Introduction à la Cybersécurité

Rushed Kanawati
http://kanawati.fr

kanawati@sorbonne-paris-nord.fr

Module CyberSec

Janvier, 2023

Plan

Organisation du cours

Module Introduction à la cybersécurité **15h**

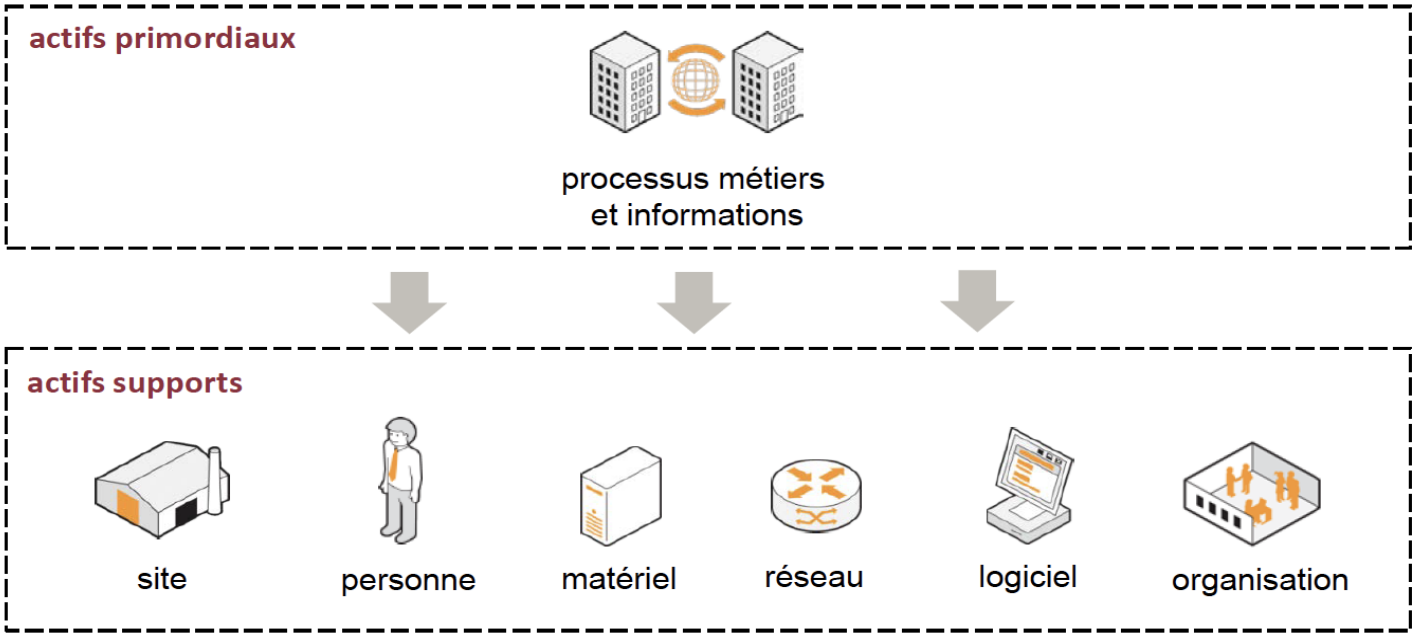
- 10 séances de cours /TP
- un contrôle long
- TP notés

Notions abordées

- Les enjeux de la sécurité des systèmes et les règles d'hygiènes informatiques
- Infrastructure de sécurité dans les réseaux informatiques
- Cryptographie

ENJEUX DE LA SÉCURITÉ DES S.I.

Le système d'information d'une organisation contient un ensemble d'actifs :



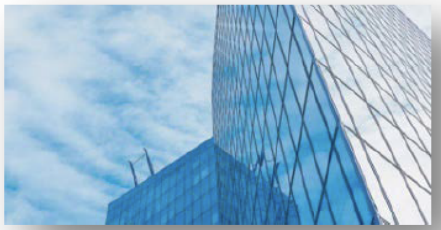
ISO/IEC 27005:2008

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

Crédit : CyberEdu - ANSII

ENJEUX DE LA SÉCURITÉ DES S.I.

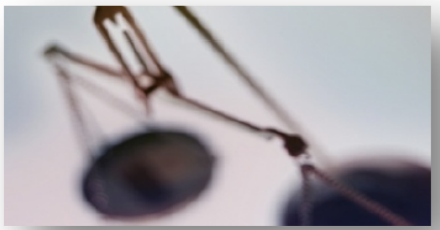
Impacts financiers



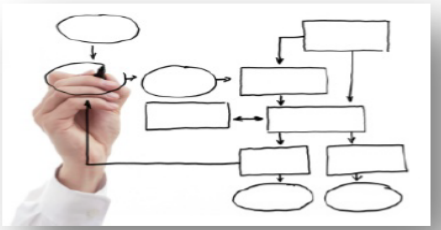
Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires



Impacts organisationnels



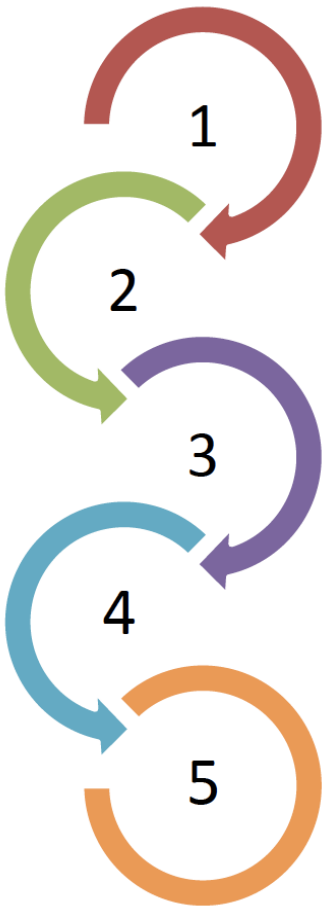
Crédit : CyberEdu - ANSII

Cyber délinquance : Motivations

- Années 80 : bidouilleurs !
- Aujourd'hui : actions organisées et réfléchies
- Criminalité organisée
- Hacktivistes
- Concurrents
- fonctionnaires au service d'un état
- mercenaires agissant pour le compte de commanditaires
- ...

ENJEUX DE LA SÉCURITÉ DES S.I.

Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs



1. des groupes spécialisés dans le **développement de programmes malveillants** et virus informatiques
2. des groupes en charge de l'**exploitation et de la commercialisation** de services permettant de réaliser des attaques informatiques
3. un ou plusieurs **hébergeurs** qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates
4. des groupes en charge de la **vente des données volées**, et principalement des données de carte bancaire
5. des **intermédiaires financiers** pour collecter l'argent qui s'appuient généralement sur des réseaux de **mules**

Crédit : CyberEdu - ANSSI

IMPACTS SUR LA VIE PRIVÉE

- Impact sur l'image / réputation
- Usurpation d'identité
- Perte définitive de données
- Impacts financiers
- ...

IMPACTS SUR LES INFRASTRUCTURES CRITIQUES

- Infrastructures critiques = un ensemble d'organisations parmi les secteurs d'activité suivants, et que l'État français considère comme étant tellement critiques pour la nation que des mesures de sécurité particulières doivent s'appliquer
  - Secteurs étatiques : civil, justice, militaire…
  - Secteurs de la protection des citoyens : santé, gestion de l'eau, alimentation
  - Secteurs de la vie économique et sociale : énergie, communication, électronique, audiovisuel, information, transports, finances, industrie.

- Ces organisations sont classées comme **Opérateur d'Importance Vitale (OIV).** La liste exacte est classifiée (donc non disponible au public).

Crédit : CyberEdu - ANSSI

IMPACTS : EXEMPLES

Quelques exemples d'attaques, ce qui pourrait arriver

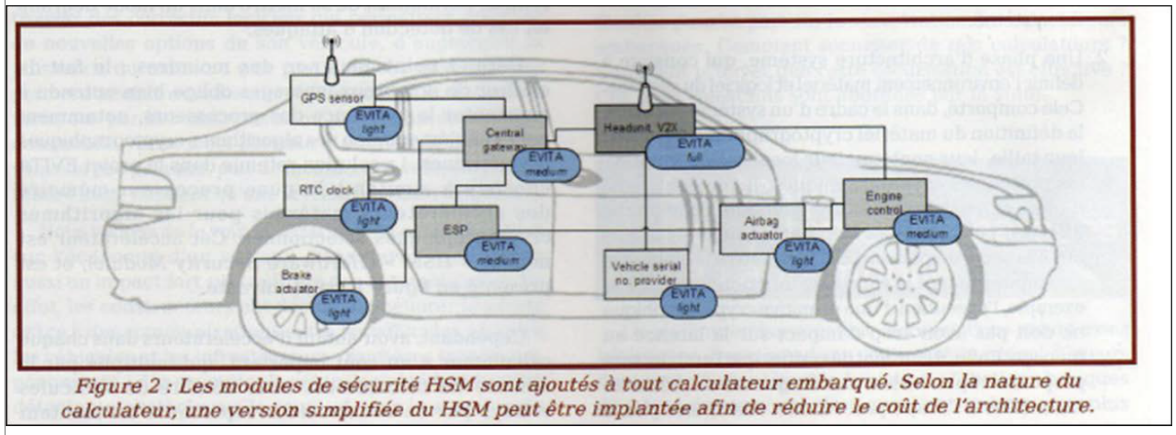
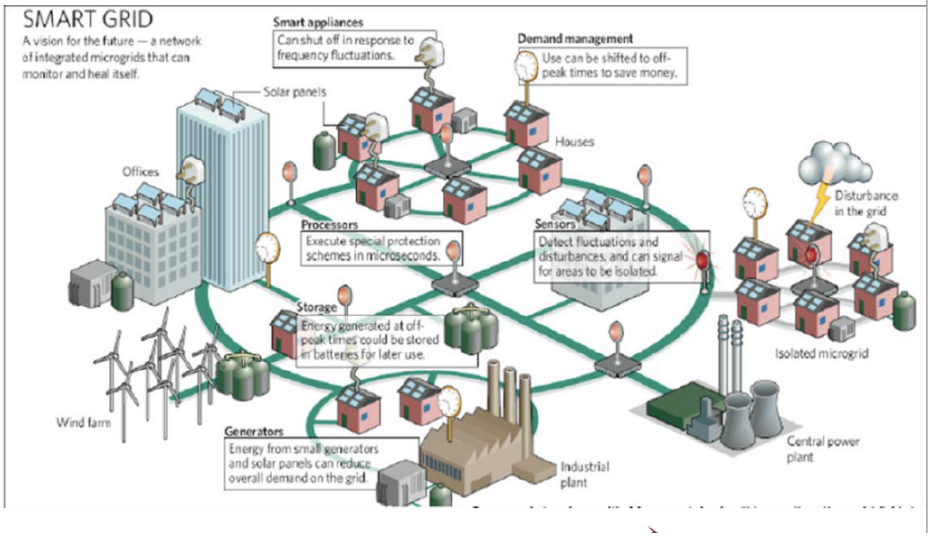


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout calculateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

Cyberattaques sur la voiture connectée envisagées à l'horizon 2020
Exemple : Prise de contrôle du système de frein

Déploiement des smart grid prévu à l'horizon 2030
Exemple : Blackout sur une grille.



Crédit : CyberEdu - ANSSI

SÛRETÉ OU SÉCURITÉ ?

