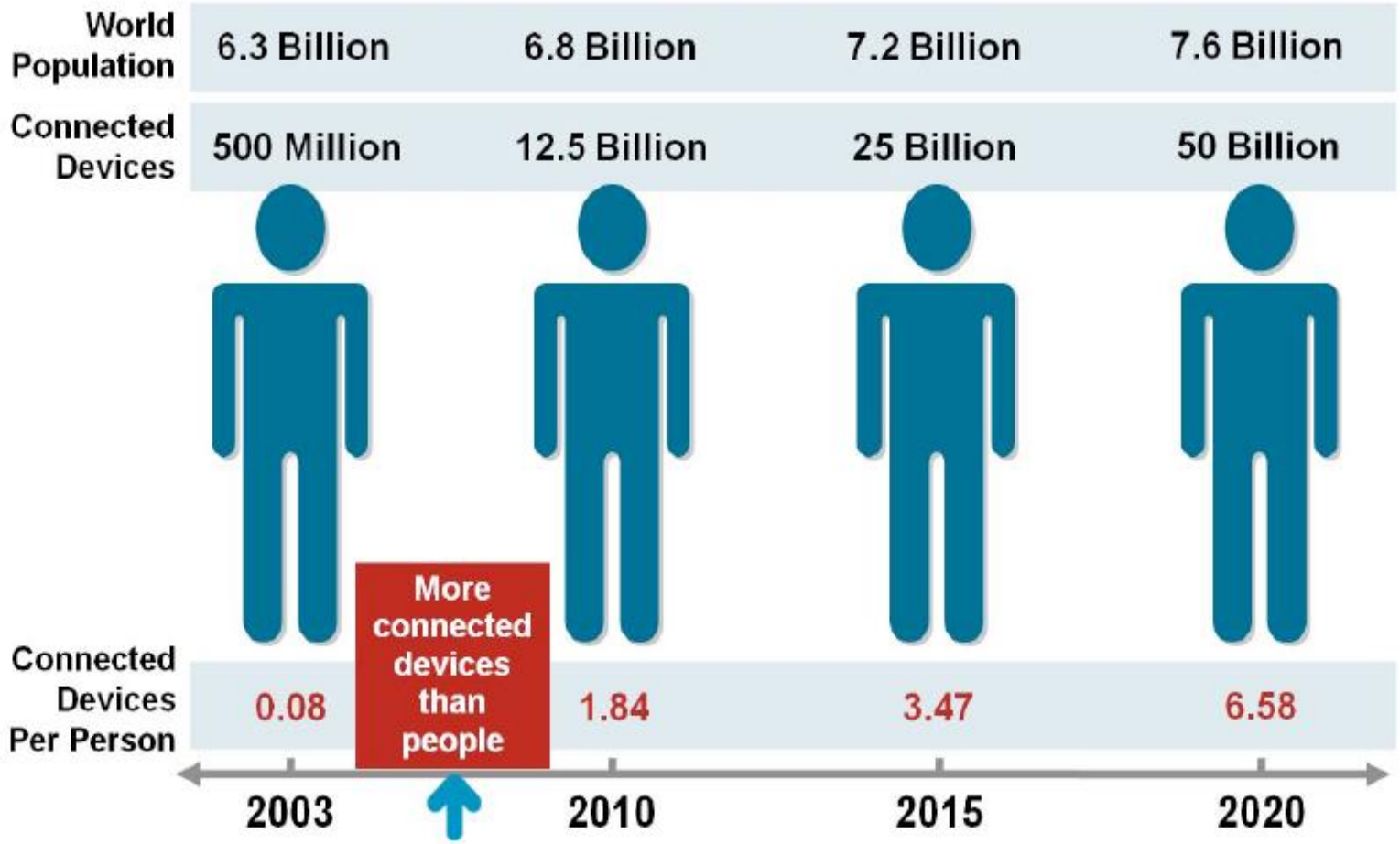
Premières notions de sécurité

Dr. Noureddine Chikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Plan du cours

- Principaux généraux
- Propriétés de sécurité
- Classification des attaques
- Aspects techniques de la sécurité

