مدرسة علوم المعلومات
ⵜⵉⵎⵔⵉⵜ ⵏ ⵜⵓⵙⵙⵓⵔⵉ ⵏ ⵜⵣⵔⴼⵜ
ECOLE DES SCIENCES DE L'INFORMATION
www.esi.ac.ma

INITIATION AUX RÉSEAUX INFORMATIQUES

PARTIE 6 : INTRODUCTION À LA SÉCURITÉ

Module M1.5.1 **Année universitaire 2021-2022**

INTRODUCTION À LA SÉCURITÉ

I. Introduction

II. Paradigmes de la sécurité des réseaux informatiques

III. Exemples de menaces

IV. Exemples de moyens pour garantir la sécurité

Introduction

Problématique

- Les réseaux informatiques font partie intégrante de notre quotidien
  - Des milliards d'utilisateurs
  - Des milliards d'objets connectés
  - Un trafic en Téraoctets !
- Une des problématiques majeures dans les réseaux informatiques est la **sécurité**

Problématique

- Les systèmes d'information connectés en réseau sont confrontés à des menaces qui évoluent de jour en jour

➔ Il est nécessaire de mettre des formes de protection contre ces menaces

➔ **Sécurité des réseaux informatiques**

Sécurité des réseaux informatiques

- La sécurité des réseaux informatiques définit l'ensemble des moyens mis en œuvre pour garantir un minimum de protection des échanges et des intervenants dans un réseau informatiques
- Elle concerne l'ensemble des paradigmes du réseau informatique

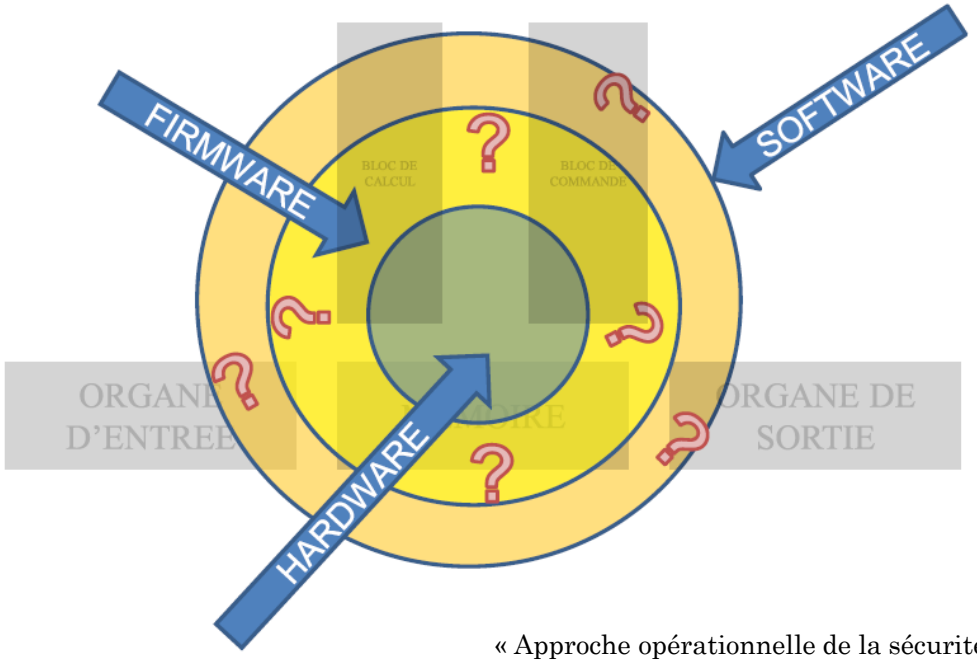
Paradigmes de la Sécurité des réseaux informatiques

Paradigmes du réseaux informatique

- Quatre paradigmes
  - Électricité et l'électromagnétisme
  - Stations (machines)
  - Communication
  - Données