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

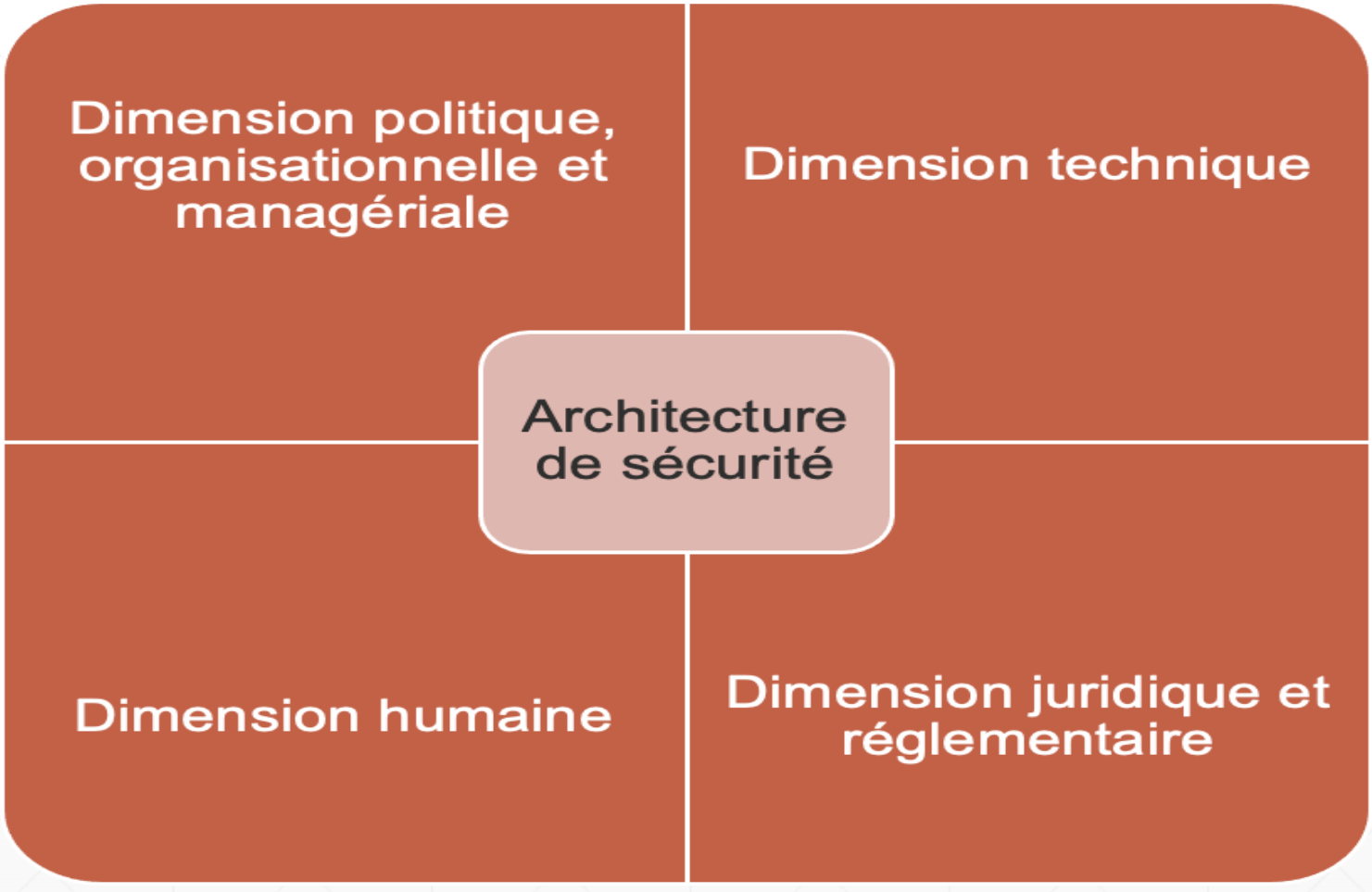
Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage…*

Crédit : CyberEdu - ANSSI

ARCHITECTURE DE SÉCURITÉ : DIMENSIONS



Problématique

Problèmes de sécurité

- Problèmes de gestion
  - Perte de données suite à des mauvaises manipulations,
  - Conséquences des incendies, catastrophes naturelles, etc.
  - Duplication, repartition des données, Journalisation, sauvegarde automatique
- **Problèmes liés à des *attaques* d'un tiers malveillant**

Objectifs d'un système de sécurité

- **Confidentialité**
  Seuls les utilisateurs ayant droit ont accès aux données
- **Intégrité**
  Seuls les utilisateurs ayant droit peuvent modifier les données
- **Disponibilité**
  Garantir l'accessibilité des données aux utilisateurs ayant-droit
- **Authenticité**
  Garantir d'avoir l'identité exacte de la source d'une action
- **Non-répudiation**
  Garantir que le destinataire (resp. émetteur) d'un message ne peut pas prétendre ne pas l'avoir reçu (resp. envoyé).

Le cycle PPR

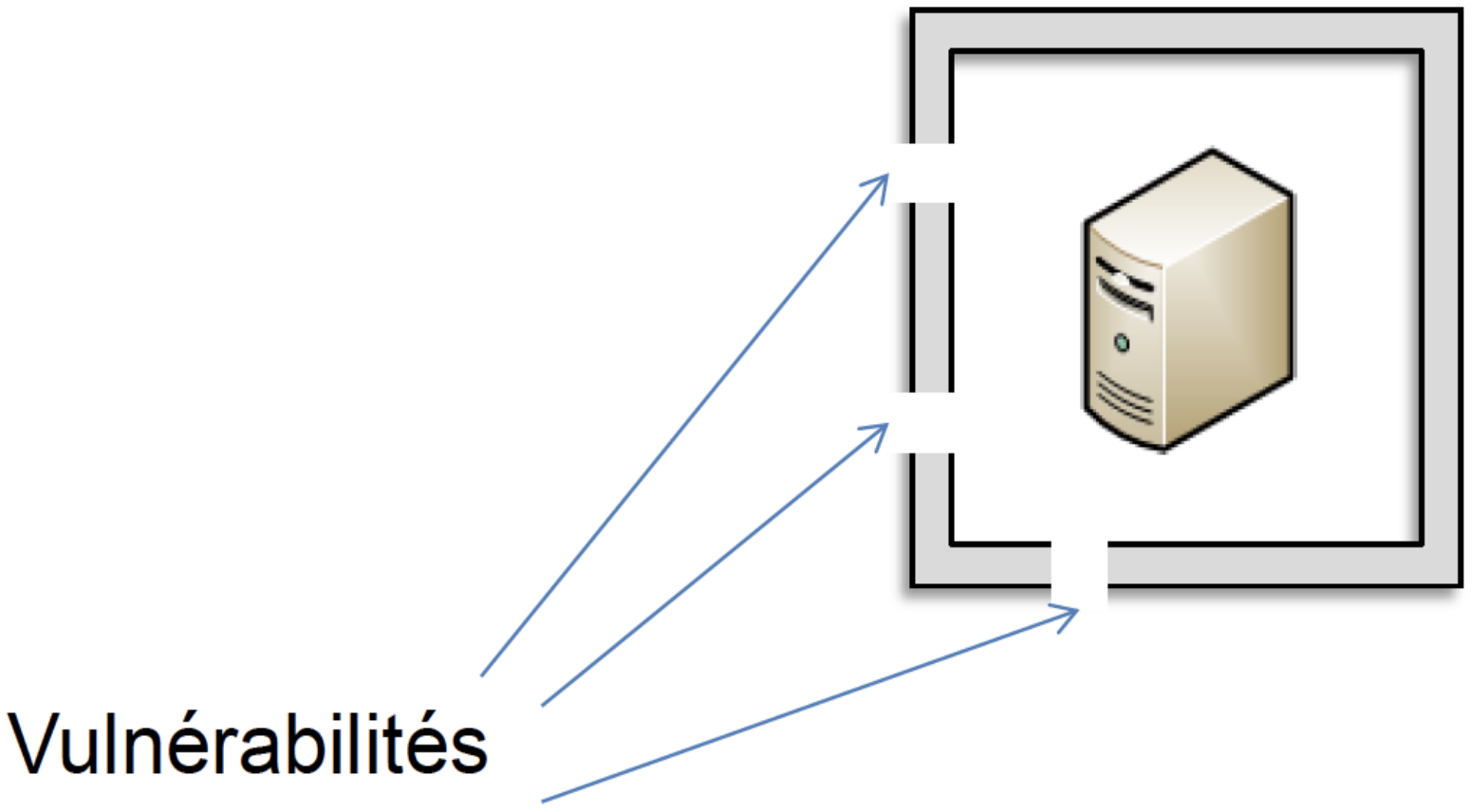
- **PPR** : Planification → Protection → Réaction
- **Planification** : Analyses des menaces (montant des dommages, Probabilité, coût de la protection, priorité) → règles & règlement
- **Protection** : Sélection et installation des outils, mise à jour, audit (test et mise à l'épreuve).
- **Réaction** : Détection de l'incident, procédure de réaction, restauration et sanction, **retour d'expérience** et réparation de failles.

Notions de base

Vocabulaires

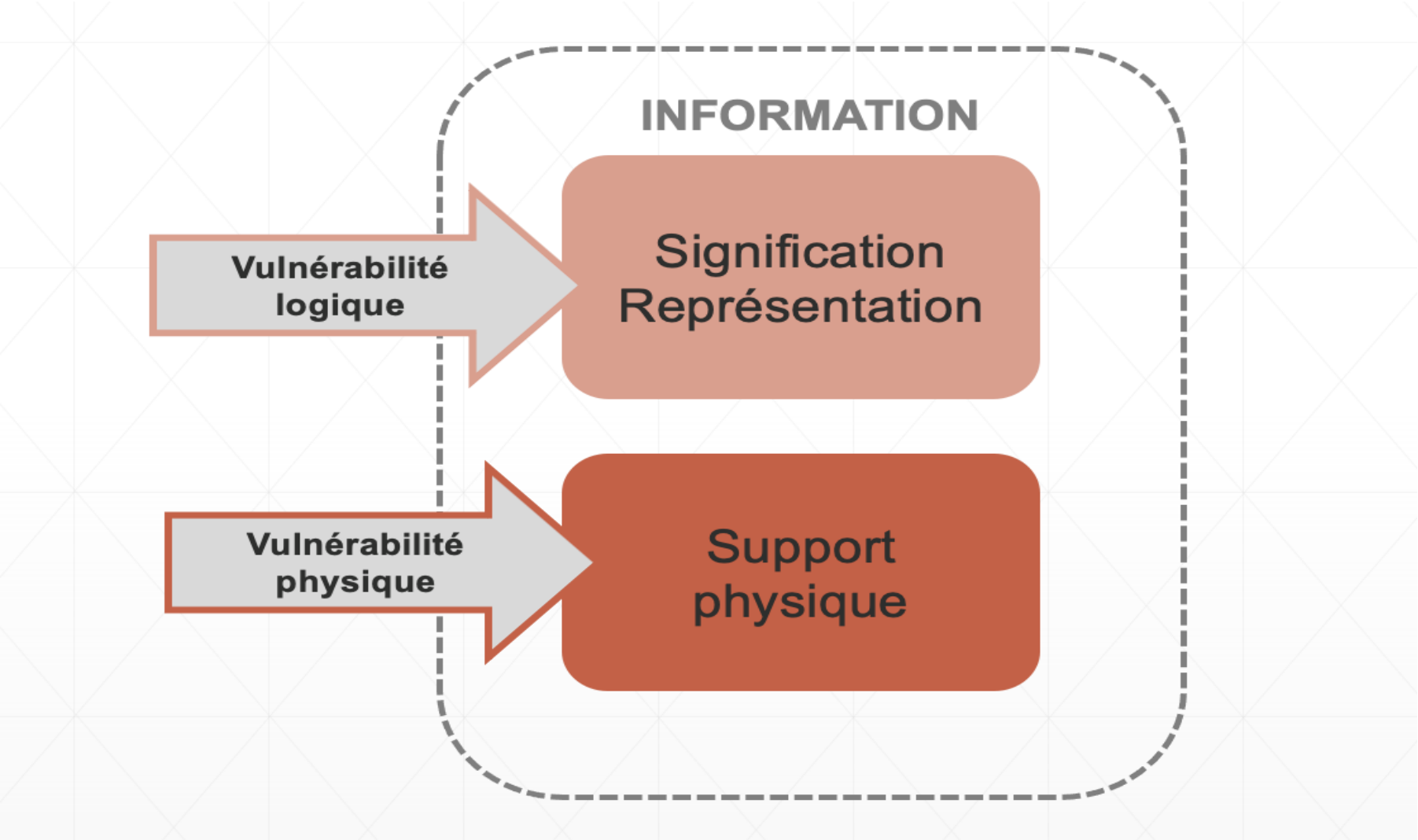
- **Vulnérabilité** : Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).
- **Menace** : Cause potentielle d'un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait
- **Attaque** : Une action qui vise à compromettre la sécurité d'un système.
- **Intrusion** : Prise de contrôle, partielle ou totale d'un système distant.
- **Usurpation** : (spoofing) la prise d'identité d'autrui (utilisateur ou système) afin de gagner une accès illégitime à un système.

