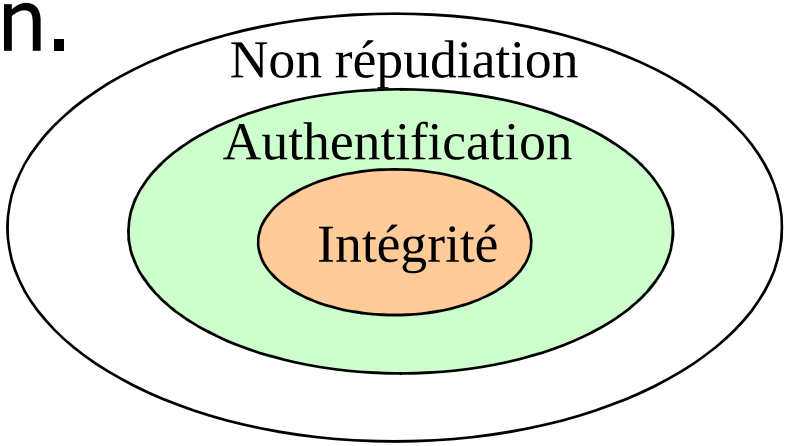
Services de sécurité: Intégrité

- Détecter si les données ont été modifiées depuis la source vers la destination
  - Service orienté connexion: Protection contre la duplication, la destruction, l'insertion, la modification, le rejeu, le reclassement, etc.
  - Service non orienté connexion: Protection contre la modification uniquement.

- Techniques utilisées: cryptage, signature numérique, contrôle d'accès, contrôle d'intégrité

Services de sécurité: Non répudiation

- Empêche l'émetteur ou le receveur de nier avoir transmis ou reçu un message.
  - Non répudiation d'envoi: Le destinataire prouve que la source prétendue vient démettre le message en question.
  - Non répudiation de réception: L'émetteur prouve que son message a été reçu effectivement par la destination prétendue.
- Techniques utilisées: signature électronique (asymétrique), notarisation.



La disponibilité : Propriété ou service ?

- X.800 et RFC 2828 définissent la disponibilité comme étant la **propriété** d'un système ou d'une ressource du système accessible et utilisable suite à la demande d'une entité autorisée.

- X.800 considère la disponibilité comme étant une **propriété** associée aux services de sécurité.

- La disponibilité considérée comme un **service:**
  - Un service qui protège un système pour assurer sa disponibilité.
  - Un service qui dépend du service de contrôle d'accès et des autres services de sécurité.

Les attaques de sécurité

- X.800 et RFC 2828 classifient les attaques selon deux classes :
  - **Attaques passives :** tentent de collecter ou utiliser des informations relatives au système, mais elles n'affectent pas les ressources du système.
  - **Attaques actives :** tentent d'introduire des modifications sur les ressources du système ou affecter leur fonctionnement normal.

Attaques de sécurité: Attaques passives

- Difficiles à détecter puisqu'elles n'entraînent aucune altération de données.
  - **Interception:** l'intrus est capable d'interpréter les données et d'extraire l'information (ex: email contenant des informations confidentielles, communication téléphonique) à partir du trafic échangé.
  - **Analyse de trafic:** même en présence de mécanismes de cryptage des données transmises, l'intrus peut extraire des informations utiles sur la communication en observant l'identité des utilisateurs, la fréquence et la longueur des messages échangés, etc.
- Détection difficile, protection assez simple (ex: cryptage)

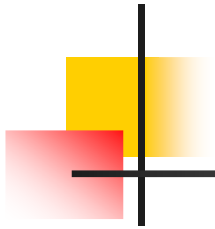
Attaques de sécurité: Attaques actives

- Mascarade: Une entité prétend être une **entité différente** afin d'obtenir des **privilèges supplémentaires**. Généralement ceci fait appel à d'autres techniques d'attaques actives.

- Rejeu (Replay): **capture passive** des données et leurs **transmission ultérieure** en vue de réaliser **des actions non autorisées**.

- Fabrication: Création et injection de messages afin de produire un effet non autorisé.

- Modification: Altération, destruction, ou reclassement d'une partie des messages échangés en vue de produire un effet non autorisé.