Paradigmes de la sécurité informatique

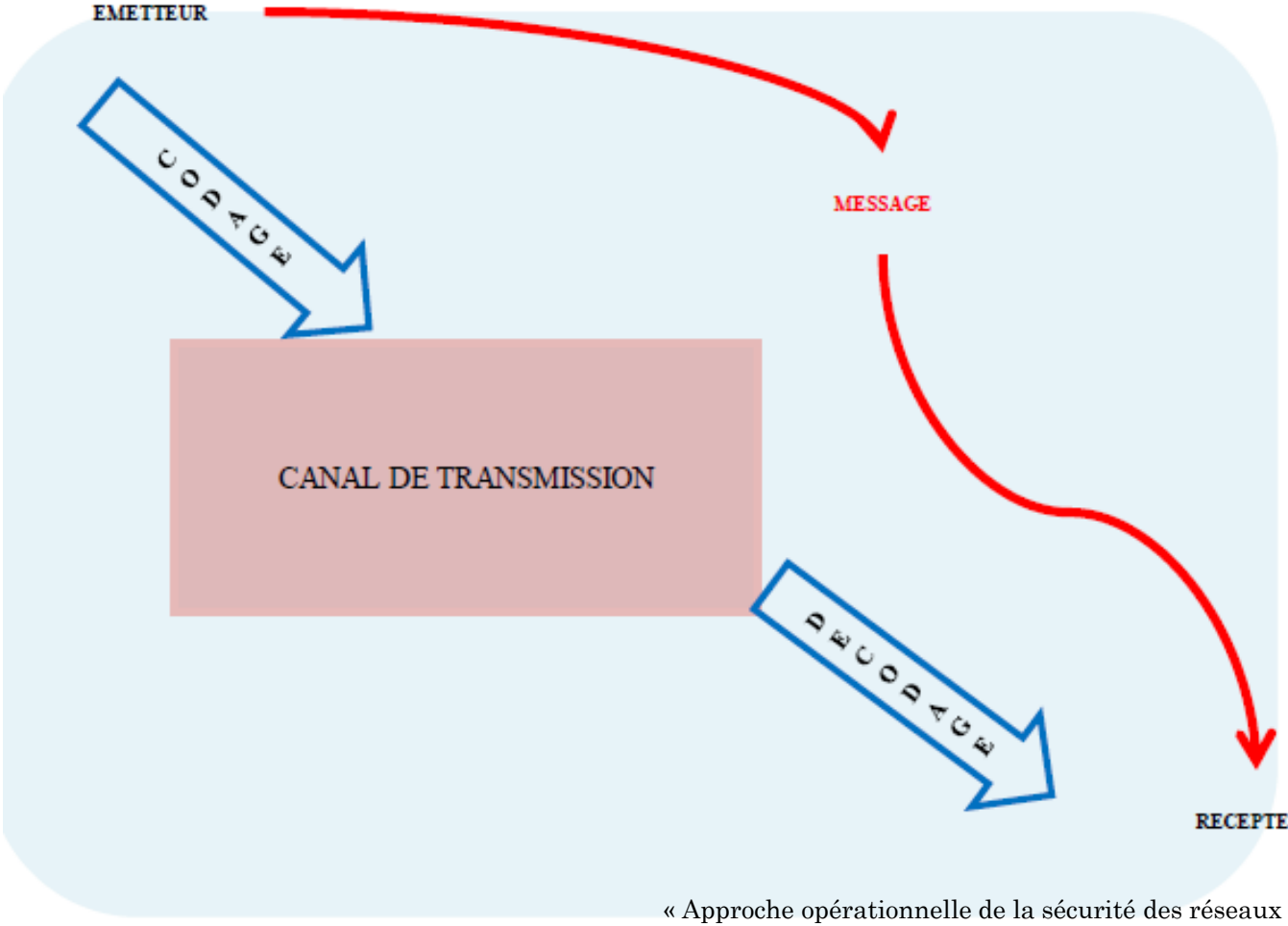
- Électricité et électromagnétisme
  - Sensibilité aux variations, instabilité magnétique, interférences, sensibilité aux rayonnements…
- Stations



« Approche opérationnelle de la sécurité des réseaux », Didier SPELLA

Paradigmes de la sécurité informatique

- Communication



« Approche opérationnelle de la sécurité des réseaux », Didier SPELLA

Paradigmes de la sécurité informatique

- Communication: chaîne constituée de
  - L'émetteur
  - Le récepteur
  - Le message transmis
  - Le code qui sert à transmettre le message
  - Le canal de transmission
  - Le contexte

Paradigmes de la sécurité informatique

- Données
  - La **disponibilité** : les données doivent être accessibles et utilisables à la demande par les utilisateurs qui en auront besoin
  - La **confidentialité** : la transmission des données échangées sur un réseau doit être privée ➔ elles ne peuvent être accessibles que par les personnes autorisées