VULNÉRABILITÉ



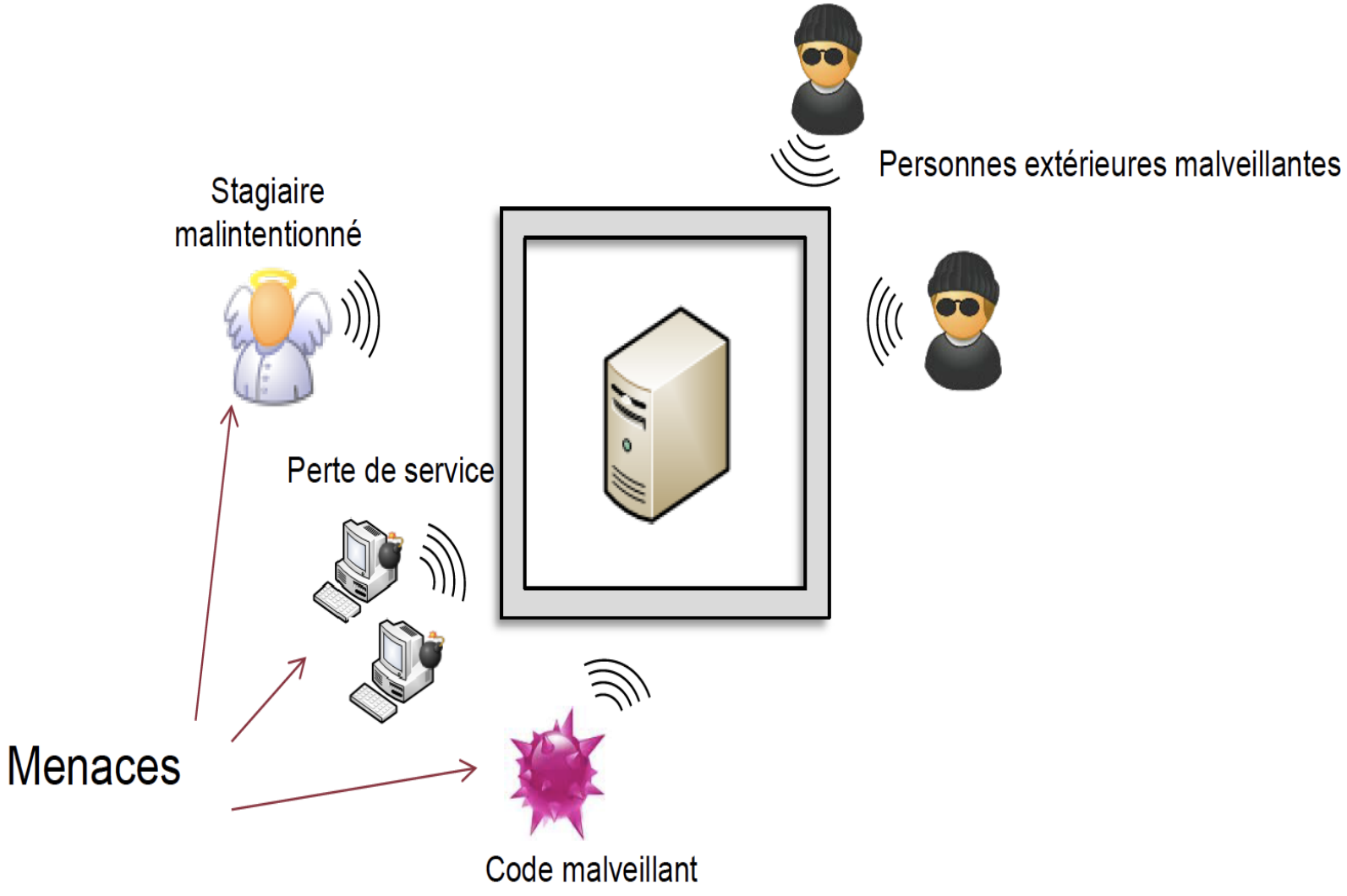
Crédit : CyberEdu - ANSSI

VULNÉRABILITÉ : TYPES



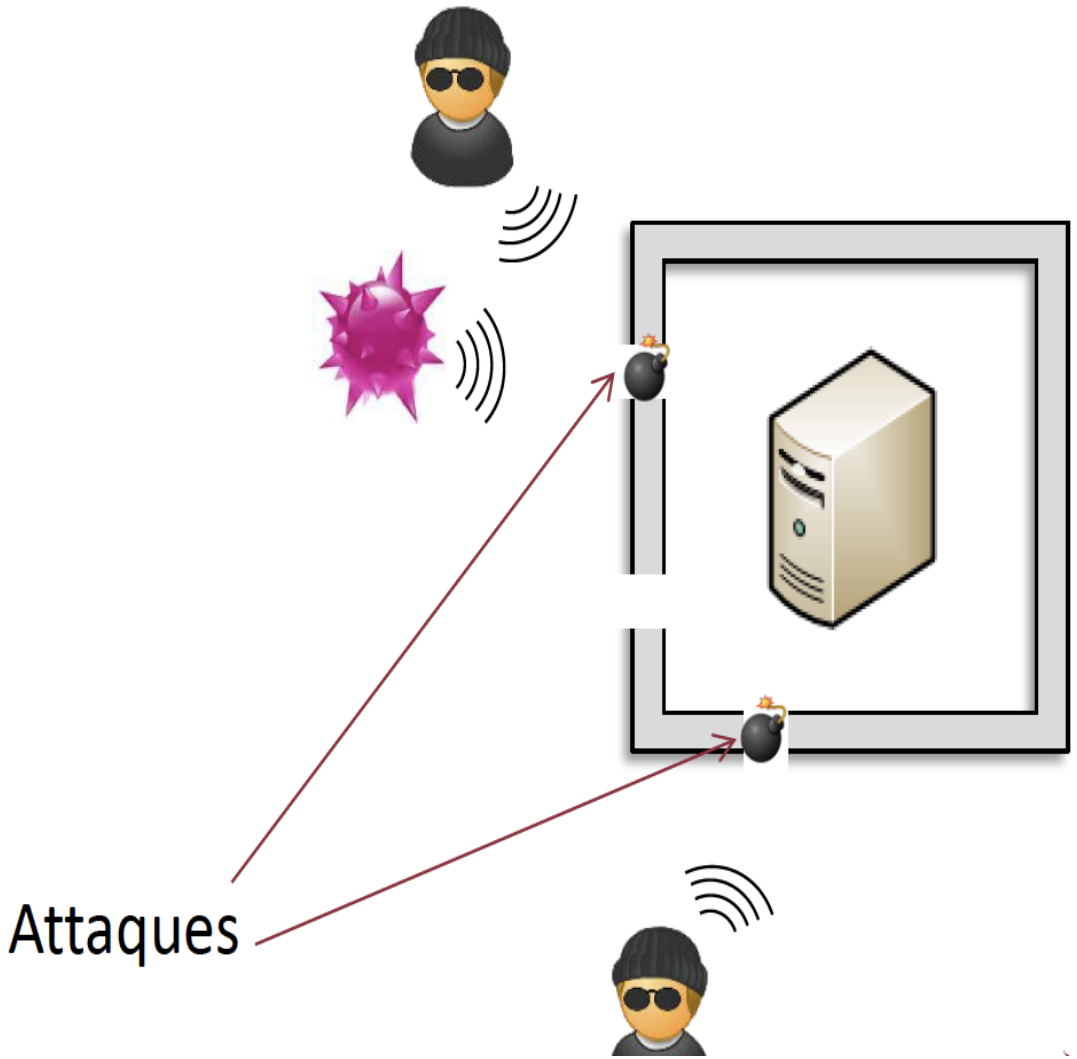
Crédit : CyberEdu - ANSSI

Menace



Crédit : CyberEdu - ANSSI

Attacque

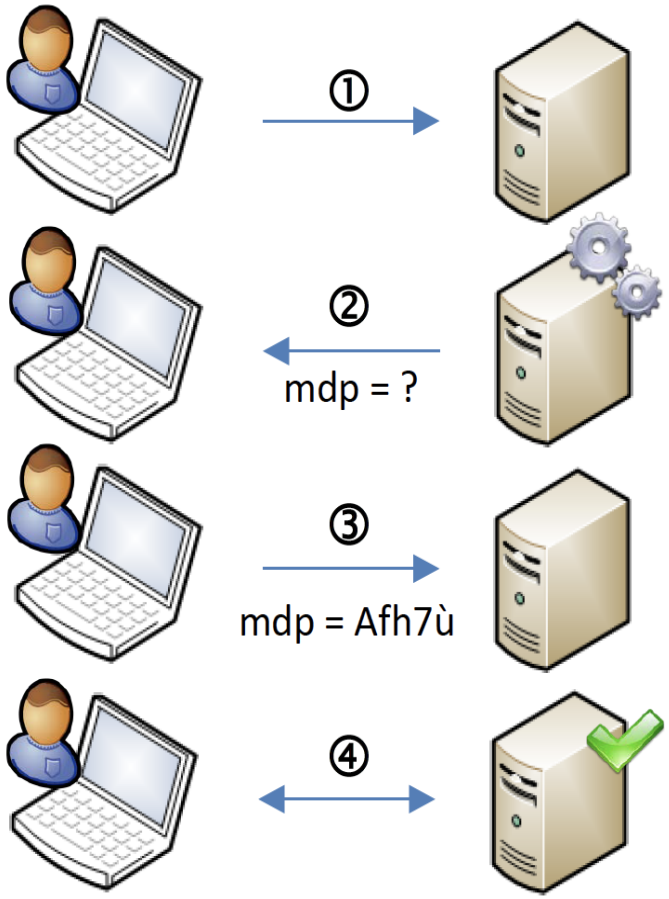


Crédit : CyberEdu - ANSSI

VULNÉRABILITÉ : EXEMPLE APPLICATION VNC

Description du fonctionnement normal de l'application

L'utilisateur effectue une demande de connexion au serveur depuis son PC client



Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat*, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur

L'utilisateur s'authentifie selon la méthode choisie par le serveur

Le serveur valide l'authentification (si elle est correcte) et autorise donc la connexion

Crédit : CyberEdu - ANSSI

VULNÉRABILITÉ : EXEMPLE APPLICATION VNC

L'attaquant effectue une demande de connexion au serveur depuis son PC client

①

Description du fonctionnement modifié par un attaquant

②

mdp = ?

Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat*, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur

L'attaquant choisit de s'authentifier avec le mécanisme de son choix, et non pas avec le mécanisme choisi par le serveur. Ici il choisit la méthode « pas d'authentification »

③

authent = NON

④

Le serveur valide l'authentification (car elle est valide i.e. aucune authentification est une méthode valide) et autorise donc la connexion

Crédit : CyberEdu - ANSSI

Types d'attaques

- **Attaques non ciblées**
  - Attaques contre des proies aléatoires.
  - Utilisation de **maliciels** (malware)
  - Vecteurs de propagation : e-mail, sites web contaminés, SMS, etc.
- **Attaques ciblées**
  - Attaque contre une cible identifiée afin de compromettre une propriété de base de la sécurité de systèmes (intégrité, disponibilité, confidentialité, . . . , etc.)