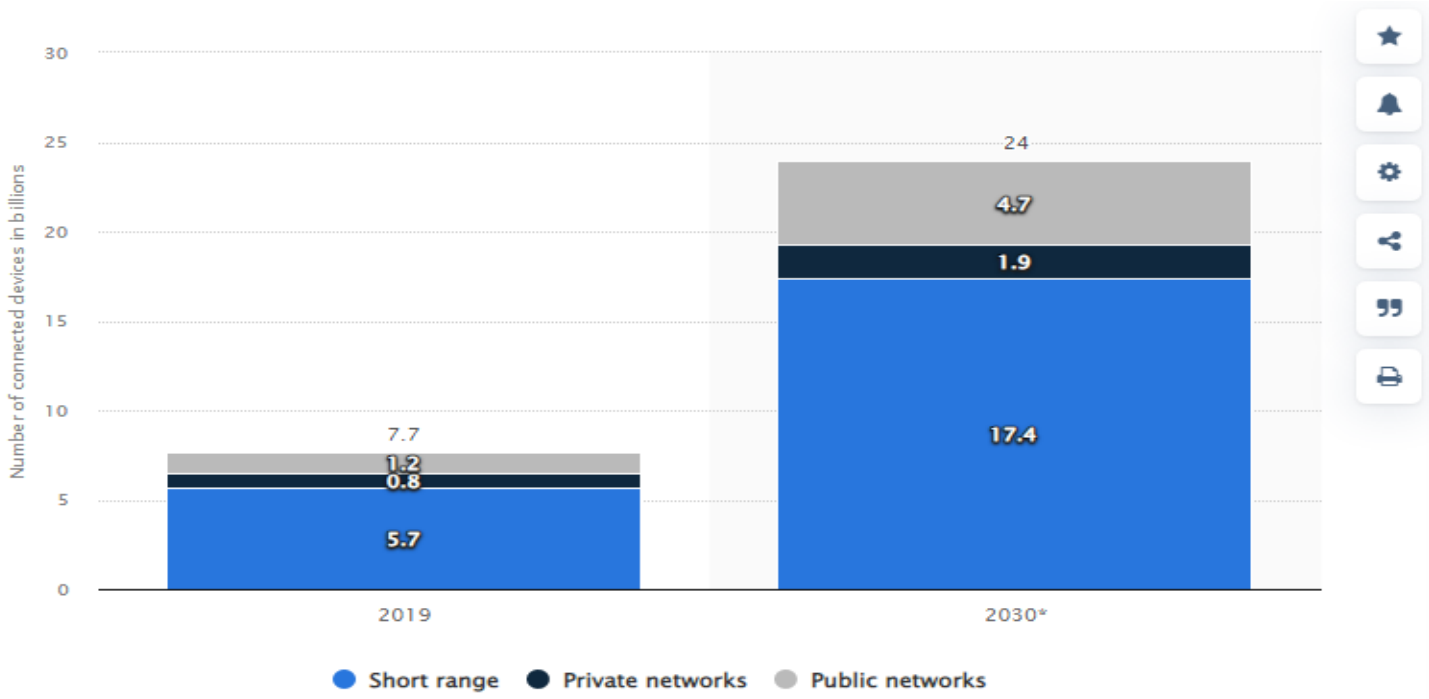
Principaux généraux



Source: Cisco IBSG, April 2011

Principaux généraux

- **Internet of Things (IoT) connected devices worldwide in 2019 and 2030, by technology***(in billions)*



Principaux généraux

CompTIA

Certifications

Connect Membership Resources Events & Education

Home / Blog

30 Internet of Things Stats & Facts for 2022

February 10, 2022 | By Ashley Watters

Security of IoT Devices Statistics

The connectivity of IoT means that our devices are constantly communicating on networks and with other technologies to help us be more efficient. However, much of that data flows continuously without being protected by necessary security protocols.

- The IoT security market is forecast to grow up to $18.6 billion in 2022. Kaspersky reported 1.5 billion IoT cyberattacks in the first six months of 2021, a number that was up from 639 million in all of 2020.
- More than 25% of all cyberattacks against businesses will involve IoT, reports Gartner.
- Endpoint security is expected to reach more than $19 billion in 2025, according to Statista.
- According to CompTIA, 63% of companies say IT security is a critical skill for IoT.

Principaux généraux

- Quelques biens à protéger
  - Matériel
  - Documentation
  - Réseaux,
  - Applications web
  - Logiciels
  - Données, …

Principaux généraux

- **Sécurité Informatique:**

  moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique.

- **Sécurité de l'information:**

  Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. En outre, d'autres propriétés, telles que l'authenticité, la non-répudiation et la fiabilité, peuvent également être concernées *(ISO/IEC 27000:2014)*

Principaux généraux

- **Sécurité des systèmes d'information (SSI):**

  L'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver rétablir et garantir la sécurité de l'information et du système d'information.

  (Wikipédia)

Principaux généraux

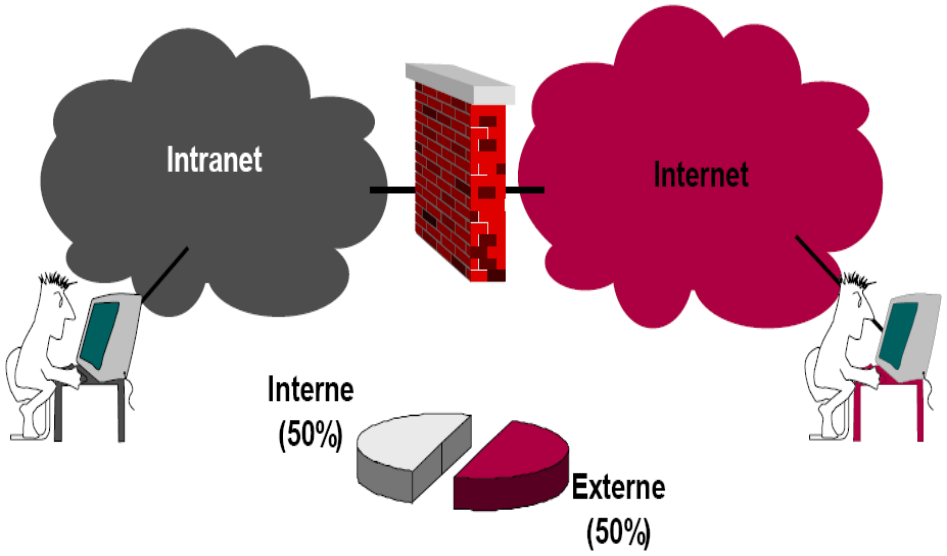
- **Vulnérabilité:**
  - Est une faiblesse (faille) dans la protection du système, sous la forme d'une menace qui peut être exploitée pour intervenir sur l'ensemble du système ou d'un intrus qui s'attaque aux actifs (matériels, logiciels, processus,…).
- **Menace:**
  - Est une personne ou entité (e.g. application web, logiciel, etc.) qui peut exploiter une vulnérabilité dans un système pour modifier, obtenir ou empêcher l'accès à un dispositif informatique ou plus encore le compromettre.

