# Chapitre 3: Problématique de la sécurité des communications

**laurent.vigneron@univ-lorraine.fr**

**Polytech Nancy**

Année 2021/2022

# Sécurité des communications

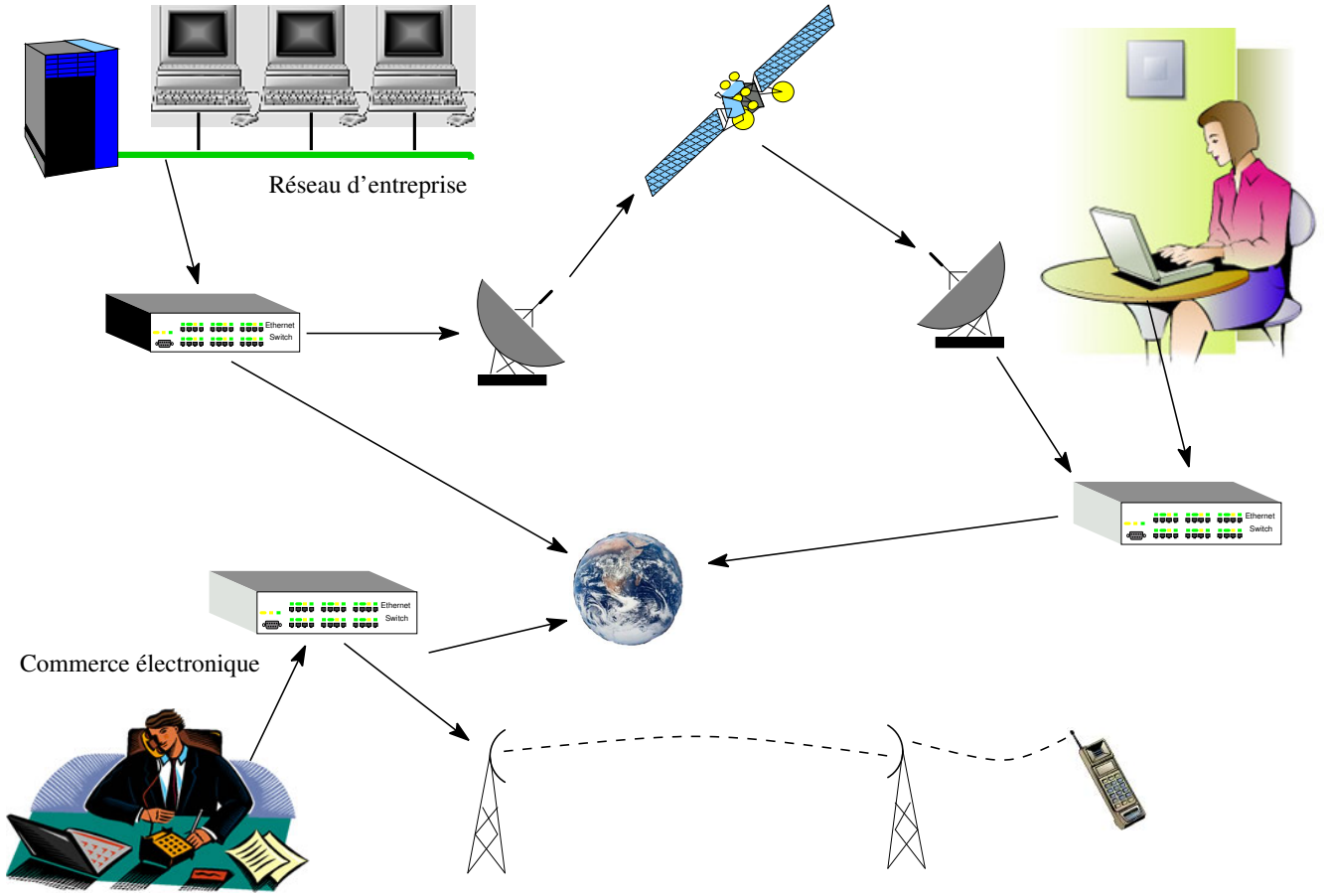
## Introduction

1 Problématique

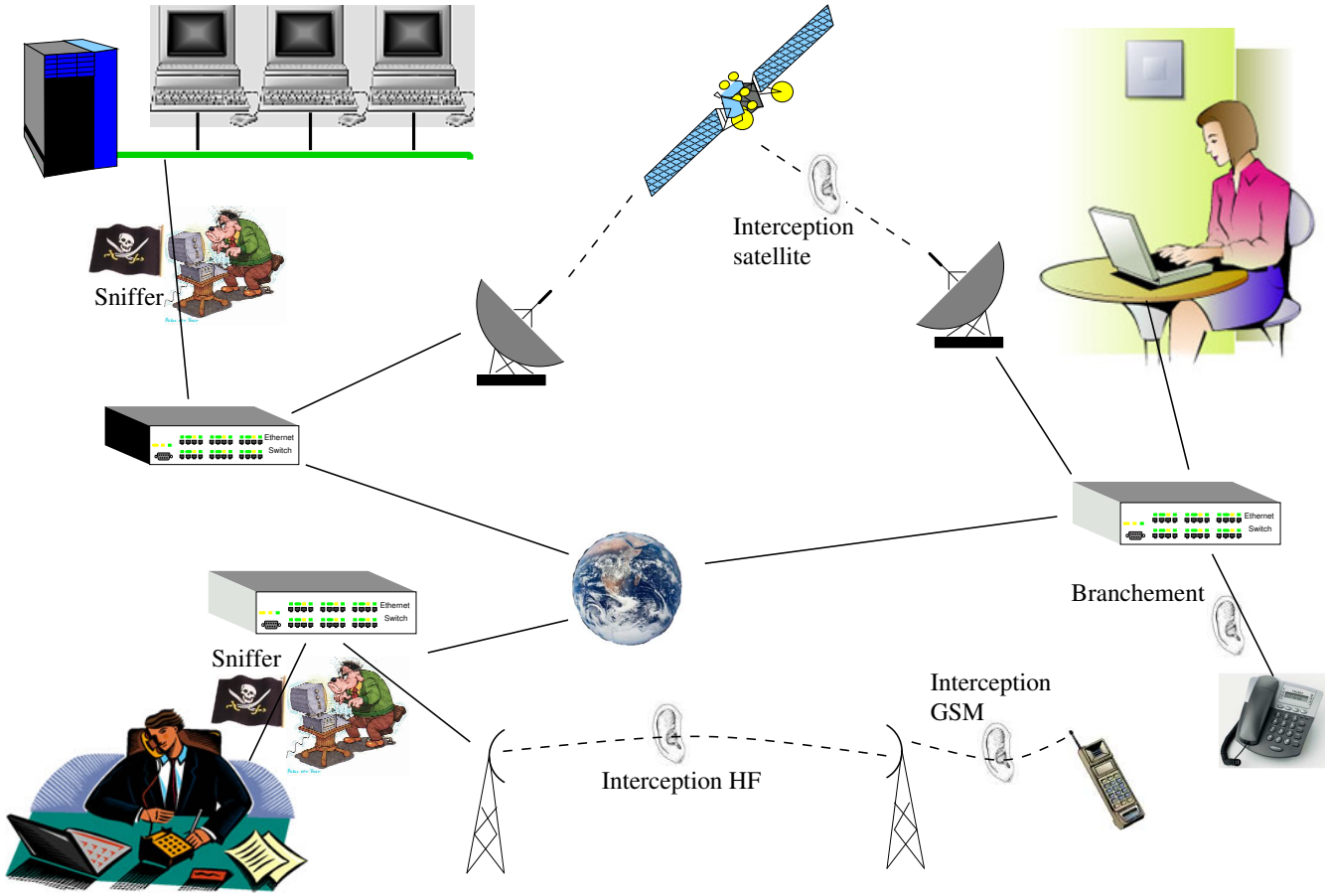