Types d'attaques

- **Attaques passives**
  - Interception
  - Ecoute
  - Espionnage
  - Cartographie
- **Attaques actives**
  - Modification
  - Fabrication
  - Interruption
  - Destruction

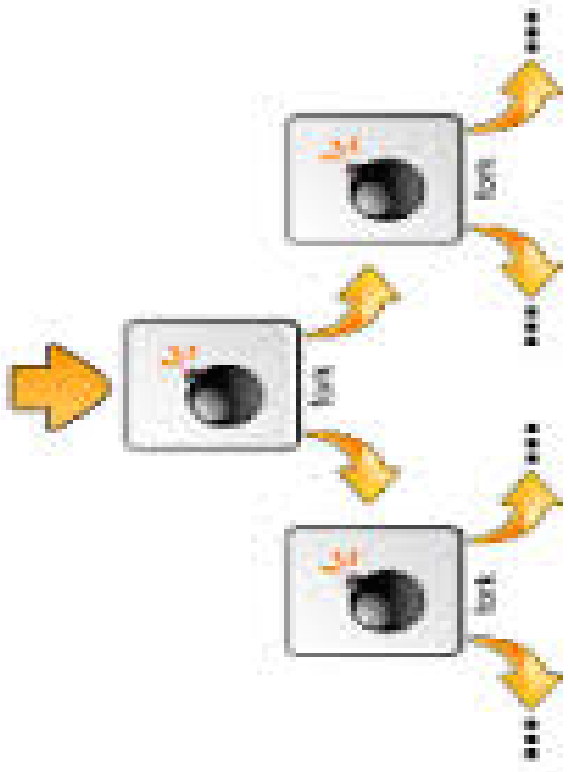
MALICIELS : VIRUS

- Virus informatique : Un programme capable de se répliquer et conçu pour se propager à d'un ordinateur à un autre en s'insérant dans des logiciels légitimes, appelés **hôtes**.

MALICIELS : VERS

- Vers : un programme capable de se répliquer et conçu pour se propager d'une manière autonome à travers les réseaux.

MALICIELS : WABBIT



- Wabbit : un programme capable de se répliquer mais ne possède pas la capacité de propagation dans les réseaux.
- **:(){ :|: & };:**

Maliciels : Cheval de Troie

- Cheval de Troie : Un maliciels qui prend l'apparence d'un logiciel légitime.
- Vecteur de propagation: sites de téléchargement !
- Souvent employé pour mettre en place d'autres maliciels : virus, vers, trappes, logiciels d'espionnage, etc.

MALICIELS : TRAPPE (BACKDOOR)

- Trappe : un programme installé sur la machine victime et qui se connecte à la machine de l'attaquant pour lui donner un accès à la machine infectée.
- Installé par un développeur d'une application, ou par un autre maliciels (ex. cheval de Troie).

MALICIELS : ESPIONS (SPYWARE)

- Logiciel espion : logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur n'en ait connaissance.
- `Keylogger` : Matériel ou logiciel qui enregistre les touches frappées sur le clavier et les transmettre via les réseaux ou via des ondes électromagnétiques.

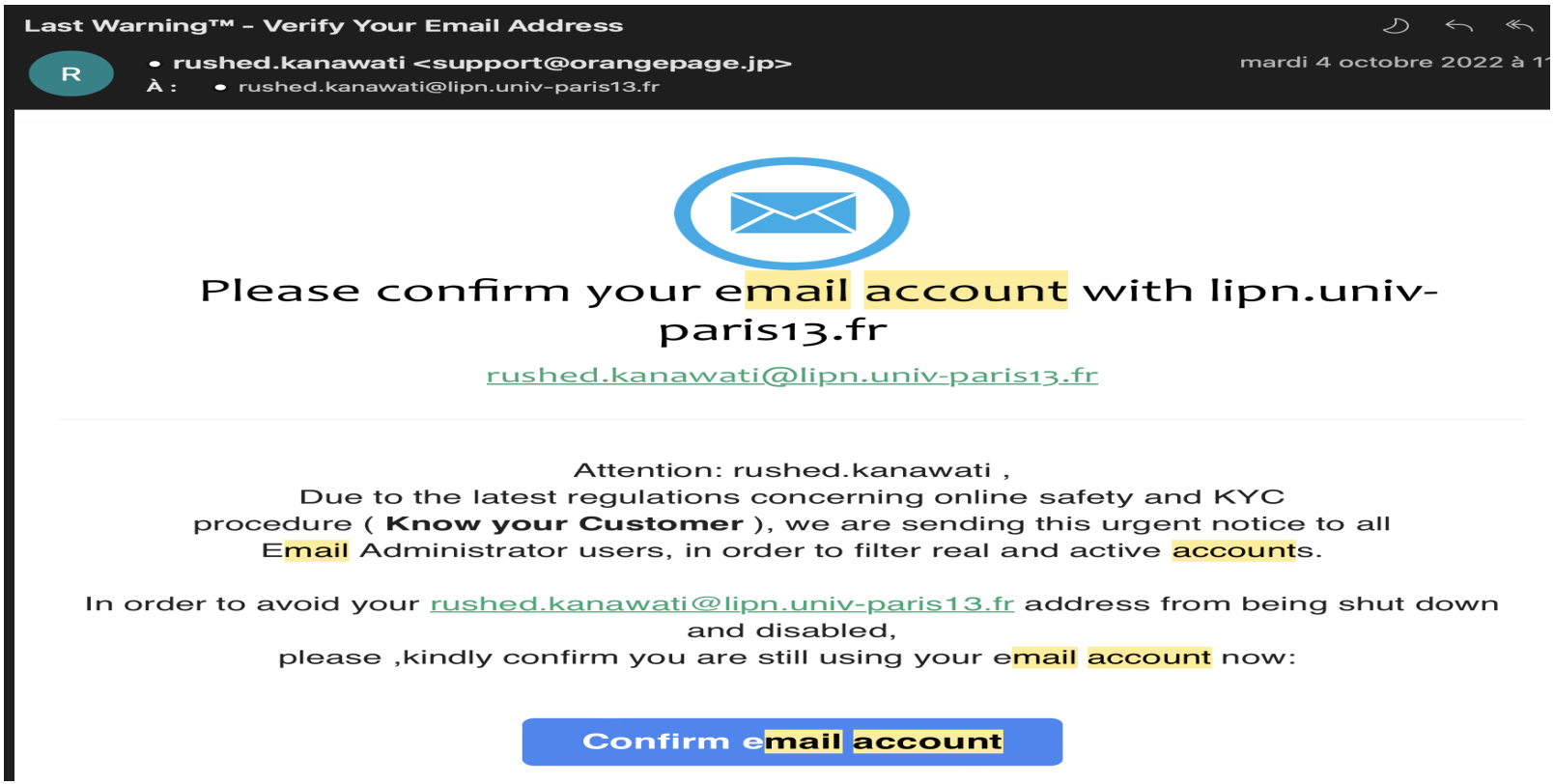
MALICIELS : ATTAQUES PAR-E-MAIL

- **Hoax** (Canular) : Courrier électronique incitant le destinataire à retransmettre le message à ses contacts sous divers prétextes (bon sentiments, alarmes, légendes urbaines, etc.)

  `http://www.hoaxbuster.com/`
- **Spam** : courriers non sollicité qui encombrent le réseau.
- **hameçonnage** (phishing) : courrier dont l'expéditeur se fait généralement passé pour un organisme demandant au destinataire de fournir des informations confidentielles