Principaux généraux

- **Attaque :**

  Une action malveillante qui compromet la sécurité des données ou systèmes d'informatique.

D'où viennent les attaques?



Principaux généraux

- **Contre- mesure**
  - C’est l'ensemble des actions réalisées en prévention de la menace.
- **Risque :**
  - Il signifie la probabilité qu'une menace exploitera une vulnérabilité du système.
  - Trois facteurs importante pour déterminer le risque: la nature de la menace, la vulnérabilité du système et l’importance de l’actif qui pourrait être endommagé ou rendu indisponible. On peut formaliser le risque comme suit:

Risque = Menace * Vulnérabilité * Actif

Principaux généraux

- **Risque (Cont.):**

Menace	Vulnérabilité	Actif et Impact	Risque	Recommandations de contrôle
Attaque DDoS par des humains malveillants (interférence) **Élevée**	Le pare-feu est correctement configuré et dispose d'une bonne atténuation des attaques DDoS **Faible**	Site Web. Les ressources du site Web seront indisponibles **Critique**	**Moyen** Perte potentielle de 8 900 € par heure d'indisponibilité	Surveiller le pare-feu

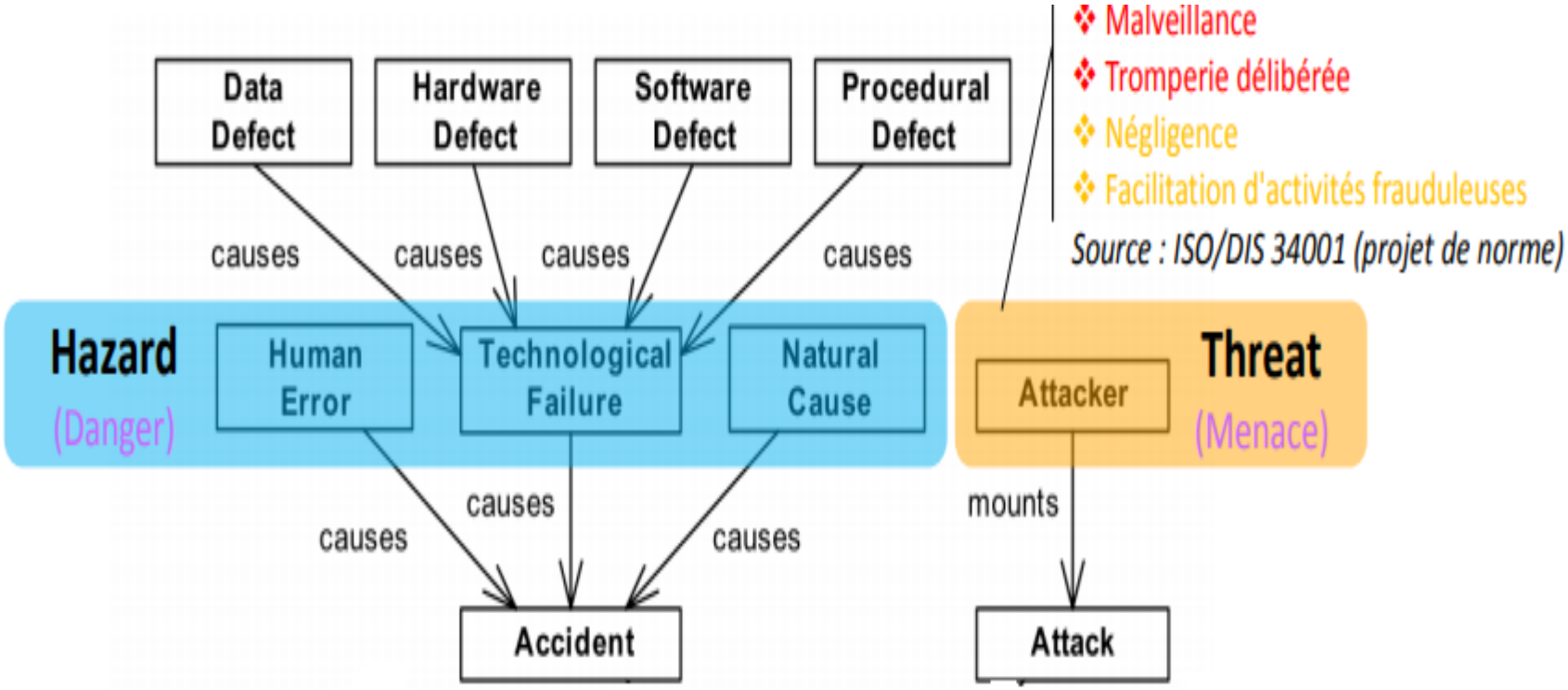
Source: https://www.netwrix.fr/information_security_risk_assessment_checklist.html

