



République Algérienne Démocratique Et
Populaire

Ministère De L'enseignement Supérieur Et De
La Recherche Scientifique



Département Génie des systèmes Informatique
Filière IMSI , RT: 4^{ème} année ingénieur

Sécurité des systèmes d'information

DR F.KABLI

Fatima.kabli@en
p-oran.dz

Introdu ction

- ❑ Qu'est-ce que la sécurité du système d'information ?
- ❑ La sécurité globale et les domaines d'application.
- ❑ La sécurité physique et environnementale
- ❑ La sécurité logique

Introdu ction

Qu'est ce que la sécurité des systèmes informatiques ?

La sécurité des systèmes informatiques correspond à un ensemble de techniques mises en œuvre pour garantir la **sécurité** et l'**intégrité** d'un système informatique. Ces techniques peuvent être :

- *Fonctionnelles*
- *Organisationnelles*
- *Politiques*
- *Juridiques*
- *Humaines ...*

La sécurité des systèmes informatiques ?

- ❑ La mise en place de la sécurité informatique est généralement assurée par un administrateur réseau en interne à l'entreprise ou une société indépendante.
- ❑ Il existe de nombreux techniques permettant d'assurer la protection d'un système informatique : **la cryptographie, la restriction d'accès par mot de passe, les antivirus, le pare-feu, un système de détection d'intrusion.**

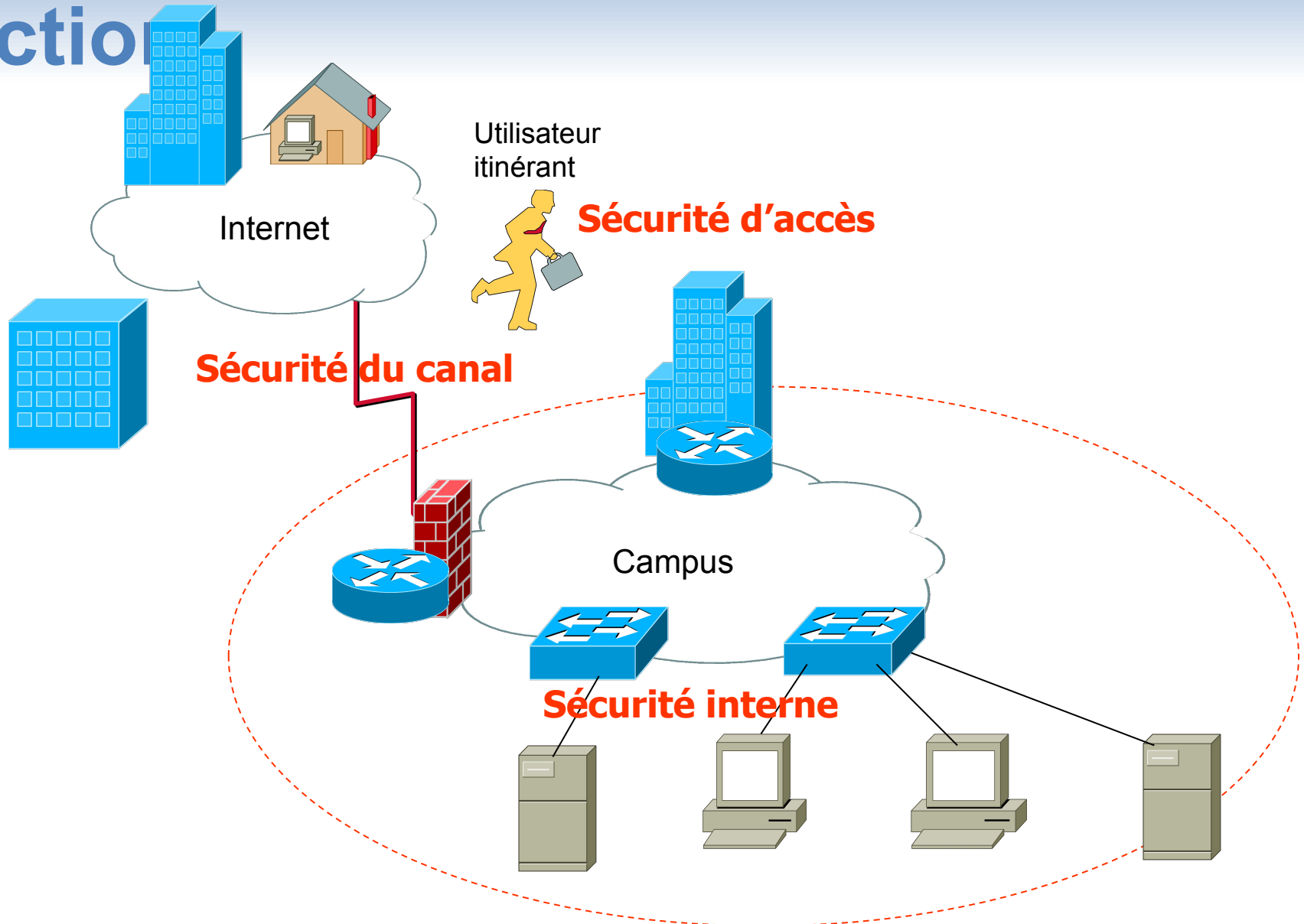
Approche globale de la sécurité

- ❑ Il faut traiter la sécurité d'un système informatique en sa totalité, car il est inutile d'avoir une porte blindée et en même temps avoir les fenêtres ouvertes sur le monde extérieur.
- ❑ Partant de cette idée, on doit donc aborder la sécurité dans son contexte global c'est-à-dire, on doit assurer les différents aspects de sécurité suivants :