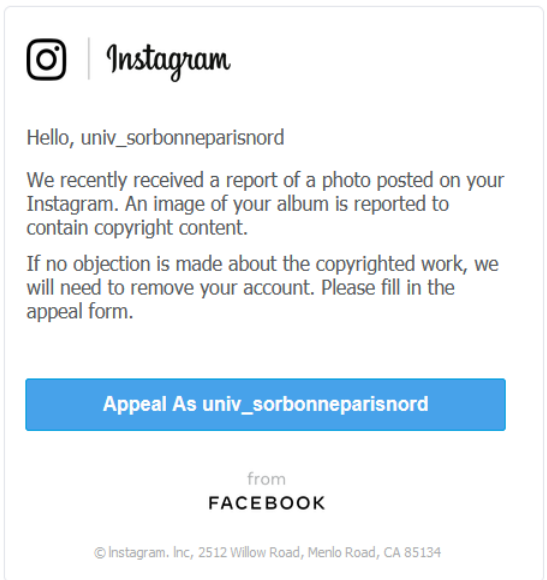
PHISHING : EXEMPLE

PHISHING : EXEMPLE

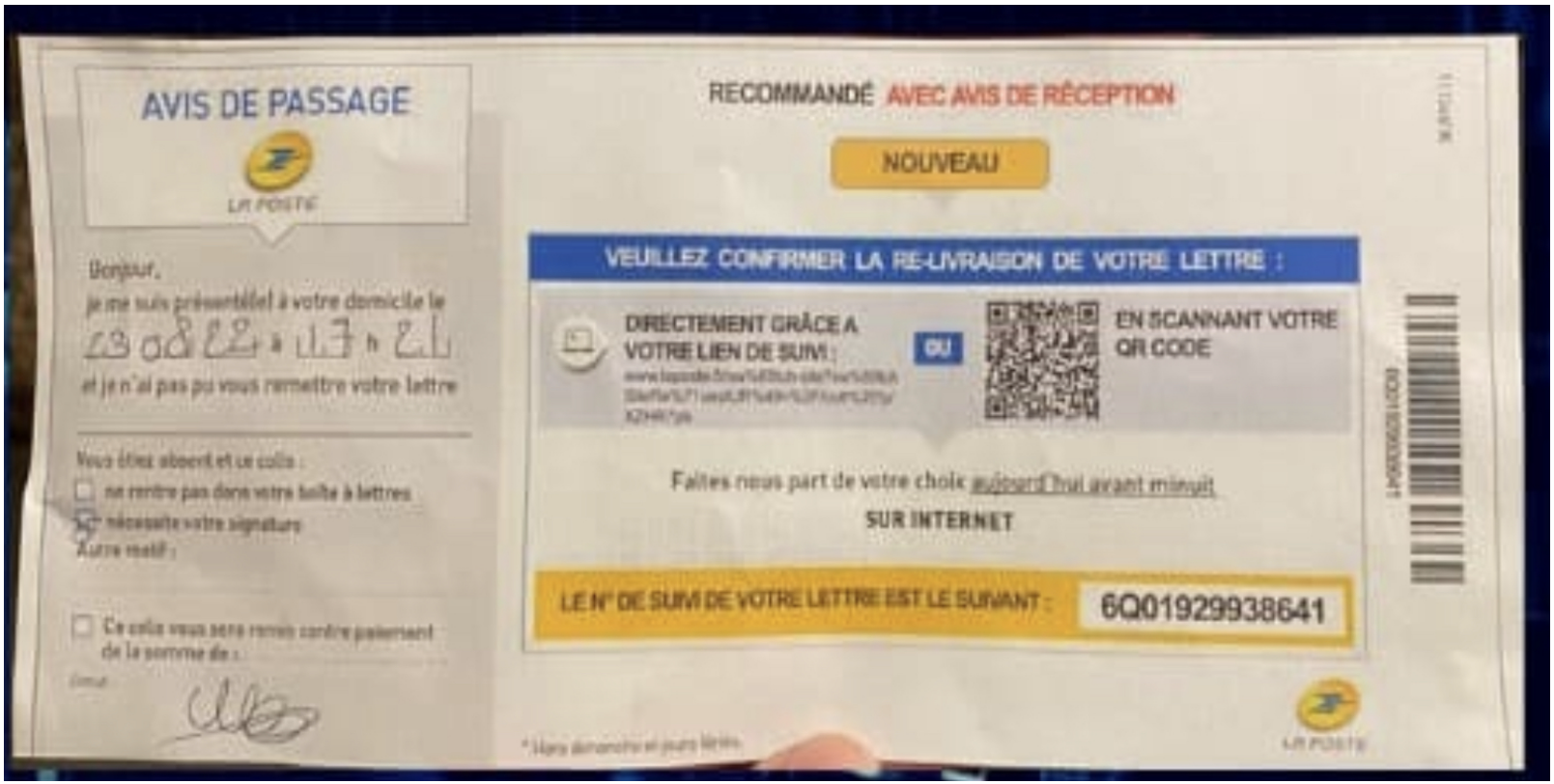


PHISHING : EXEMPLE

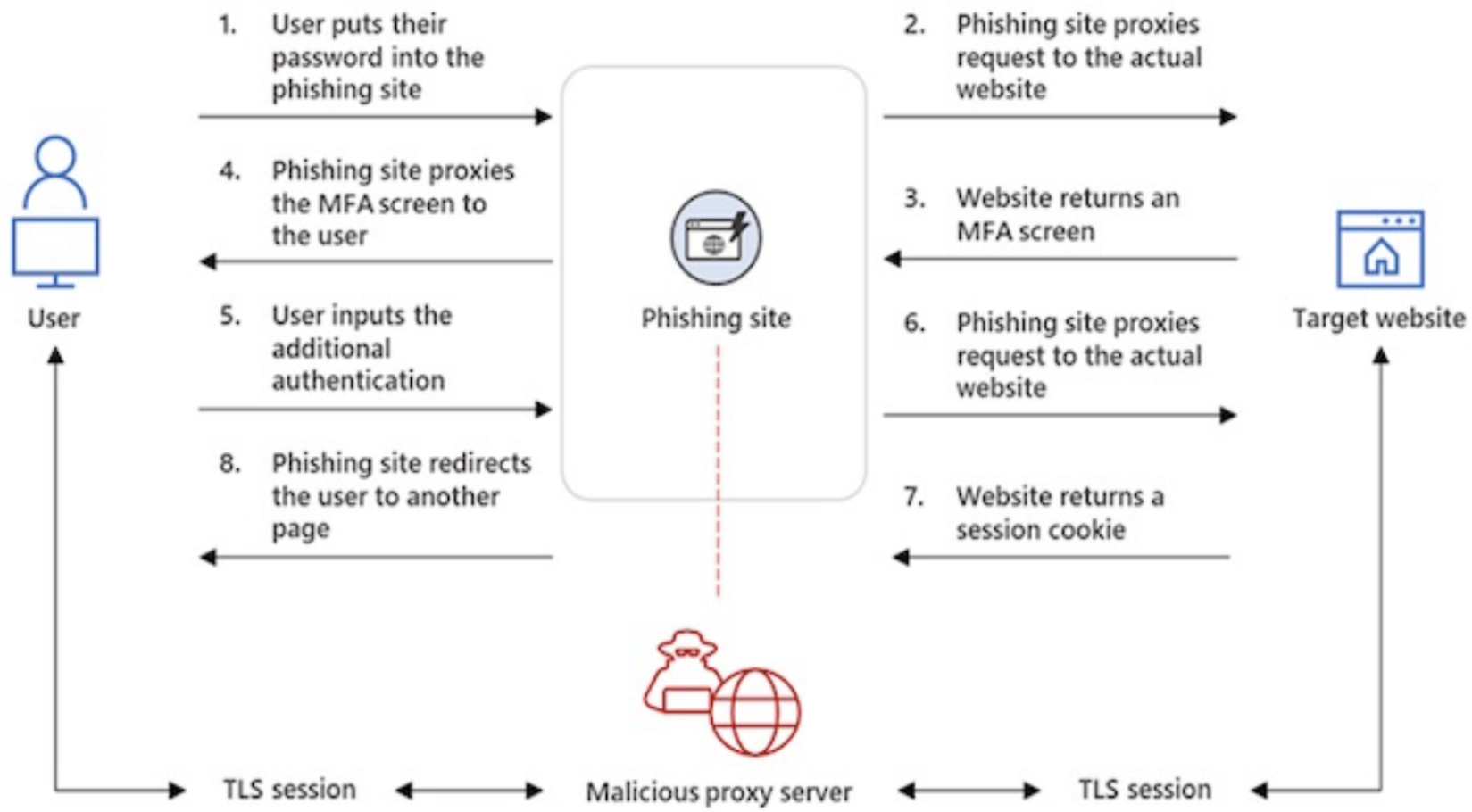
-------- Message transféré --------
Sujet : Copyright @univ_sorbonneparisnord #458609
Date : Mon, 28 Mar 2022 08:57:33 +0000
De : Copyright <info@supports-meta.com>
Pour :communication@univ-paris13.fr



Phishing : exemple



EvilProxy


1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
4. Phishing site proxies the MFA screen to the user
3. Website returns an MFA screen
User
Phishing site
Target website
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
8. Phishing site redirects the user to another page
7. Website returns a session cookie
TLS session
Malicious proxy server
TLS session

Attaques ciblées: buts 1/2

- **Attaques des systèmes**
  - **Interruption** : réduire la disponibilité d'un système

    Déni de service (DoS)
  - **Cartographie** : Reconnaitre les machines et les services actifs et les versions des systèmes d'exploitation

    Balayage des machines et des ports
  - **Modification de données**

    DNS poisoning, ARP poisoning

ATTAQUES CIBLÉES: BUTS 2/2

- **Attaques des communications**
  - **Interception de messages**

    Ecoute & analyse de traffic (snifing)
  - **Modification, fabrication de messages**

    Usurpation d'adresses IP
  - **Vol de sessions**

Attaques : Attaques DoS simples

Ping de la mort

- Envoyer un paquet `ping` malformé (taille > taille max de 65 535)
- La plupart des systèmes jusqu'au 1998, ne peuvent pas traiter un tel paquet

LAND

- Envoyer un paquet `SYN` malformé : mêmes adresses IP sources et destinations et mêmes ports
- Conséquence: blocage du système visé

Teardrops

- Envoyer des fragments IP avec des informations erronées de décalage (offsets).

ATTAQUES PAR SATURATION

Rafales de SYN

- Envoyer une rafale de paquets `SYN`.
- La victime alloue une partie de ses ressources à chaque demande : on assiste à à un phénomène de saturation, voire de pannes

Rafales d'Echo-Reply

- Envoyer un message `echo-request` avec @Source = @Victime, @Dest: mode diffusion
- Si la victime est reliée à un routeur opérant en mode diffusion, tous les ordinateurs du réseau répondent à la victime par des `echo-reply`.

ARP POISONING

- Envoyer un paquet ARP avec @MAC: pirate et @IP: @victime
- Le trafic vers la victime sera d'abords adressée au pirate tant que la victime n'as pas communiqué avec la machine cible !
- Mise à jours sans relâche de la table ARP.

Quelques outils

nmap

- nmap: Network Mapper
- Téléchargement: `http://insecure.org`.
- Logiciel de balayage de ports (tcp; udp, rcp)
- Interface graphique et API pour script
- A étudier en TP1

Avertissement

Tout acte de balayage de réseau non-autorisé est assimilé à une attaque et donc répréhensible selon la loi française.

NMAP

Principe

Solliciter des machines à balayer des réponses montrant l'état des différents ports. Par défaut on balaye les ports systèmes (< 1024)

Etats des ports

- **open** (ouvert) : port associé à un service actif.
- **closed** (fermé) : port associé à un service inactif.
- **filtered** (filtré) : Port inaccessible à cause d'un pare-feu par exemple.
- **unfiltered** (non filtré) : port accessible mais `nmap` n'arrive par à déterminer s'il est ouvert ou fermé.

NMAP : FONCTIONNEMENT

- Si l'adresse de la machine cible est donnée sous forme symbolique, une résolution `DNS` est déclenchée (à moins que l'adresse IP de la machine est donnée dans le fichier local *hosts*)
- `nmap` envoie un paquet ICMP et attends le retour (opération ping). Cette phase peut être évitée en utilisant l'option `-P0`.
- Si la destination est spécifiée sous forme d'adresse IP, une phase de résolution inverse `DNS` est déclenchée. Cette phase peut être évitée en utilisant l'option `-n`.
- Le balayage spécifié est exécuté.

Syntaxe

```
nmap [types de scans] [options] cibles
```

NMAP : TYPES DE BALAYAGES

Table: Principaux types de balayage

Type de balayage	Syntaxe	mode root exigé
TCP SYN	`-sS`	OUI
TCP connect	`-sT`	NON
FIN	`-sF`	OUI
XMAS Tree	`-sX`	OUI
NULL	`-sN`	OUI
PING	`-sP`	NON
Détection de version	`-sV`	NON
UDP	`-sU`	OUI
IP	`-sO`	OUI
Acquittement	`-sA`	OUI
Idle	`-sI`	OUI

Quelques outils

scapy

- http://www.secdev.org/projects/scapy/
- API en Python pour la manipulation de paquets.
- Fonctions de construction, d'écoute et réactions.
- Logiciel de forage de paquets et de trames
- Permet d'envoyer des paquets mal-formés, usurpation d'adresses (MAC, IP, ports)
- Utilisé pour des tests et d'audits de politiques de sécurité
- Sera étudié en TP.

SCAPY : UTILISATION

Forage de paquets

- Chaque paquets peut être construit couche par couche
- Fournit un opérateur d'encapsulation qui respecte l'hiérarchie ISO/OSI
- Chaque champs d'un entête peut être manipulé
- Chaque champs d'un entête a des *valeurs fonctionnelles* par défaut
- Chaque champs peut avoir une ou plusieurs valeurs

SCAPY : UTILISATION

Exemples

```
a=IP()
a.ttl=70
b=TCP(dport=[21,22,80])
c=a/b
```

3 paquets sont ainsi générés !

SCAPY : UTILISATION

Quelques commandes

- `send` : envoi de paquets au niveau 3
- `sendp` : envoi de trames au niveau 2
- `sr` : envoi et réception de paquets au niveau 3
- `srp` : envoi et réception de trames (niveau 2)
- ...

Pare-feux

Définition

Un équipement, logiciel ou matériel, chargé de contrôler l'échange de paquets entre le réseau protégé et l'Internet.

Fonctions

- **Contrôle** : Gérer les connexions sortantes à partir du réseau local.
- **Sécurité** : Protéger le réseau interne des intrusions venant de l'extérieur.
- **Vigilance** : Surveiller/tracer le trafic entre le réseau local et internet.

Pare-feux : types

- Pare-feu au niveau réseau

  Filtrage des paquets
  Transparente pour les utilisateurs

- Pare-feu au niveau applicatif

  Proxy dédié à une application : proxy web, proxy ftp, etc.
  Possibilité d'interpréter le contenu du trafic

- Pare-feu des applications

  Restrictions au niveau des différentes applications `/etc/ftpaccess` *pour ftp*

Pare-feux à filtrage statique

Principe

- Utilisation d'un ensemble de règles de format : **SI-Alors**
- **Les règles sont évaluées d'une manière séquentielle** : La première règle applicable est exécutée !

  Dans quelle ordre faut-il inscrire les deux règles : interdir les paquets `SYN/FIN` *et accepter les connexion tcp à un serveur donné ?*
- Les règles de filtrage ne sont pas symétriques
- Le filtrage est basé sur les informations contenues dans les entêtes des paquets/trames

  Adresses src/dest, drapeaux, et numéros de port
- Nécessité de définir une politique par défaut

  ex. Bloquer tout !

Pare-feux à filtrage statique

Filtrage en sortie : règles communes

- Bloquer l'émission des paquets IP dont l'adresse source n'est pas une adresse de l'organisme !