Système traditionnel

- **Vulnérabilité:**
  - Fenêtres ne sécurisée
  - Absence système d'alarme
  - Clés traditionnelles, ….
- **Menace:**
  - Voleur,
  - Assassin, …
- **Attaque :**
  - Vol argent,
  - Vol documents,
  - Tuer, …
- **Contre-mesure:**
  - Système alarme,
  - Caméra, …
- **Risque :**
  - Elevé
  - Moyen, …

- **Vulnérabilité:**
  - Mots de passe faible,
  - Absence de pare-feu
  - Absence de IDS,
- **Menace:**
  - Hacker,
  - Gouvernement
  - Société concurrent,
  - Zombie, …
- **Attaque :**
  - Vol d'information,
  - Déni de service,
- **Contre-mesure:**
  - Anti-virus,
  - Mot de passe fort, …
- **Risque :**
  - Faible,
  - Moyen, …

Accidents vs. Attaques



Source : Common Concepts Underlying Safety, Security, and Survivability Engineering - Donald G. Firesmith (Carnegie Mellon University)

Principaux généraux

Contrôle d'accès:

Associe des droits d'accès a une personne/application pour accéder a une ressource selon le principe du AAA.

- Authentification (Authentication):

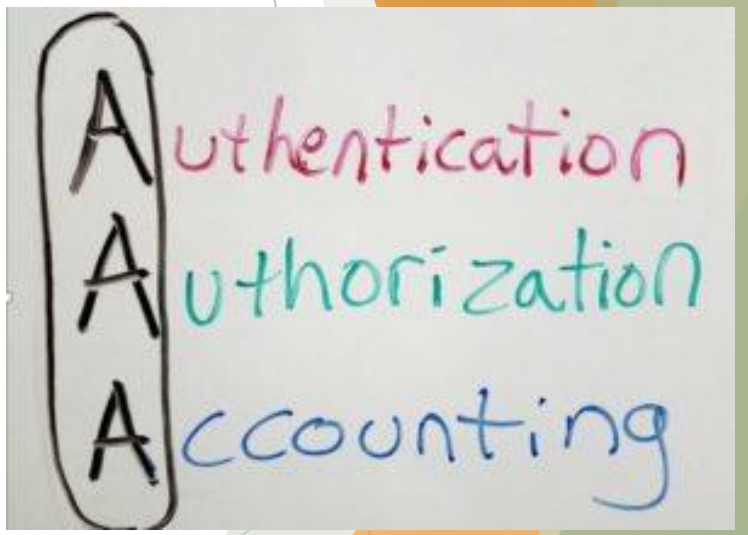
Vérification de l'identité de la personne

- Autorisation (Authorization):

Vérification des droits / privilèges de la personne authentifiée pour l'action envisagée.

- Traçabilité (Accounting):

Tracer les accès qui ont été contrôlés et effectues.



Plan du cours

- Principaux généraux
- Propriétés de sécurité
- Classification des attaques
- Aspects techniques de la sécurité

Les propriétés de sécurité

- propriétés de sécurité,
- exigences fondamentales,
- services de sécurité,, …

À quoi s'attendent les utilisateurs des systèmes informatiques ?

1- Confidentialité

- La confidentialité des données signifie que les informations secrètes ne peuvent être lues que par les entités autorisées.
- Pour réaliser cette propriété, il y a deux méthodes complémentaires :
  - contrôler et limiter l'accès
  - Algorithmes de chiffrement
- L'objectif principal de l'attaquant est d'obtenir le message en clair. Pour cela, il intercepte le message chiffré et utilise les techniques de cryptanalyse.
- **Exemples d'attaques**: Sniffing, intercepion de message.

2. Intégrité

- L'intégrité est un mécanisme qui a été mis pour s'assurer que les informations reçues n'ont pas été modifiées durant la transmission des données.
- Les méthodes de vérification de l'intégrité des données:
  - Somme de contrôle (C*hecksum*),
  - contrôle d'erreur (*Cyclic Redundancy Code*),
  - Fonction de hachage.
- **Exemples d'attaques:** modification du message, brouillage.

3. Authentification

- L'authentification est un mécanisme permettant de prouver des personnes ou des entités et de prouver leur identité.
- Les approches utilisées pour réaliser l'authentification d'une entité:
  - Signature numérique,
  - Protocole d'authentification
  - Login et mots de passe,
  - Certificat
- **Exemples d'attaques:** usurpation d'identité.

4. Disponibilité

- Une information ou une ressource est disponible aux entités autorisées (e.g. client, serveur, mobile, terminal, etc.).
- L'information ou service est toujours accessible et ne peut être bloquée/perdue.
- Le service peut être une application web, un logiciel, une application client-serveur, etc.
- **Exemples d'attaques:** Déni de service (DoS), bombardement et saturation du réseau.