Attaques de sécurité: Attaques actives

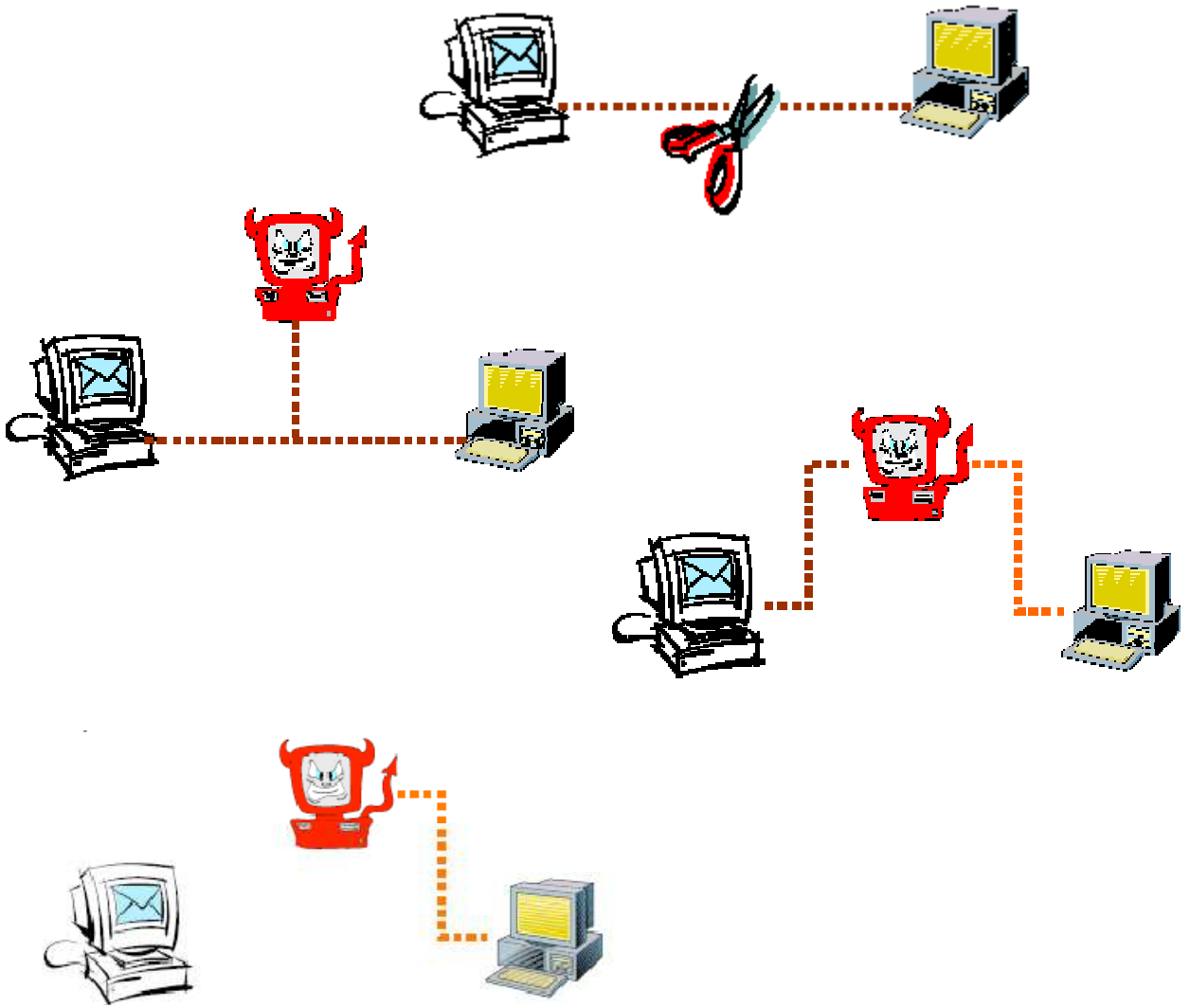
- Déni de service: Empêcher ou inhiber l'utilisation normale des moyens de communications:
  - Perturbation de l'utilisation normale des ressources (réseau ou système) en les surchargeant de trafic inutile pour dégrader leurs performances.
  - Interruption et suppression des messages en direction d'une destination particulière (ex: service d'audit sécurité)

- Difficulté d'empêcher les attaques actives de façon absolue à moins de protéger physiquement tous les moyens et chemins de communications en même temps.

- Le but est de détecter et de récupérer de n'importe quelle perturbation ou retard causé par ces attaques.