  Eviter à un pirate interne ou externe d'envoyer des paquets d'attaques
- Filtrage des paquets ICMP (sauf ECHO-request)

  Pourquoi ?
- Filtrage de segments RST
- Filtrage de ports de serveurs
- Autorisation des connexions clientes

  Numéro de ports source $\in [49152, 65536]$

Pare-feux à filtrage statique

Limites

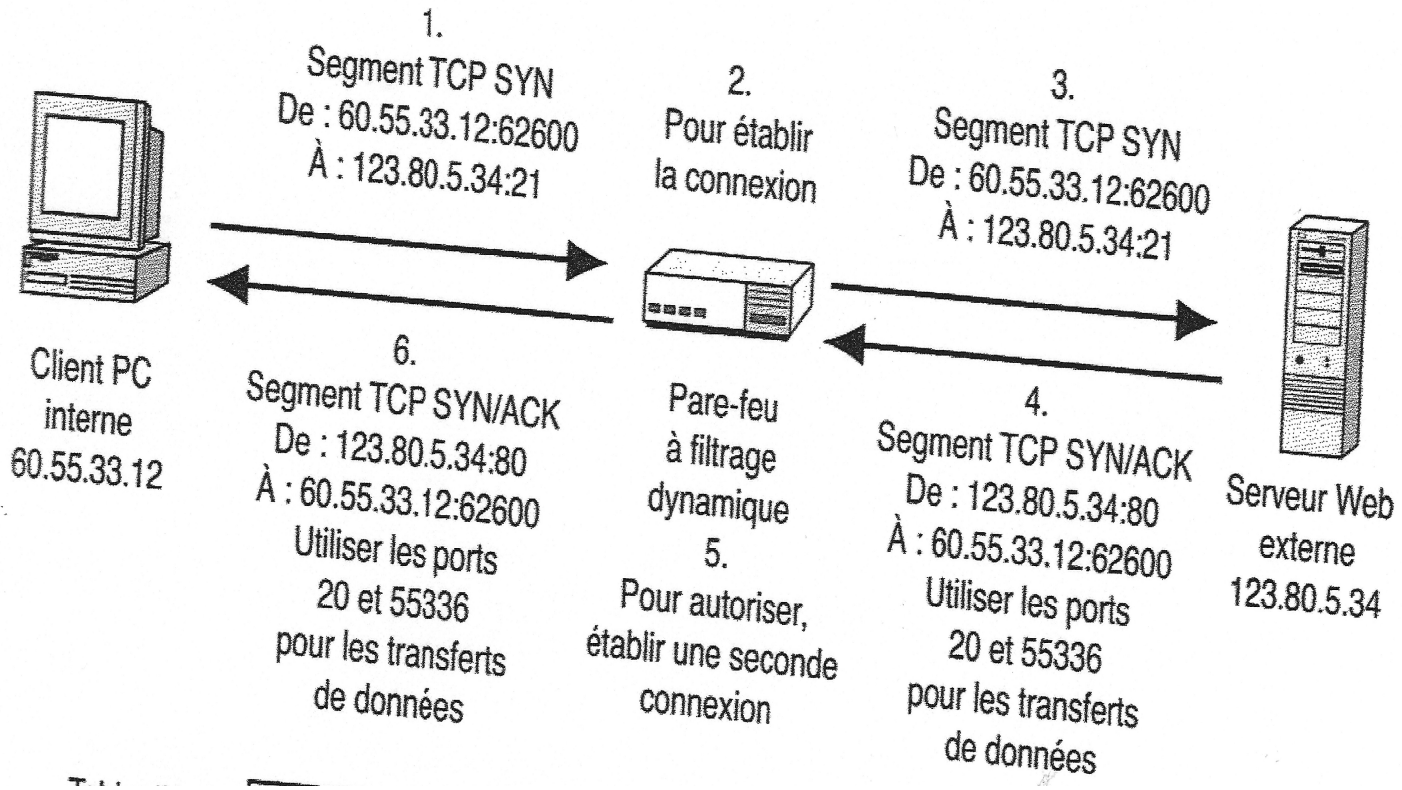
- Pas de prise en compte de l'état d'une session
- Faute rejeter un segment entrant `SYN/ACK` ?
- Difficile d'interpréter le trafic avec commutation de ports (cas de FTP par exemple).

Pare-feux à filtrage dynamique

Principe

- Le pare-feu maintiens une **table de connexions** ouvertes (TCP)
- Autorisation des passages de paquets pour les sessions ouvertes
- Extension du concept de session aux protocoles non-connectés (UDP, ICMP)
- Prise en compte de commutation de port dans certains cas (ex. ftp)

Pare-feux à filtrage dynamique



Type	Adresse IP interne	Numéro de port interne	Adresse IP externe	Numéro de port externe	État
TCP	60.55.33.12	62600	123.80.5.34	21	OK
TCP	60.55.33.12	55336	123.80.5.34	20	OK

Pare-feux: Translation d'adresses

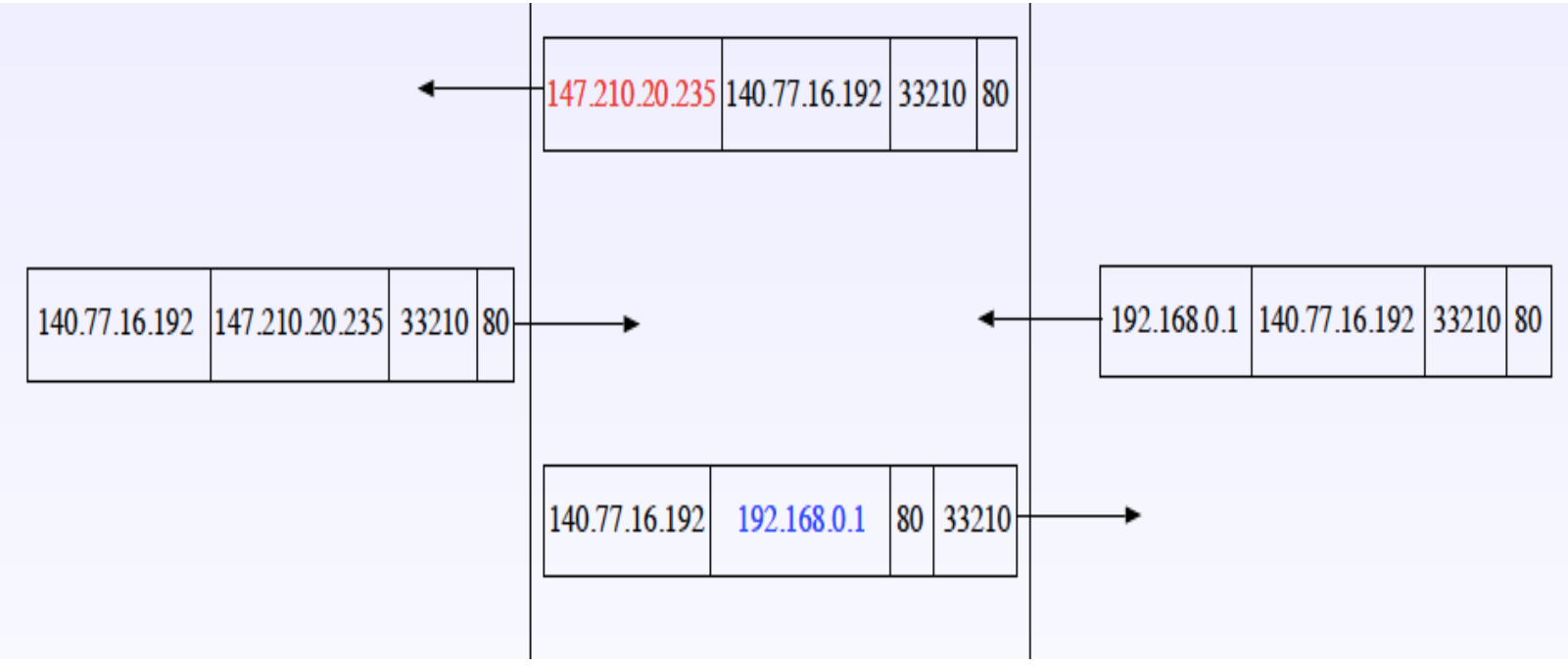
NAT : Intérêt

- Gérer la pénurie d'adresses au sein d'un réseau
- Masquer l'intérieur du réseau par rapport à l'extérieur.
  Changements d'adresses IP et des numéros de ports utilisés ← limiter l'intérêt d'écoute du trafic !
- Faciliter la modification de l'architecture du réseau interne

NAT : Types

- **Statique**: n @-publiques $\leftrightarrow$ n @ privées
- **Dynamique**: 1 @-publique $\leftrightarrow$ n @ privées

NAT STATIQUE



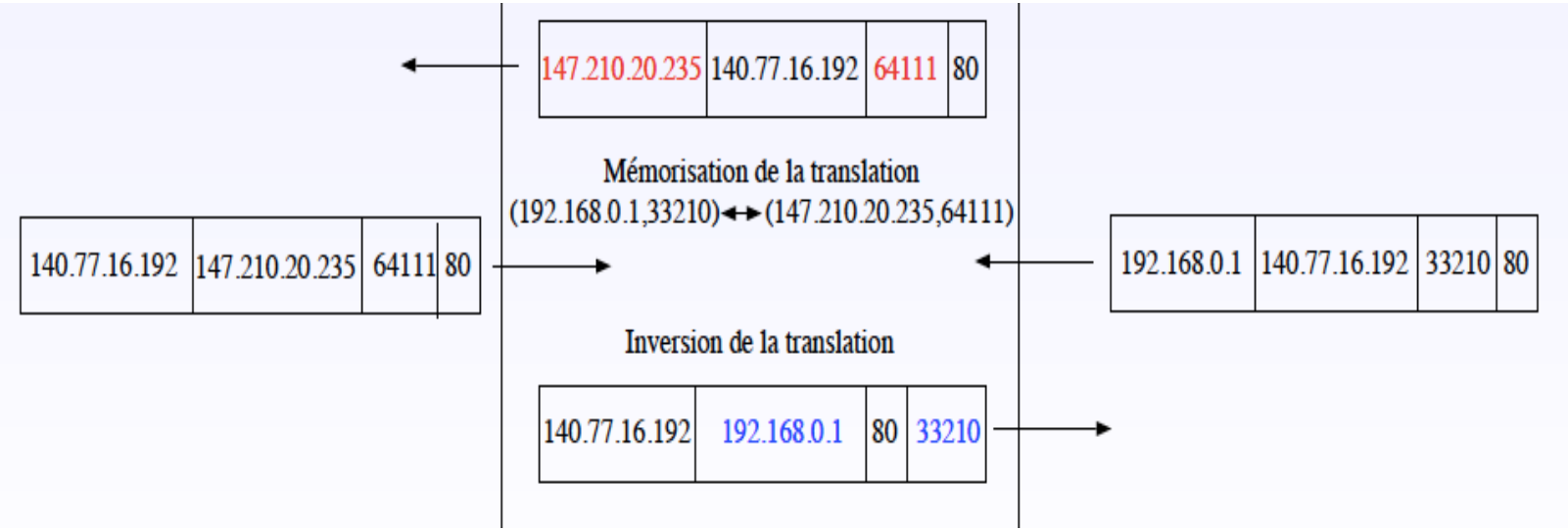
NAT : Advantages/inconvenients

+ Facilité de mise en œuvre

+ Sécurité de l'échange

- Non résolution du problème de pénurie d'adresses.

NAT DYNAMIQUE



NAT : Advantages/inconvenient

Nécessité d'implémenter une méthode spécifique aux protocoles non-connectés (ex/ identifiant ICMP).