2 Définitions

3 Motivation

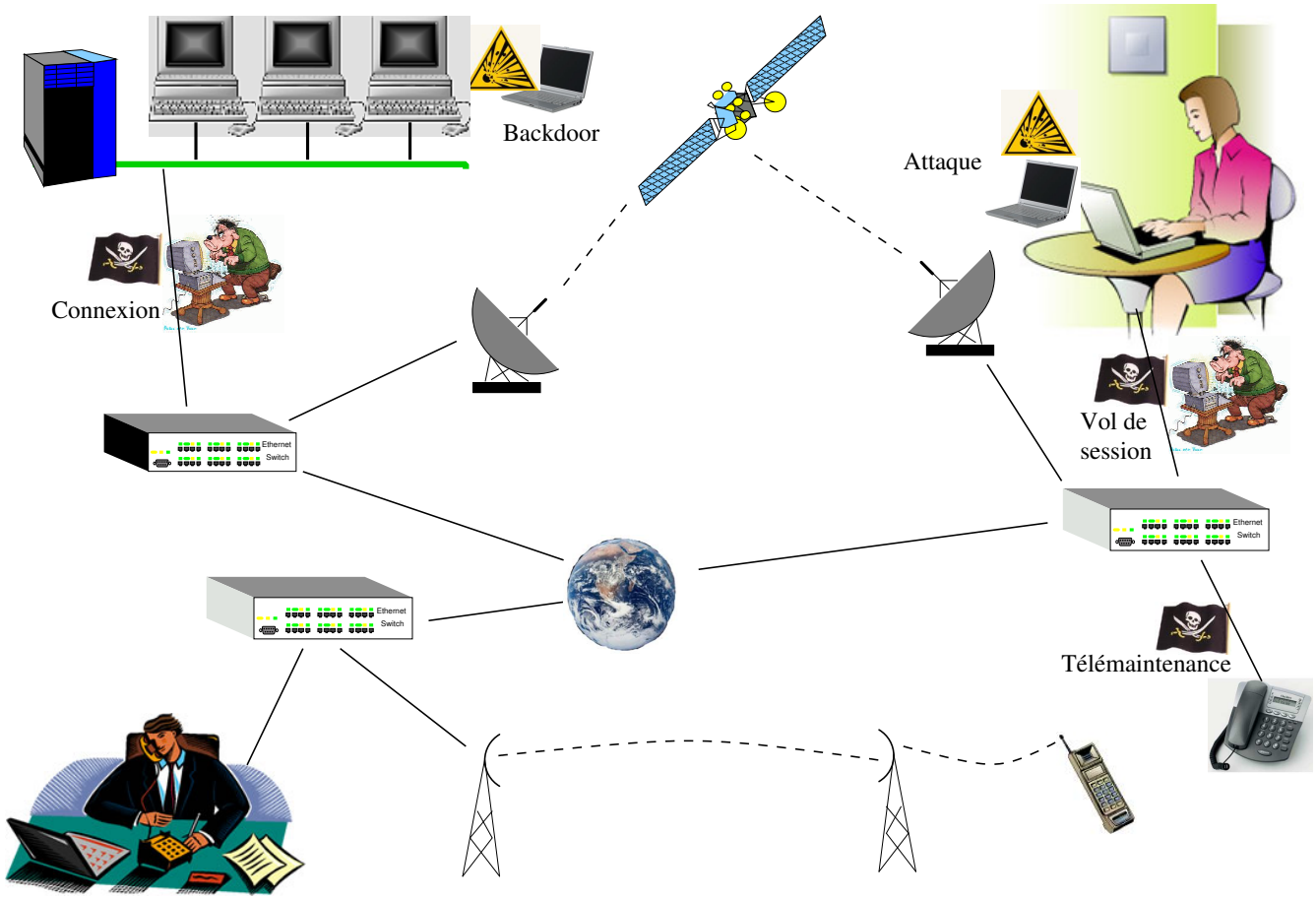
# Les systèmes d'information sont distribués...