Paradigmes de la sécurité informatique

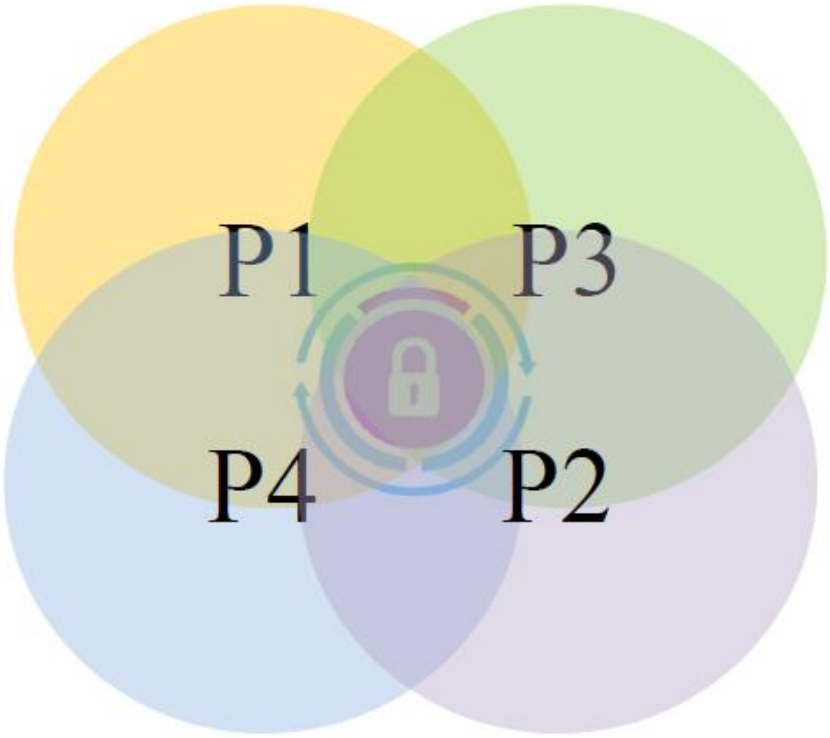
- Données
  - L'**intégrité** : les données ne peuvent être modifiées que par les personnes autorisées et seulement par les moyens autorisés
  - L'**authentification** : permet d'éviter la fraude et la substitution de personnes ➔ chacun doit connaître l'identité de son interlocuteur
    - Le service d'authentification assure que le message provient de l'endroit d'où il prétend venir

Paradigmes de la sécurité informatique

- Données
  - La **non-répudiation** : permet au récepteur / émetteur de ne pas nier la réception / émission d'un message.
    - Le récepteur peut prouver que le message a bien été envoyé par l'émetteur
    - L'émetteur peut démontrer que le message a bien été reçu par le bon récepteur

Paradigmes de la sécurité informatique

- Le niveau de sécurité d'un réseau informatique est celui du paradigme qui a le niveau de sécurité le plus faible



« Approche opérationnelle de la sécurité des réseaux », Didier SPELLA

Notion de risque

- Le risque zéro n'existe pas
- L'objectif n'est pas d'empêcher les attaques mais de réduire leurs effets

➔ Avoir une protection acceptable avec un risque acceptable et un coût acceptable

Exemples de menaces

Sources d'attaques

- Externes
  - Pirates
  - Saboteurs
  - Concurrents
  - Anciens employés
  - Organisations criminelles
  - …

Sources d'attaques

- Externes
- Internes
  - Employés mécontents
  - Fraudeurs
  - Espions
  - …

Types d'attaques

- Spoofing
  - Usurpation d'adresses IP
- Sniffing
  - Écoute d'une ligne à travers laquelle des données importantes peuvent être transmises telles que les mots de passe

Types d'attaques

- Malware (logiciel malveillant)
  - Virus ; Vers ; Chevaux de troie ; quelques logiciels P2P
- Déni de service
- Exploits
- Ransomware
- …

Exemples de moyens pour garantir la sécurité

Contrôle d'accès

- Besoin de limiter et de contrôler les accès réseau aux systèmes et applications
  - Ne pas donner les mêmes droits à toutes les personnes connectées ➔ plusieurs profils
  - Chaque entité qui demande un accès doit s'identifier afin d'accéder **uniquement** aux ressources qui lui sont autorisées
- Outils : mots de passe, pare-feux, logiciels antivirus, VPN, certificats numériques…