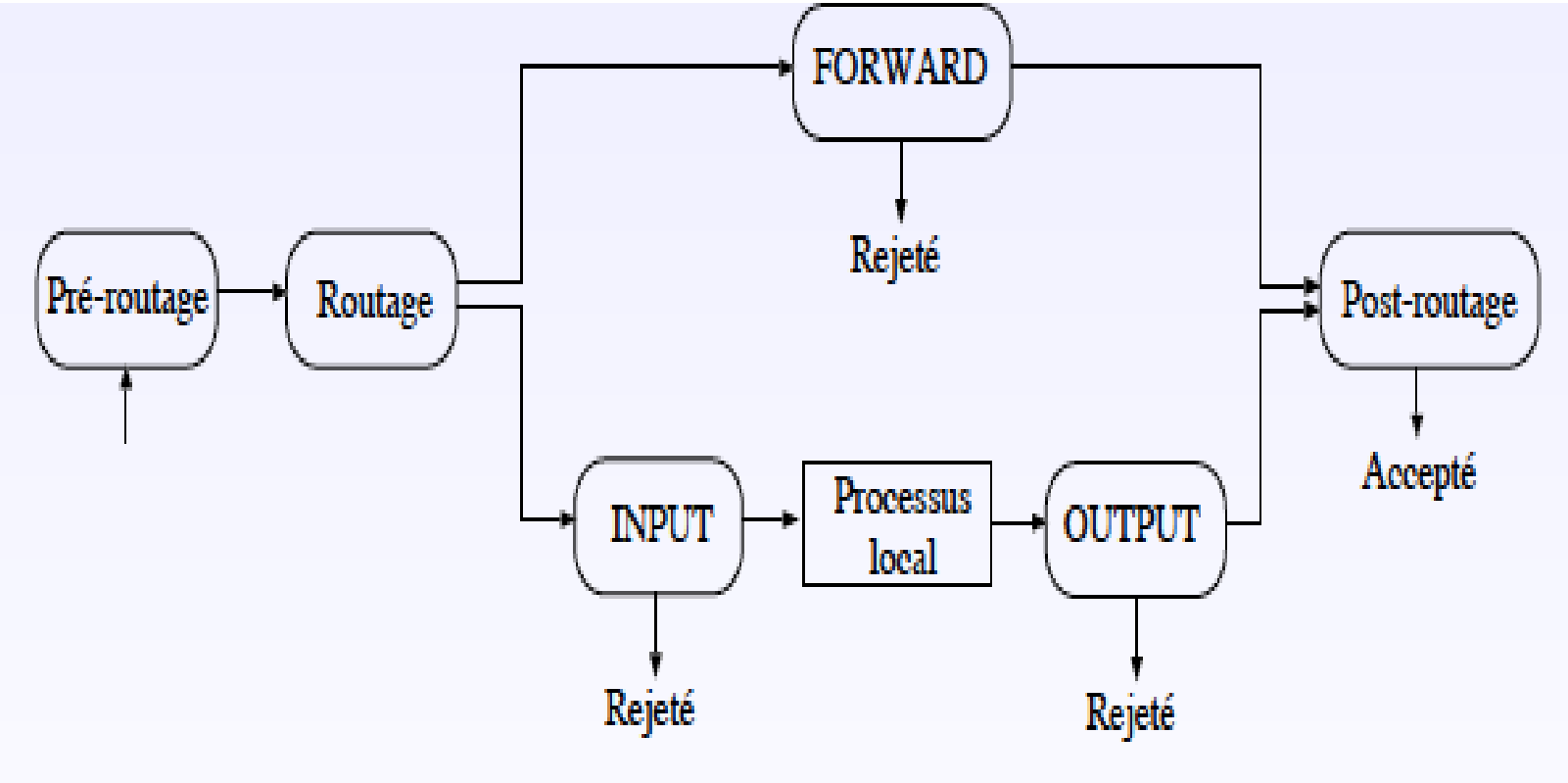
Nécessité de faire de la redirection de port pour rendre les machines internes joignables : Toutes les connexions entrantes sur un port donné sont redirigées vers une machine du réseau privé sur un port

IPTABLES : LOGICIEL DE FILTRAGE DE PAQUETS

- Module du noyau Linux réalisant le filtrage de paquets
- Filtrage statique (sans prise en compte de contexte de session) ou dynamique
- Fonctionnement : La transition d'un paquets dans différentes *chaines,* A chaque chaine on peut exercer un contrôle en appliquant des règles contenues dans des tables
- Différent types de tables :

  `filter` : règles de filtrage de paquets
  `nat` : règles de translation d'adresse
  `mangle` : règles de modification des entêtes.
  `raw` (ou conntrack)

IPTABLES



Tous les paquets émis par des processus locaux au routeur traversent la chaîne OUTPUT.

Circuit des paquets générés par la machine

1. raw OUTPUT
2. mangle OUTPUT
3. nat OUTPUT
4. filter OUTPUT
5. mangle POSTROUTING
6. nat POSTROUTING

Circuit des paquets en transit

1. raw PREROUTING
2. mangle PREROUTING
3. nat PREROUTING
4. mangle FORWARD
5. filter FORWARD
6. mangle POSTROUTING
7. nat POSTROUTING

COMMANDES IPTABLES

Syntaxe

```
iptables [-t table] command [match] [target/jump]
```

Principales Commandes

- **-L** : affichage
  ```
  iptables -t nat -L PREROUTING
  ```
- **-P**: Politique par défaut
  ```
  iptables -P INPUT DROP
  ```
- **-A** : ajout d'une règle
  ```
  iptables -A INPUT -s 193.48.143.10 -j ACCEPT
  ```
- **-D** : effacer une règle
  ```
  iptables -D INPUT -s 193.48.143.10 -j ACCEPT
  ```
- **-F** effacer toutes les règles d'une table
  ```
  iptables -F
  ```

IPTABLES : CRÉATION DE CHAINES

- **-N** : création d'une chaîne
- `iptables -N LOGACCEPT`
- `iptables -A LOGACCEPT -j LOG --log-prefix "LOGACCEPT : "`
- `iptables -A LOGACCEPT -j ACCEPT`

IPTABLES: EXEMPLES

- Politique par défaut, jeter tous les paquets entrants
- `iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j ACCEPT`
- Accepter tous les paquets destinés à l'adresse du routeur 192.168.1.1.
- `iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP -sport 1024:65535 -dport 80 -j ACCEPT`
- ?
- `iptables -A INPUT -p icmp -icmp-type echo-request -m limit -limit 1/s -i eth0 -j ACCEPT`
- Accepter un paquet `echo-request` par seconde

IPTABLES: NAT

- `iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -j MASQUERADE`
- Association entre toutes les adresses privées du sous-réseau 192.168.0.0/24 avec l'interface eth1.
- `iptables -t nat -A POSTROUTING -o eth2 -s 192.168.1.0/24 -j MASQUERADE`
- Association entre toutes les adresses privées du sous-réseau 192.168.1.0/24 avec l'interface eth2.
- `iptables -t nat -A PREROUTING -p tcp -i eth0 -d 140.77.13.2 -dport 80 -sport 1024:65535 -j DNAT -to 192.168.0.200:8080`
- Transférer les connexions sur le port 80 de l'adresse 140.77.13.2 sur la machine ayant l'adresse privée 192.168.0.200 sur le port 8080

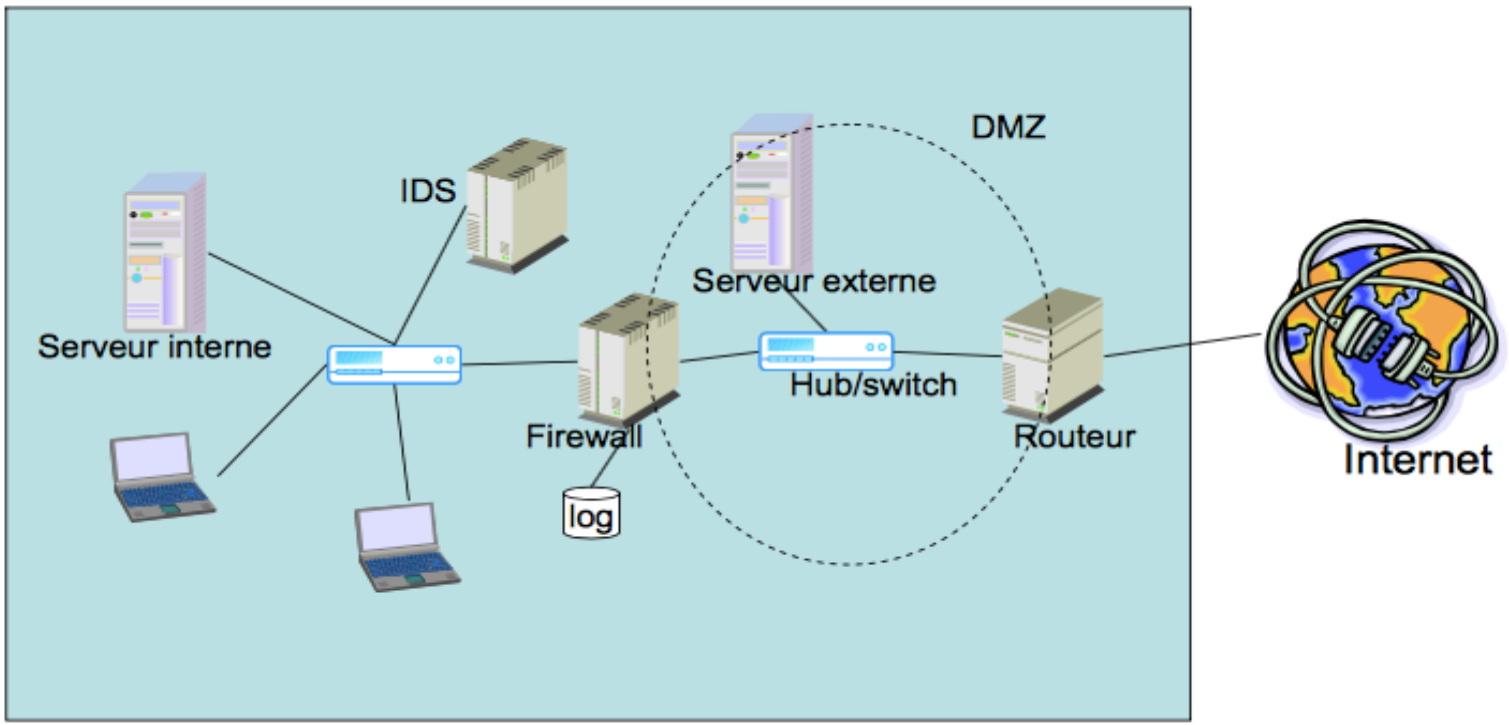
Filtrage dynamique

- Suivi des connexions disponible (conntrack)
- 4 états possibles d'une connexion : NEW, ESTABLISHED, RELATED, INVALID
- `iptables -A OUTPUT -o eth0 -m state -state ESTABLISHED,RELATED -j ACCEPT`
- Autoriser tous les paquets émis par le routeur concernant des connexions déjà établies.

DMZ

- Une zone démilitarisée (DMZ) est un sous-réseau se trouvant entre le réseau local et le réseau extérieur.
- Les connexions à la DMZ sont autorisées de n'importe où.
- Les connexions à partir de la DMZ ne sont autorisées que vers l'extérieur.
- intérêt : mettre en place des serveurs publiques : DNS, SMTP, WEB, etc

DMZ


DMZ
IDS
Serveur externe
Serveur interne
Hub/switch
Firewall
Routeur
log
Internet

IDS: Système de détection d'intrusions

Définition

Un équipement, logiciel ou matériel, qui automatise le processus d'analyse des événements d'un ordinateur/réseau pour y détecter des signes de problèmes de sécurité.

- un IDS détecte **mais n'empêche pas** les attaques
- Recherche de **signature d'attaque** : *motifs spécifiques* indiquant une intention suspecte.

IDS : CLASSIFICATION

Trois Critères

- **Architecture** :

  Centralisé
  Hiérarchique
  P2P

- **Mode de fonctionnement**

  Batch: analyse de *log* d'événements d'une manière périodiques ou programmé.
  Temps réel : analyse et détection en continue.

- **Type de signature**

  Granularité : Atomique ou composite
  Méthode de construction : par motif, par détection d'anomalie.

Signature atomique

- Caractérise un seul événement (paquet)
- Exemple : Quelle est la signature d'une attaque LAND ?
- Avantages : Simple à définir, et ne nécessite pas de beaucoup de ressources pour la détection.
- Inconvénients : ne détecte que les attaques simples et connues.