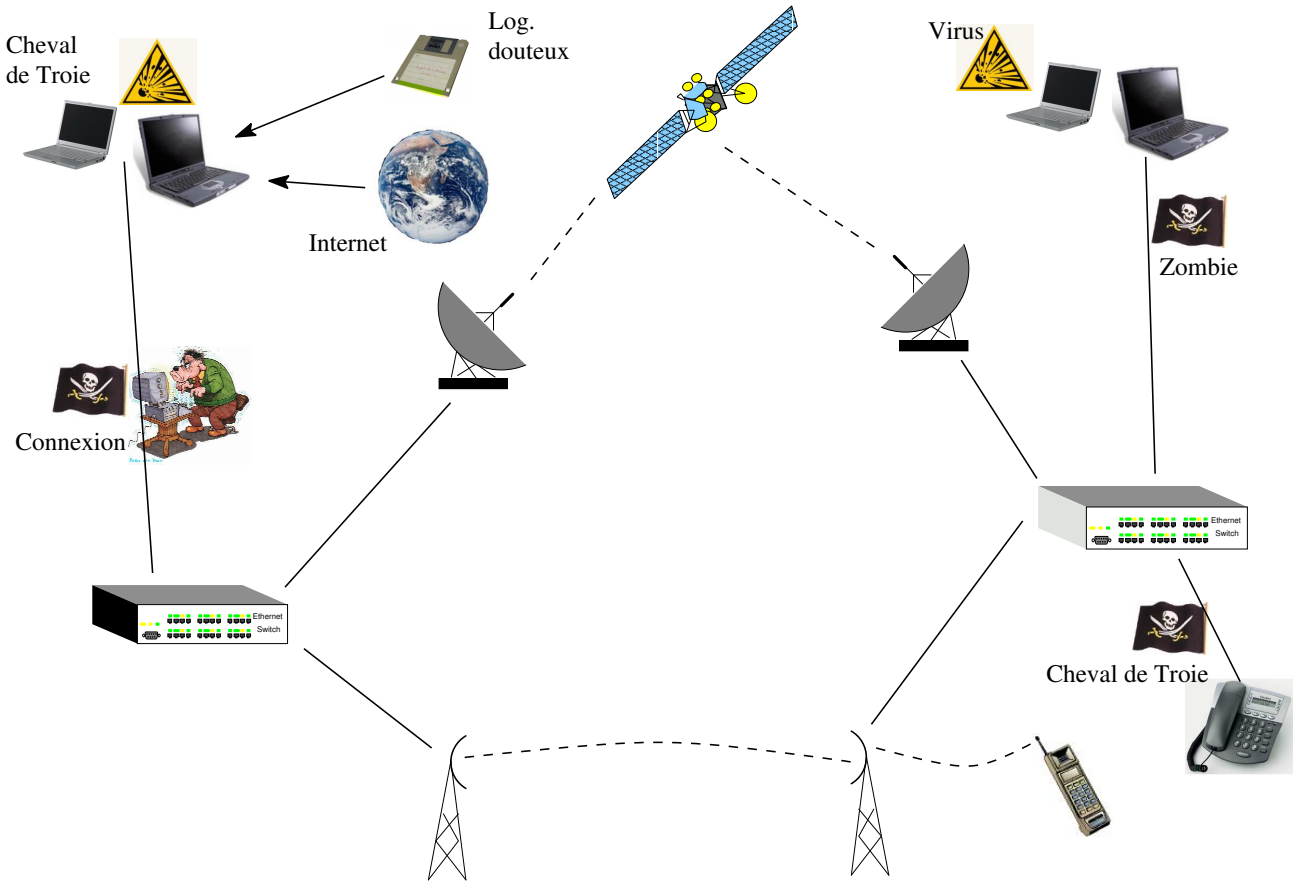
# . . . vulnérables à l'écoute passive



# . . . vulnérables à l'intrusion



# . . . vulnérables à la prise de contrôle



# Définitions

**Vulnérabilité.** Faiblesse/faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système.

**Attaque.** Action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité.

**Intrusion.** Faute opérationnelle, externe, intentionnellement nuisible, résultant de l'exploitation d'une vulnérabilité dans le système.

**Menace.** Violation potentielle d'une propriété de sécurité.

**Risque.** Couple (menace, vulnérabilité).

# Définitions

**Bombe logique.** Partie de programme qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein.

**Cheval de Troie.** Programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime ; la fonction illicite peut être de divulguer ou d'altérer des informations, ou peut-être une bombe logique.

# Définitions

**Backdoor.** (porte dérobée) Moyen de contourner les mécanismes de sécurité ; il s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier) ; ces passages secrets sont aménagés par les concepteurs de logiciels pour fournir des accès privilégiés pour les tests ou la maintenance ; mais les pirates qui les découvrent peuvent déjouer tous les mécanismes de sécurité et rentrer dans le système.