Termes à ne pas confondre

- Interruption
- Interception
- Modification
- Fabrication



Exemples d'attaques actives

- « A » transmet un fichier contenant des données à protéger à « B ». « C », qui n'est pas autorisé à lire ce fichier est capable de capturer une copie durant sa transmission.

- Un administrateur réseau « D » transmet un message à un ordinateur « E » afin de mettre à jour un fichier d'autorisation (contenant une liste d'utilisateurs). « F » intercepte ce message, le modifie, et le transmet à E.

- Au lieu d'intercepter le message, « F » construit son propre message, et le transmet à « E » comme si ce dernier émane de « D ».

- Un message est envoyé de « A » à « B » contenant des instructions pour des transactions. « A » nie avoir envoyé ce message.

Mécanismes de sécurité

- Cryptage
  - Utilisation **d'algorithmes mathématiques** pour transformer les messages en une forme **inintelligible**.
  - La transformation dépend d'un algorithme et de zéro à plusieurs clés.
- Signature numérique
  - **Ajout** de données, ou **transformation cryptographique irréversible**, à une unité de données afin de prouver la source et l'intégrité de cette unité de données.
- Échange d'authentification
  - Mécanisme assurant l'identité d'une entité à travers un échange d'information.

Mécanismes de sécurité

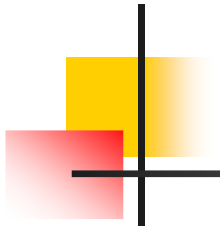
- Notarization:
  - Utilisation d'une tierce partie afin d'assurer certaines propriétés liées à un échange de données.
- Horodatage (Timestamping)
  - Inclusion d'une date et d'un temps correct dans un message.
- Mécanismes non cryptographiques:
  - *Traffic Padding* : Insertion d'un certain nombre de bits au niveau d'un flux de données pour faire échouer les tentatives d'**analyse du trafic**.
  - Détection d'intrusions
  - Implémentation de Firewalls

Domaine de sécurité

- **Problème**: Impossible de déployer un(des) mécanisme(s) de sécurité pour chaque composante (serveur, système, applications, …).

- **Solution**: Regrouper les composantes par domaine de sécurité et déployer un(des) mécanismes de sécurité pour tout le domaine.

- **Définition**: Un **domaine de sécurité** est une partie du **système d'information** qui regroupe des composantes de **niveau de sécurité** identique et sujets à des **menaces** de même nature.



Domaine de sécurité

- Un domaine de sécurité peut être géré et contrôlé indépendamment des autres domaines de sécurité.

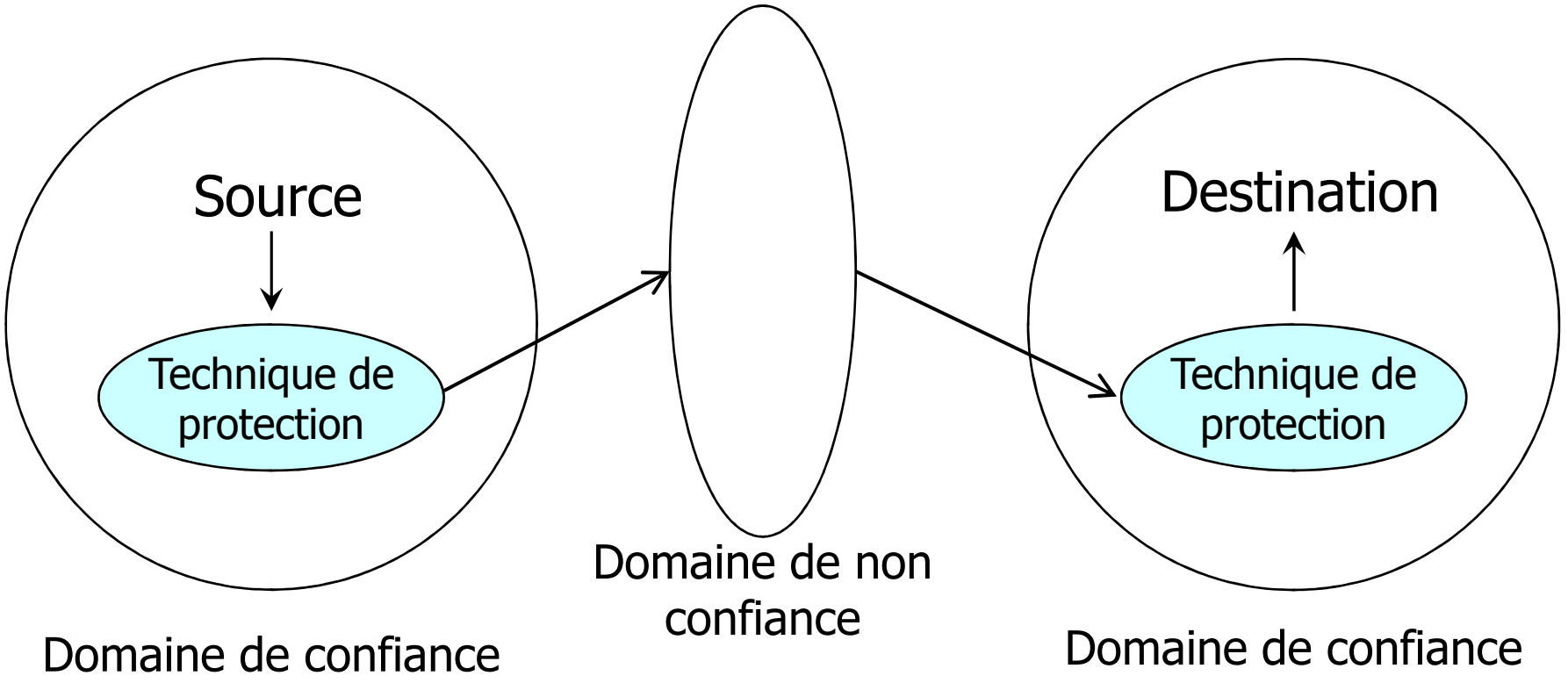
- Les règles de sécurité sont appliquées uniformément à tout le domaine.