Mot de passe

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

https://www.komando.com/security-privacy/check-your-password-strength/783192/

Mot de passe

- Exemple de générateur de mots de passe

https://www.motdepasse.xyz/

- Vérifier la force du mot de passe sur

https://www.security.org/how-secure-is-my-password/

Pare-feu

- Un composant matériel et/ou logiciel qui restreint l'accès entre un réseau protégé et d'autres réseaux, y compris Internet
  - Programmé de façon à intercepter chaque paquet de messages qui passe entre les deux réseaux
  - Analyse les caractéristiques et rejette les messages ou les tentatives d'accès non autorisés

Pare-feu

- Limitation
  - Ne peut protéger contre les connexions qui ne passent pas par lui
  - Ne peut pas protéger le réseau contre des menaces nouvelles (non paramétrée)
  - Ne peut le protéger contre les virus

➔ Les 2 derniers points sont pris en charge par certains pare-feux de nouvelle génération ainsi que les UTM

VPN

- Connexion **distante sécurisée** entre deux sites d'une organisation qui permet de transmettre des données cryptées à travers un réseau non sécurisé, notamment Internet

VPN

- Composantes
  - Serveur VPN : serveur d'accès distant servant à chiffrer et déchiffrer les données du côté de l'organisation
  - Client VPN: entité distante ayant la possibilité de chiffrer et de déchiffrer les données du côté utilisateur
  - Protocoles de tunneling : utilisés par les clients VPN pour créer des connexions sécurisées sur un serveur VPN (IPSec, MPLS…)

Cryptage

- Moyen de chiffrement des données permettant de protéger les informations en les rendant illisibles ou incompréhensibles sauf pour le bon destinataire
- Basé sur deux éléments fondamentaux
  - Chaîne de nombres binaires appelée **clé**
  - Algorithme sous forme d'une fonction mathématique qui va combiner la clé et le texte à crypter pour chiffrer le texte

Cryptage

- On distingue deux types
  - Symétrique
  - Asymétrique

Cryptage

- Symétrique
  - Une seule clé secrète partagée entre les deux entités échangeant les informations
  - Cette clé va servir en même temps au chiffrement et au déchiffrement du message
  - Plusieurs algorithmes se basent sur ce principe, notamment DES, IDEA, RC2, RC4…

Cryptage

- Symétrique
  - Avantage : cryptage rapide
  - Limite : la non-répudiation n'est pas assurée puisqu'un utilisateur, possédant la même clé que son correspondant, peut fabriquer un message en usurpant l'identité de celui-ci

Cryptage

- Asymétrique
  - Appelé aussi **cryptage à clé publique**
  - Basé sur l'utilisation d'une paire de clés appelée **bi-clés**
    - Une clé publique qui sert à chiffrer le message
    - Une clé privée qui sert à déchiffrer le message
  - Les deux clés sont générées simultanément et sont liées par des algorithmes

Cryptage

- Asymétrique
  - Avantage : assure un grand niveau de sécurité car même si la clé publique est connue il est impossible de détecter la clé secrète
  - Limite : lenteur en comparaison avec le cryptage symétrique

Certificat numérique

- Association d'une clé publique et des informations concernant l'identité du propriétaire
  - Propriétaire : une personne, un ordinateur, un organisme…

➔ Il est issu de la relation entre une clé publique, son propriétaire et l'application pour laquelle il est émis

- Le certificat assure que la connexion est bien réalisée au site auquel on veut accéder

Pour aller plus loin

- MOOC **Sécurité des Réseaux Informatiques** sur https://www.fun-mooc.fr/fr/

مدرسة علوم المعلومات
ⵜⵉⵎⵔⵉⵜ ⵏ ⵜⵓⵙⵙⵓⵔⵉ ⵏ ⵜⵣⵔⴼⵜ
ECOLE DES SCIENCES DE L'INFORMATION
www.esi.ac.ma

INITIATION AUX RÉSEAUX INFORMATIQUES

PARTIE 6 : INTRODUCTION À LA SÉCURITÉ

Module M1.5.1 **Année universitaire 2021-2022**