# Définitions

**Virus.** Segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'application), et qui devient ainsi un cheval de Troie ; propriétés : infection, multiplication, fonction nocive.

**Ver.** Programme autonome qui se reproduit et se propage à l'insu des utilisateurs.

**Spyware.** Contraction de *spy* et *software* ; logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers ; exemple : Keylogger (transmettre les données saisies au clavier).

# Définitions

**Spamming.** Usage abusif d'un système de messagerie destiné à exposer délibérément (et de manière répétée) les utilisateurs à des contenus non pertinents et non sollicités.

**Sniffing.** (écoute passive) Accéder aux données transmises sur canal de communication (exemple : câble de réseau), stockées sur un support vulnérable (exemple : disque externe).
*Menace :* accès à des informations sensibles ;
exemple : mot de passe d'un utilisateur tapé sur un terminal connecté à un ordinateur central, et qui transite en clair entre ce terminal et la machine.

# Définitions

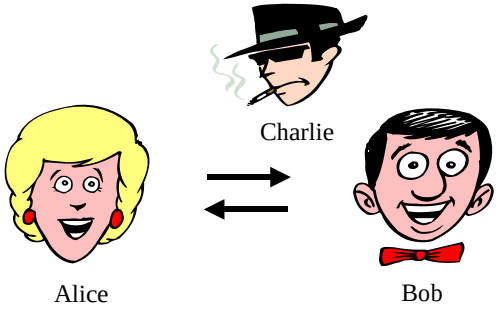
**Spoofing.** (usurpation d'identité) Se faire passer pour quelqu'un d'autre afin de faire une action malveillante (exemple : envoi virus, spam,...).
*IP spoofing :* utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité.
*Phishing :* Site miroir « contrefait » semblable à un portail de renom ; but : attirer les internautes réellement clients du site plagié.

# Définitions

**DoS/DDoS.** (déni de service) Attaque d'un serveur destinée à l'empêcher de remplir sa fonction.
*Méthode classique :* faire crouler le serveur sous une masse de requêtes généralement mal formées à dessein pour entraîner un réponse anormale et paralysante.
Utilise très souvent une multitude de PC zombies travaillant de concert, infectés par des backdoors / chevaux de Troie et mobilisables à distance par un pirate ; possibilité de bloquer aussi à distance des routeurs en tirant parti de failles de leur software.

# Motivation


- Le monde est distribué :
  - Nos infrastructures sont de plus en plus basées sur des systèmes d'information en réseau.
  - Business, finance, communication, distribution d'énergie, transport, ...




Alice → Bob@Banque : « Transférer 100€ sur le compte $X$ »

Bob@Banque → Alice : « Transfert effectué »

- Comment Bob sait-il qu'il discute vraiment avec Alice ?
- Comment Alice sait-elle que c'est Bob qui a répondu ?
- Confidentialité, intégrité, disponibilité, non-répudiation, anonymat, ... ?

# Motivation


- Le monde est distribué :
  - Nos infrastructures sont de plus en plus basées sur des systèmes d'information en réseau.
  - Business, finance, communication, distribution d'énergie, transport, ...
- Il faut protéger les informations par chiffrement, ...
- et des protocoles, essentiels pour développer des services réseaux et de nouvelles applications.
- Les erreurs dans la conception de protocoles sont coûteuses.

| | |
|---|---|
| Argent : | mises-à-jour coûtant des centaines de millions \$/€. |
| Temps : | protocoles retardés d'années en années. |
| Confiance : | érosion de la confiance en la sécurité d'Internet et des nouvelles applications. |

# Utilisation de protocoles de sécurité

## Communication dans un environnement ouvert

Alice et Bob échangent des Messages
Un Intrus peut contrôler le canal de communication

## Objectifs de sécurité pour : *A envoie un message M à B*

Confidentialité (seuls A et B connaissent M)
Intégrité des données (M n'est pas altéré)
Authenticité (B sait que A a envoyé M)
Non répudiation (A ne peut nier qu'il a envoyé M)

## Protocoles cryptographiques

SSL : navigateurs sur Internet
PGP : courrier électronique
SET : commerce électronique
Kerberos : connexion à distance...