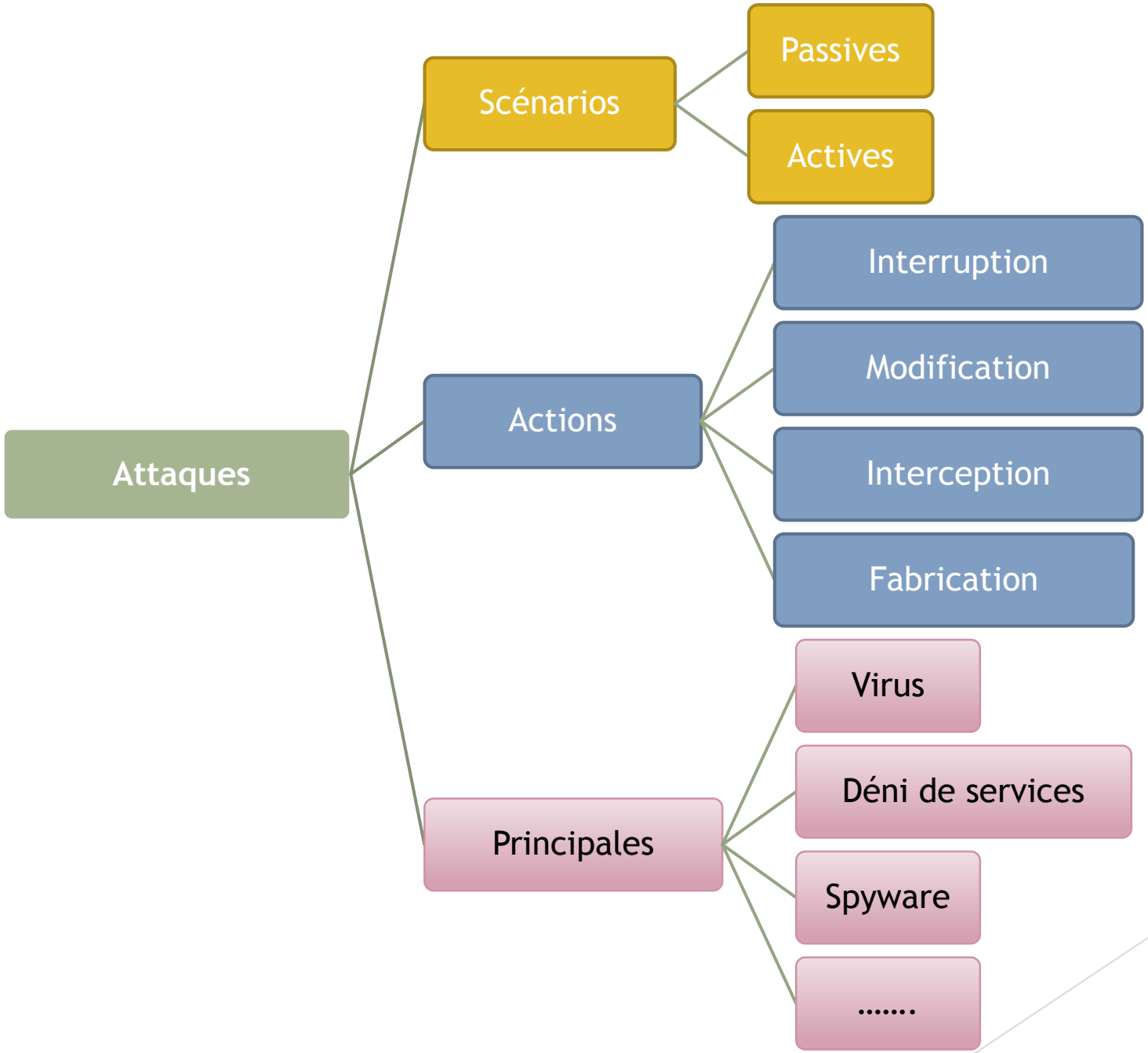
5. Non-répudiation

- La non-répudiation: garantir qu'une transaction ne peut être niée.
  - non-répudiation de l'origine prouve que les données ont été envoyées,
  - non-répudiation de l'arrivée prouve qu'elles ont été reçues.
- La signature numérique est utilisée pour réaliser non-répudiation.
- **Exemples d'attaques:** Modification du journal, répudiation.


Propriétés de sécurité
Confidentialité
Les informations secrètes ne peuvent être lues que par les entités autorisées
Intégrité
Assurer que les informations reçues n'ont pas été modifiées durant la transmission des données
Disponibilité
Une information ou une ressource est disponible aux entités autorisées
Non-répudiation
La possibilité de vérifier que les participants honnêtes sont bien les parties qui disent avoir respectivement envoyé ou reçu le message.
Authentification
Prouver des personnes ou des entités et de prouver leur identité.

Plan du cours

- Principaux généraux
- Propriétés de sécurité
- Classification des attaques
- Aspects techniques de la sécurité


Attaques
Scénarios
Passives
Actives
Actions
Interruption
Modification
Interception
Fabrication
Principales
Virus
Déni de services
Spyware
.....