- Un domaine de sécurité ne peut communiquer avec les autres domaines qu'au travers des **points de contrôle** bien définis.

Domaine de confiance

- **Problème**: La protection contre tout type d'intrus est **impossible**.
- **Solution**: Nécessité d'identifier les **domaines de confiance** avant de concevoir une solution ou une technique de sécurité.
- **Définition**: Un domaine de confiance comprend des systèmes (réseaux) ou une partie des systèmes (ordinateurs, modules) avec l'hypothèse: Aucun intrus n'est supposé être dans ce domaine de sécurité.
- **Propriété**: Un domaine de confiance est toujours attaché à un seul ou un groupe d'utilisateurs.

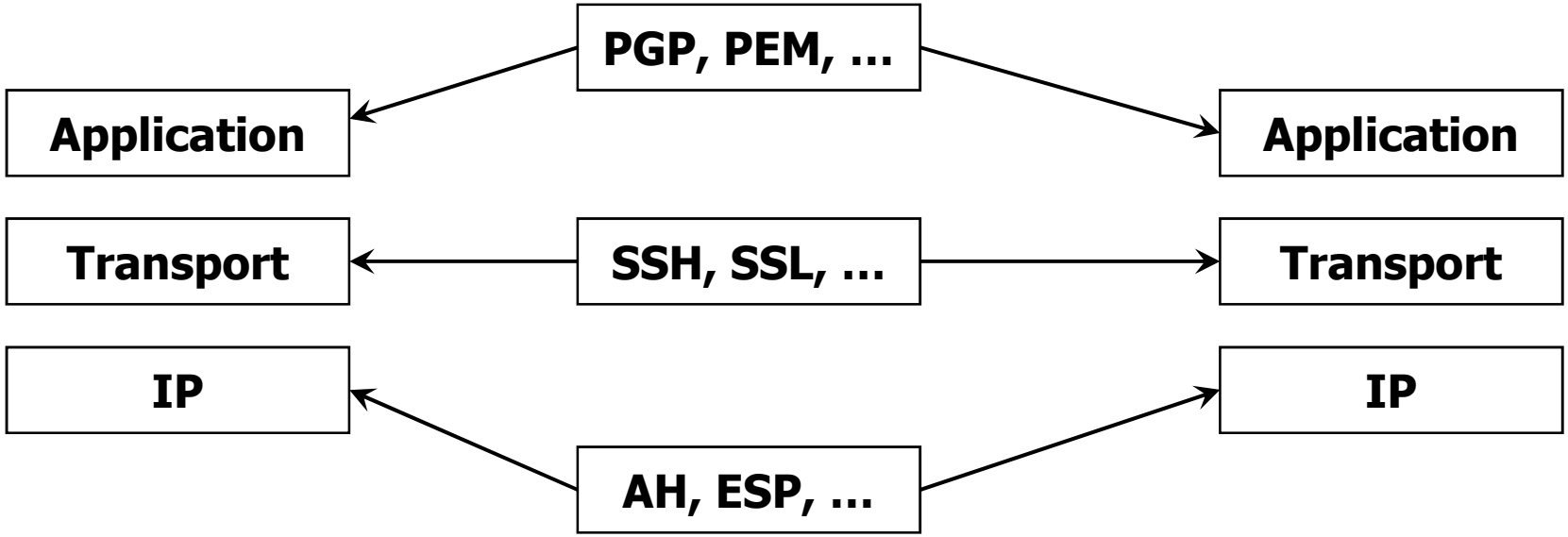
Communication entre domaines de confiance.