Introdu ction

- ❑ La Sécurité Organisationnelle
- ❑ La sécurité physique et environnementale
- ❑ La sécurité des accès
- ❑ La sécurité des réseaux
- ❑ La sécurité des serveurs
- ❑ La sécurité des données
- ❑ La sécurité énergétique
- ❑ La sécurité antivirale (c'est la sécurité contre les virus informatiques)

Introdu ction



La Sécurité Organisationnelle

- ❑ Définir les rôles des différents acteurs : Qui fait quoi ?
- ❑ Sensibiliser les utilisateurs aux problèmes de la sécurité.
- ❑ Intégrer **le facteur sécurité** dans tout projet informatique dès sa conception jusqu'à sa réalisation.
- ❑ Mise en œuvre de la sécurité.

Introdu ction

La sécurité physique et environnementale

- ❑ Règles de sécurité des locaux qui abritent les serveurs sensibles et les équipements d'interconnexion : équiper ces locaux par des détecteurs d'incendie et par un système d'extinction automatique.
- ❑ Verrouillage des locaux contre le vol du matériel.
- ❑ Accès permis seulement aux personnes autorisées (utiliser des clés spéciales ou une carte à puce pour contrôler les accès à la salle informatique).

Introdu

ction

Enquête :

- ☐ 89% des sociétés ont déjà été confrontées à un vol d'ordinateur portable.
- ☐ 67% des vols d'ordinateurs portables ont lieu au bureau
- ☐ Seulement 3% des ordinateurs portables volés sont récupérés

ction La sécurité des accès

- ❑ Sécurité des accès aux postes de travail et aux serveurs pour les utilisateurs et les administrateurs. L'accès doit être assuré par :
 - ❑ Nom utilisateur et mot de passe
 - ❑ Carte à puce : l'authentification par carte à puce est destinée à garantir l'identité d'une personne à assurer son identification via un code PIN et à protéger l'accès aux postes de travail par le biais d'un mot de passe dynamique
- ❑ Gestion des droits d'accès aux données et aux fonctionnalités des logiciels en fonction des profils des utilisateurs

Introdu ction

La sécurité des accès

Exemple:

- ❑ Carte à puce par certificats PKI (Infrastructure à Clé Publique) à mini-lecteurs (IDPrimeMD)



La sécurité des réseaux

- ❑ Assurer la sécurité des topologies LAN et WAN pour garantir la continuité de transmission des données à l'intérieur et à l'extérieur de l'entreprise.
- ❑ Contrôler le flux des données entre le système d'information et le monde extérieur (c'est-à-dire l'Internet ou le WAN) pour éviter tout risque d'attaque (alors il faut installer un serveur proxy avec un firewall).
- ❑ Détecter les intrusions qui viennent de l'extérieur et les éviter au préalable.
- ❑ Assurer la sécurité de transmission de données sur l'Internet en implantant des protocoles sécurisés SSL et en faisant le cryptage des messages.

Introdu ction

La sécurité des serveurs

- ❑ Classification des serveurs de l'entreprise (le serveur proxy doit être assez performant pour bien protéger le serveur de base de données)
- ❑ Sécuriser les procédures d'exploitation et d'administration (avec des mots de passe)

Introdu ction

La sécurité des données

- ❑ Assurer une sauvegarde quotidienne et hebdomadaire des données
- ❑ Faire la sauvegarde sur des supports multiples.
- ❑ Protéger les supports de sauvegarde, contre les incendies, dans une armoire inflammable.

Introdu ction

La sécurité énergétique

La sécurité énergétique est très importante quant au fonctionnement des équipements formant la plateforme technique. Il est

recommandé d'équiper les armoires abritant les différents éléments par des onduleurs performants pour remédier aux petites coupures du courant ou aux chutes de la tension électrique.

En revanche, pour les coupures de longue durée, il faut prévoir l'installation d'un groupe électrogène qui va assurer la continuité du courant nécessaire pour le bon fonctionnement.

ction La sécurité antivirale (c'est la sécurité contre les virus informatiques)

- ❑ Un virus est un programme informatique qui peut infecter d'autres programmes dans le but de **les modifier** pour y ajouter une copie de lui-même, de **gêner leur fonctionnement** et **voire même les supprimer** ou nuire à **certaines composantes** de l'ordinateur.
- ❑ Les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection.

La sécurité antivirale (c'est la sécurité contre les virus informatiques)

On distingue principalement quatre types de virus :

- ❑ *Vers*

- ❑ *Chevaux de Troie*

- ❑ *bombes logiques*

- ❑ *Canulars*