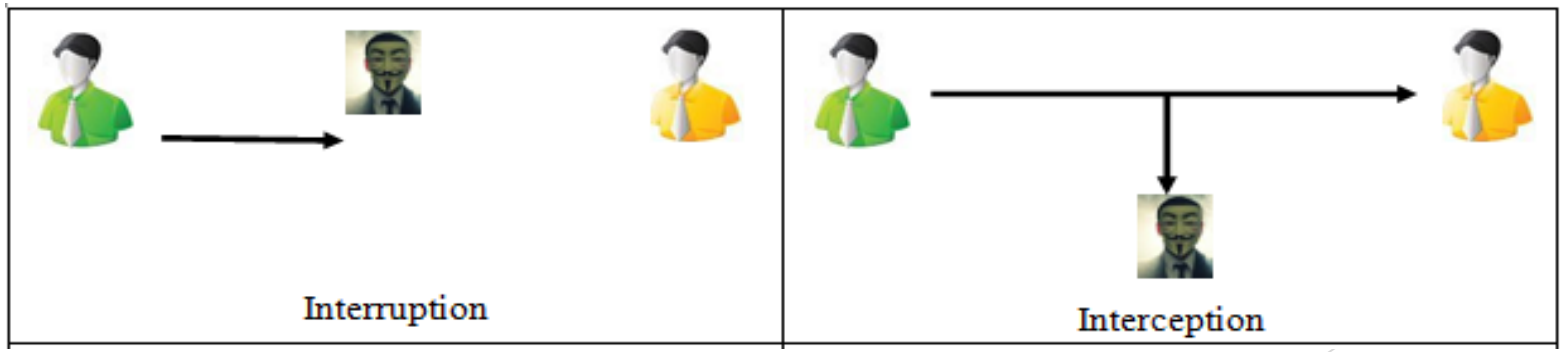
Actions des attaquants

Interruption:

- La menace bloque les messages transmis entre les communicants.
- Cette attaque vise la disponibilité des informations où les utilisateurs légitimes ne peuvent pas accéder aux informations demandées.

Interception:

- La menace intercepte seulement les messages échangés.
- Ce type d'attaque vise la confidentialité des informations, la menace obtient le message et utilise les techniques de cryptanalyse pour trouver le texte en clair.



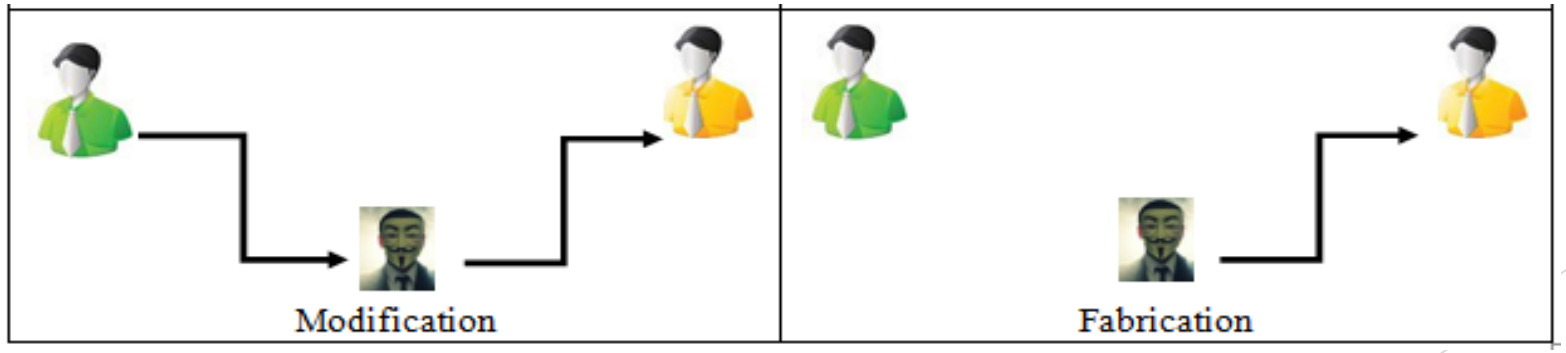
Actions des attaquants

Modification:

- La menace prend le message envoyé et fait des modifications sur celui-ci, puis envoie ce dernier au destinataire.
- Cette attaque vise l'intégrité des données.

Fabrication:

- La menace crée de nouveaux messages afin de réaliser son objectif.
- Cette attaque vise l'authenticité des entités et des informations.



Scénarios d’attaques:

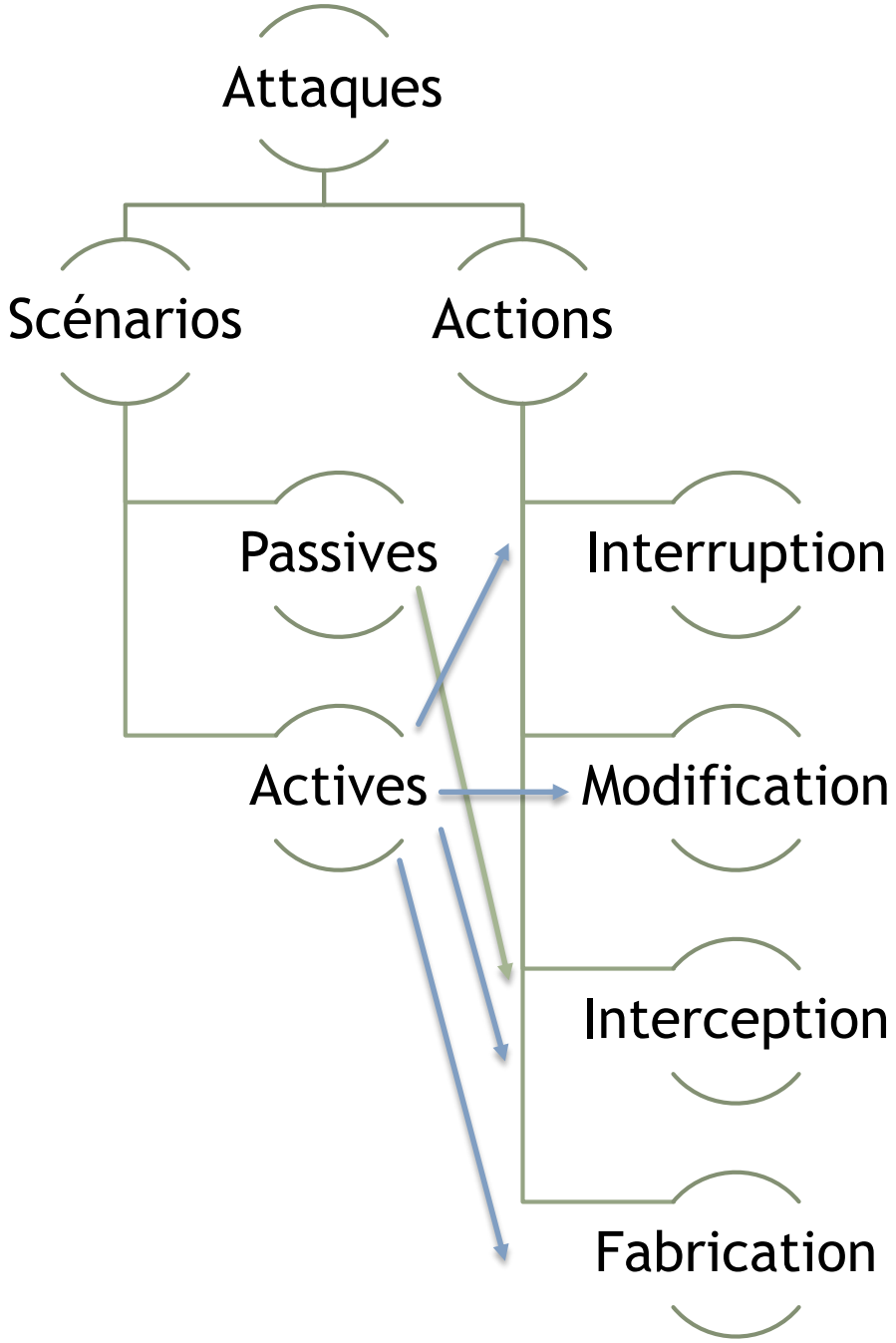
Attaques passives:

- L’intrus intercepte les messages transmit mais sans aucune action.
- L’objectif de cette menace est de briser la *confidentialité* des messages, ainsi une information sensible parvient à une personne autre que son destinataire légitime.

Scénarios d’attaques

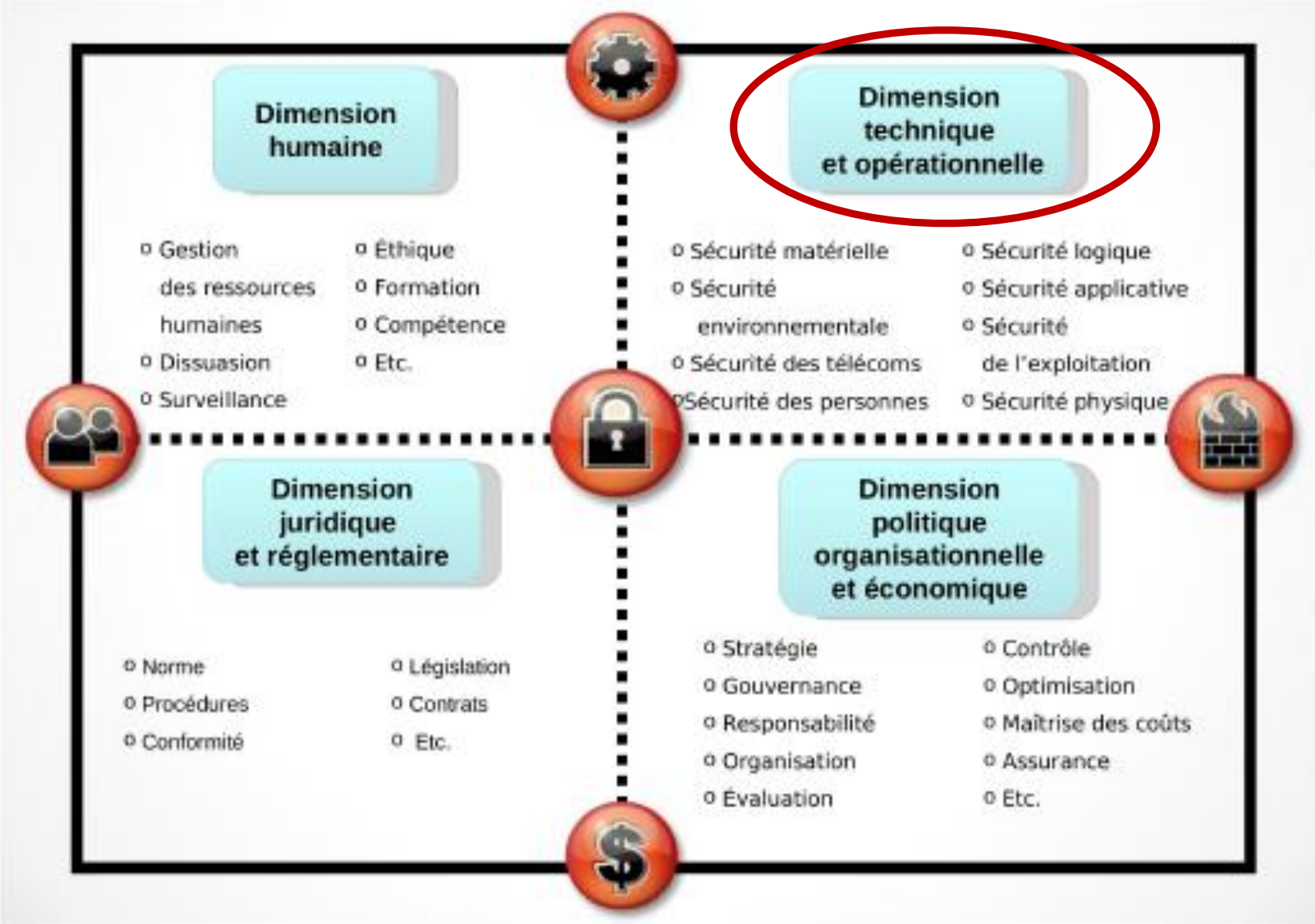
Attaques actives :