Sécurité dans les couches de protocoles

- Besoin de la sécurité dans plus d'une **couche** (routage, transport, application)
- Les couches supérieures sont plus **dépendantes** aux applications et **indépendantes** aux technologies.
- La fonction de sécurité ne doit pas **dupliquer** les fonctionnalités de communication.
- La sécurité **de bout en bout** est plus simple à fournir dans les couches supérieures, que la sécurité de **point à point** dans les couches inférieures.
- Les mécanismes de sécurité dans les **couches supérieures** sont généralement implémentés sur des **logiciels**. Les mécanismes de sécurité dans les **couches inférieures** sont généralement implémentés sur du **matériel**.

Sécurité dans les couches de protocoles



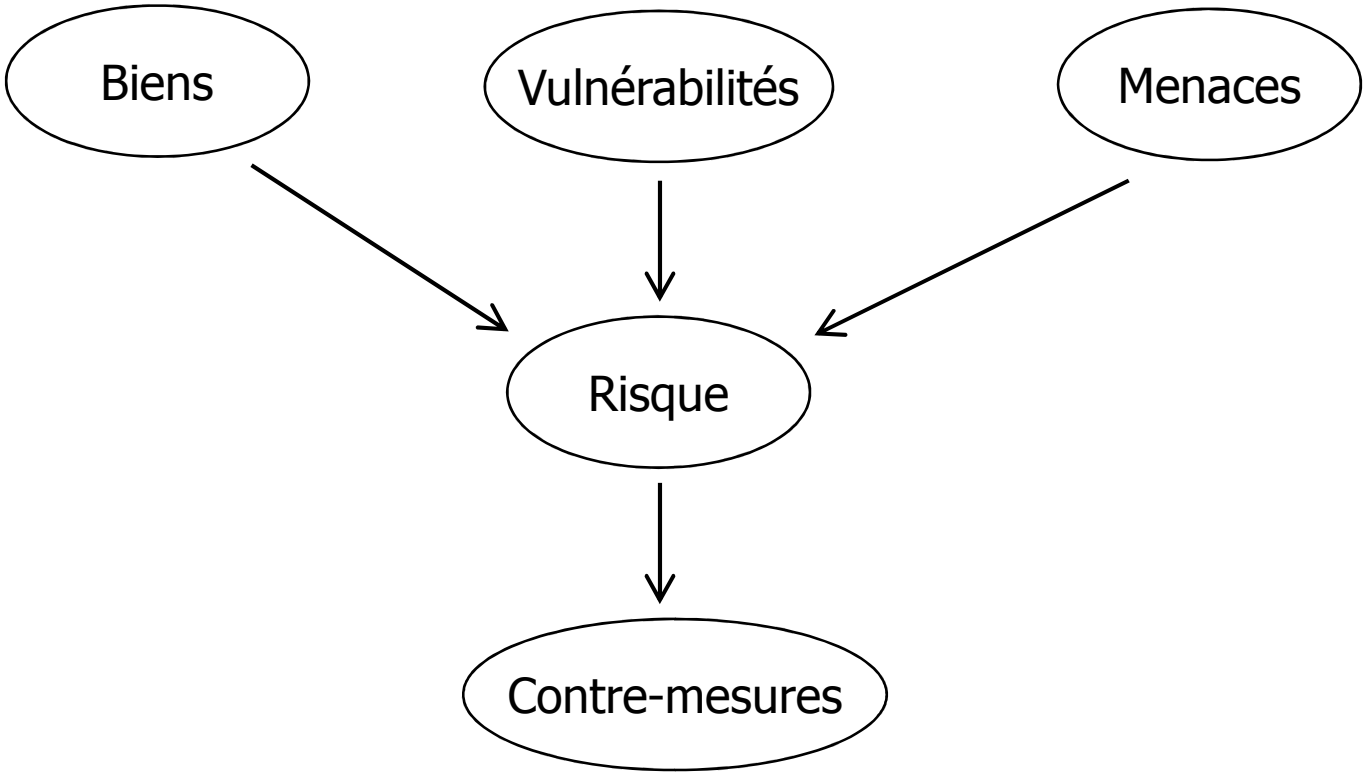
- PGP: Pretty Good Privacy, PEM: Privacy Enhanced Mail
- SSH: Secure Shell, SSL: Secure Socket Layer
- AH: Authentication Header, ESP: Encapsulating Security Payload.