- la menace se fait par une intervention dans un canal de communication entre les entités communicantes.
- L’objectif de cette menace est de briser *l’intégrité*, *la disponibilité*, *et l’authenticité*.


Attaques
Scénarios
Actions
Passives
Actives
Interruption
Modification
Interception
Fabrication

Plan du cours

- Principaux généraux
- Les propriétés de sécurité
- Classification des attaques
- Aspects techniques de la sécurité


Dimension humaine
Gestion des ressources humaines
Dissuasion
Surveillance
Éthique
Formation
Compétence
Etc.
Dimension technique et opérationnelle
Sécurité matérielle
Sécurité environnementale
Sécurité des télécoms
Sécurité des personnes
Sécurité logique
Sécurité applicative
Sécurité de l'exploitation
Sécurité physique
Dimension juridique et réglementaire
Norme
Procédures
Conformité
Législation
Contrats
Etc.
Dimension politique organisationnelle et économique
Stratégie
Gouvernance
Responsabilité
Organisation
Evaluation
Contrôle
Optimisation
Maîtrise des coûts
Assurance
Etc.

Aspects techniques de la sécurité

- Sécurité physique
- Sécurité logique
- Sécurité applicative
- Sécurité de l'exploitation
- Sécurité de l'information
- Sécurité du réseau

Aspects techniques de la sécurité

- **Sécurité physique:**
- Il faut donner de l'importance à la sécurisation du matériel informatique et l'environnement où il opère pour éviter les risques.
- Les principaux risques sont:
  - l'incendie, la poussière, la surtension, eau, le vol, l'intrusion locale, etc.

Aspects techniques de la sécurité

- **Sécurité logique:**

La Sécurité logique est fournit par les logiciels de base, le système d'exploitation, et les administrateurs du système.

- Elle vise à:
  - Assurer les services de sécurité et particulièrement, la confidentialité, l'intégrité et l'authentification en utilisant les mécanismes de la cryptographie.
  - Utiliser la science de génie logiciel à fin de tester la sécurité et évaluer la qualité des développements logiciel,
  - Réaliser des différentes procédures: détection d'intrusions et applications malveillants et contrôle d'accès logique.

Aspects techniques de la sécurité

- **Sécurité applicative:**
- On trouve plusieurs types d'applications tels que: application Web, application mobile, logiciel de gestion, etc.
- l'utilisation de ces applications dans différentes infrastructures nécessite une bonne conception du code source de l'application, qui est la sécurité applicative.

Aspects techniques de la sécurité

- **Sécurité applicative:**

Exemple: Le guide de sécurisation des applications web OWASP

- Il offre des articles, des méthodologies, documentation, des outils, codes source, et des technologies dans le domaine de la sécurité des applications Web.
- Il fournit une formation pour les développeurs, les concepteurs, les architectes et les propriétaires d'entreprises sur les risques associés aux vulnérabilités de sécurité des applications Web les plus courantes

OWASP
The Open Web Application Security Project

Aspects techniques de la sécurité

- **Sécurité de l'exploitation:** elle traite les points suivants:
  - gestion du parc informatique ;
  - gestion des configurations et des mises à jour ;
  - gestion des incidents et leur résolution ;
  - plan de sauvegarde ;
  - plan de secours ;
  - plan de tests ;
  - inventaires réguliers et, si possible, dynamiques ;
  - analyse des fichiers de journalisation et de comptabilité ;
  - gestion des contrats de maintenance ;

Aspects techniques de la sécurité

- **Sécurité de l'information:**
- La sécurité de l'information est une science qui s'intéresse à étudier les mécanismes de protection des informations transmises via un media de communication entre les différents participants a fin de protéger l'information contres les risques de menaces.
- Cette discipline fournit les outils et les moyens nécessaires pour réaliser les critères de sensibilité de l'information, qui sont des objectifs de sécurité.

Aspects techniques de la sécurité

- **Sécurité du réseau:**
- La plupart des dispositifs informatiques (PCs, mobile, etc.) sont interconnectés par un ou plusieurs réseaux (réseau local filaire, Internet, Wi-Fi, etc.)
- La raison majeure de la plupart des attaques dans le monde numérique est la faiblesse de la sécurisation du réseau.
- Pour sécuriser le réseau il faut prendre en considération les couches de l'architecture OSI.

Quiz

- Lesquelles des notions suivantes ne sont pas des propriétés de sécurité:
  - Authentification
  - Confidentialité
  - Anonymat
  - Intégrité
  - Traçabilité
- Dans une attaque passive, l'intrus peut faire :
  - Interruption
  - Modification
  - Interception
  - Fabrication