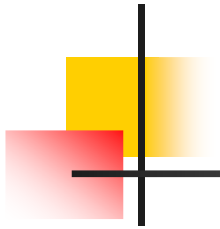
Modèle de sécurité réseau

- Nécessité de :
  - Sélectionner une **fonction de filtrage** appropriée afin d'identifier les utilisateurs et de s'assurer qu'uniquement les personnes autorisées accèdent aux ressources et informations du système.
    - Exemple: Mots de passe, certificats numériques, etc.
  - Implémenter des **contrôles internes** afin de **surveiller** l'activité des utilisateurs et **analyser** les informations pour **détecter** les actes malveillants.

Gestion de risque

Modèle:





Gestion de risque (2)

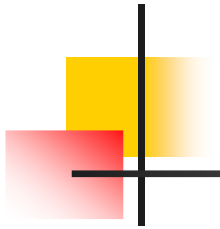
- Inventaire et estimation des biens
  - Types de Biens (Asset):
    - Matériel (CPU, disque, routeurs, …).
    - Logiciel (applications, bases de données, ...).
    - Données (configuration, archives, …).
    - Personnes (développeurs, administrateurs, …).
  - Quels sont les ressources vitales à l'entreprise ?
  - Difficulté d'évaluer proprement une ressource de type logiciel et donnée:
    - Un traitement erroné dans un logiciel de finance peut aller jusqu'à des poursuites légales.
    - Des données erronées dans un système embarqué peuvent causer l'endommagement de tout le système.

Gestion de risque (3)

- Evaluation des menaces
  - Exemple de menaces: Employé malhonnête, programme malveillant, intrus, …
  - Déterminer
    - Qui peut causer des endommagements ?
    - Quels sont les biens qui peuvent subir des attaques ?
    - Qu'est ce qui peut motiver les intrus à attaquer le système ?
    - Quels sont les formes de perte qui peuvent avoir lieu ?
    - Quels sont les formes de dégâts naturels qui peuvent avoir lieu ?

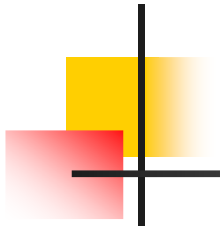
Gestion de risque (4)

- Evaluation des vulnérabilités
  - Quels sont les vulnérabilités du système ?
  - Quels sont les ressources les plus vulnérables ?
  - Un intrus tente toujours d'exploiter la vulnérabilité la moins contrôlée.



Gestion de risque (5)

- Analyse de risque
  - Déterminer les biens à protéger.
  - Définir de quelles menaces seront-t-ils protégés
  - Choisir comment les protéger.
- Contre-mesures
  - Implémentation de mécanismes et de politiques de sécurité en vues de:
    - Réduire les menaces.
    - Réduire les vulnérabilités.
    - Réduire l'impact.
    - Détecter les évènements malveillants.
    - Restaurer à partir d'un évènement malveillant.
  - La protection doit être proportionnelle à la valeur des biens à protéger.



Politique de sécurité

- Ensemble de règles spécifiant:
  - Comment les ressources sont gérées afin de satisfaire les exigences de sécurité.
  - les actions permises et les actions interdites.
- Objectif:
  - Empêcher les violations de sécurité telles que: accès non autorisé, perte de données, interruption de services, etc.
- Etendu:
  - Organisationnel, ou individuel
- Implémentation
  - Partiellement automatisée, mais toutes les personnes sont impliquées.

Politique de sécurité (2)