Signature composite

- Superviser un flux ou une suite d'événements.
- Fonctionnement : utiliser un ensemble de sondes pour générer des flux d'événements et rechercher des motifs dans les événements à *mettre en correspondance* avec une base de signatures d'attaques.
- Langage de description d'attaques: STATL (State-based Intrusion detection Language)

  Abstraction du détail de l'attaque
  Représentation d'attaques sous forme d'automates (états et transitions)
- Avantages: plus expressive qu'une signature atomique.
- Inconvénients : complexe à définir et à détecter.

Signature centrée motif

- Connaissance préalable des scénarios d'attaque, dont les occurrences sont détectées
- Disponibilité de base de signatures connues
- Avantages : faible taux de *faux négatifs*.
- Inconvénients : ne détecte que les attaques connues

SIGNATURE PAR ANOMALIES

- Principe : Apprendre un *profil* des comportements *normaux* et mesurer la *déviation* du trafic observé par rapport au profil appris.
- Mesure et techniques utilisés : Seuils de détection, mesures statistiques, . . . , etc.
- **Avantages** :

  Détecter les symptômes sans comprendre l'attaque.
  Alimenter une base de signature d'attaques
- **Inconvénients** :

  Génération de beaucoup de faux positives (fausses alarmes)
  Nécessite la disponibilité d'une base d'apprentissage fiable.

NIDS: IDS ORIENTÉ RÉSEAU

- Système d'écoute et d'analyse du trafic sur un réseau
- Souvent relié à un switch
- *Cas de beaucoup de IDS commerciaux*
- Fonctionnement : en trois phases

  Filtrage du traffic : éliminer les flux peu importants.
  Module de reconnaissance : signature, anomalie, etc.
  Module de réaction : Notification, Alerts, **trap SNMP**, action

NIDS: Avantages & Inconvénients

Avantages

- Supervision de tout un réseau
  pas besoin d'installer des IDS orientés hôtes sur chaque machine
- Déploiement sans perturbation de l'architecture réseau
- Indépendant des OS employés sur les différentes machines
- Détection en temps réel

Inconvénients

- Faible performances en cas de traffic intense
- Non opérationnel avec les flux chiffrés
- Difficulté à traiter les fragments IP.

HIDS: IDS orienté Hôte

- **Principe** : Analyse des logs des événements affectant la machine supervisée
- Source des données :

  System log
  Ecoute des ports de la machine → envoi d'alarme si un port est utilisé.
  Analyse de l'utilisation des ressources de la machine (base de registres, espace disque, mémoire, etc.)
- **Avantages** : Compatible flux crypté, pas d'ajout d'équipements, vérification de l'attaque
- **inconvénients** : OS dépendent, utilisation des ressources des machines, pas de détection en temps réel (analyse des log).

Évaluation d'un IDS

Table: Table de contingences (matrice de confusion)

Système / Réalité	Attaque	Non-attaque
Attaque	VP	FP
Non-attaque	FN	VN

Erreur du système : $E(Système) = \frac{FP+FN}{Attaque+Non-attaque}$

Évaluation d'un IDS : exemple

S_1 / Réalité	Attaque	Non-attaque
Attaque	40	10
Non-attaque	10	40

S_2 / Réalité	Attaque	Non-attaque
Attaque	30	5
Non-attaque	20	45

$$E(S_1) = \frac{10+10}{100} = 0.2$$
$$E(S_2) = \frac{5+20}{100} = 0.25$$

Prise en compte du coût de l'erreur

Table: Matrice de coût

Système / Réalité	Attaque	Non-attaque
Attaque	0	1
Non-attaque	10	0

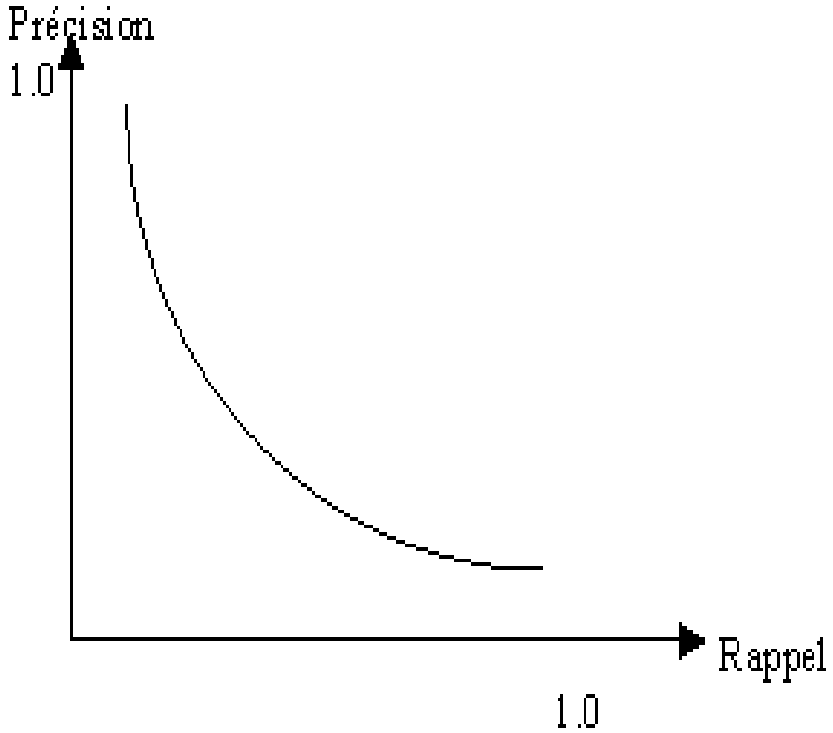
$$E(S_1) = \frac{10+100}{100} = 1.1$$
$$E(S_2) = \frac{5+200}{100} = 2.05$$

Critères d'évaluation

Trois Critères

- Précision : $P = \frac{VP}{VP+FP}$
- Rappel : $R = \frac{VP}{VP+FN}$
- F1 = $\frac{2 \times P \times R}{P+R}$

Courbe Précision / Rappel



COURBE ROC : OBJECTIFS

- Evaluation et comparaison des modèles indépendament des matrices de coput
- Opérationnel même dans le cas des distributions très déséquilibrées
- Outil graphique qui permet de visualiser les performances des modèles
- Outil permet de comparer différents modèles

Courbe ROC : principe

- Confusion Matrix

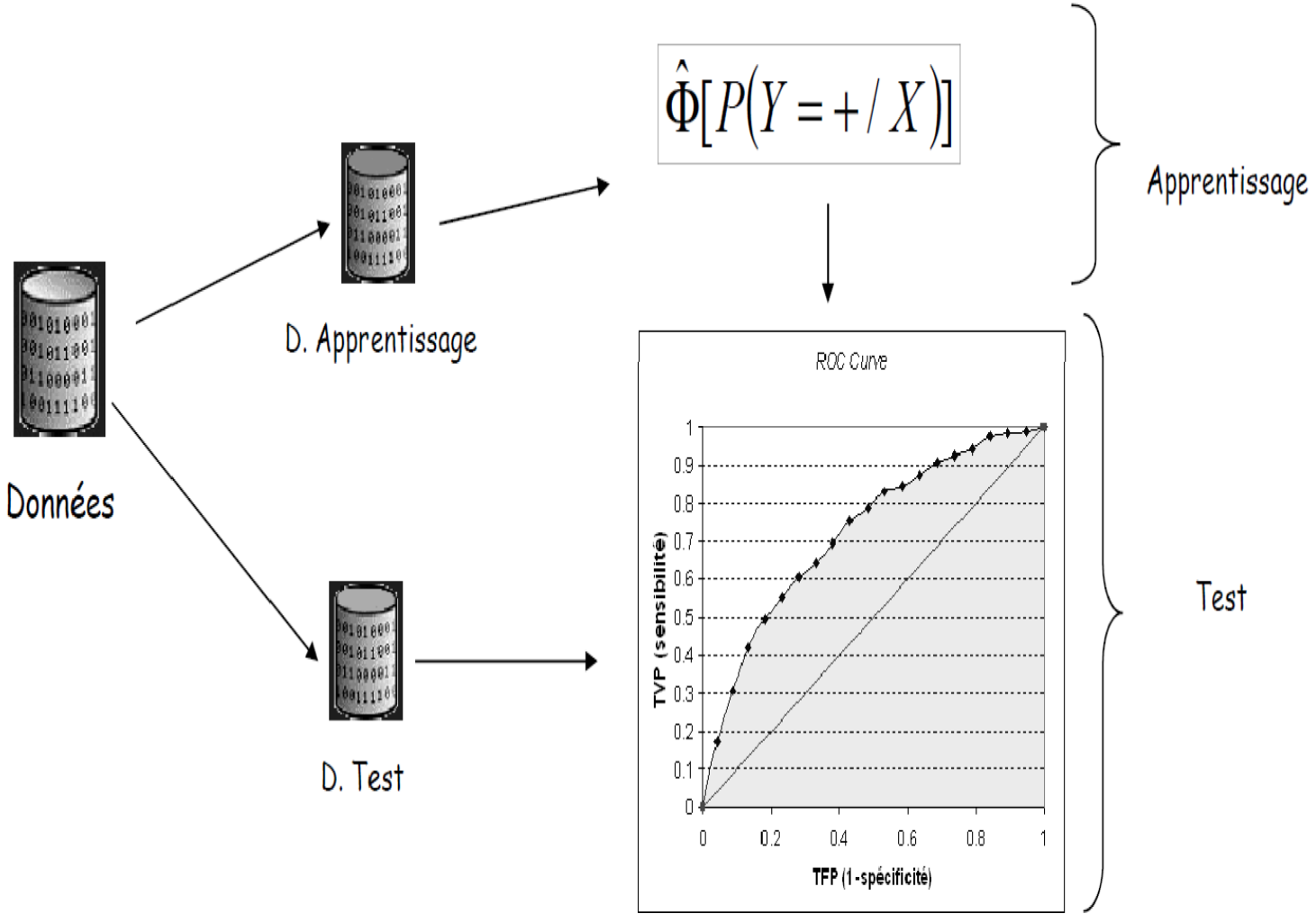
	+ Pred	- Pred
Real +	VP	FN
Real -	FP	VN

- TVP = Rappel = Sensibilité = VP/Positifs
- TFP = 1 − Spécificité= FP/Négatifs

Principe de la courbe ROC

- $P(Y = +/X) >= P(Y = -/X)$ équivaut à une règle d'affectation $P(Y = +/X) >= 0.5$ ($seuil = 0.5$)
- Cette règle d'affectation fournit une matrice de confusion MC1, et donc 2 indicateurs TVP1 et TFP1
- Si nous choisissons un autre seuil (0.6 par ex.), nous obtiendrons MC2 et donc TVP2 et TFP2 Etc.
- courbe ROC :faire varier le « seuil » de 1 à 0 et, pour chaque

Crédit M. Malek, Cyu



Crédit M. Malek, Cyu

Courbe ROC : principe

Classer les données selon un score décroissant

Individu	Score (+)	Classe
1	1	+
2	0.95	+
3	0.9	+
4	0.85	-
5	0.8	+
6	0.75	-
7	0.7	-
8	0.65	+
9	0.6	-
10	0.55	-
11	0.5	-
12	0.45	+
13	0.4	-
14	0.35	-
15	0.3	-
16	0.25	-
17	0.2	-
18	0.15	-
19	0.1	-
20	0.05	-

Positifs = 6
Négatifs = 14

Seuil = 1

	^positif	^négatif	Total
positf	1	5	6
négatif	0	14	14
Total	1	19	20

TVP = 1/6 = 0.2 ; TFP = 0/14 = 0

Seuil = 0.95

	^positif	^négatif	Total
positf	2	4	6
négatif	0	14	14
Total	2	18	20

TVP = 2/6 = 0.33 ; TFP = 0/14 = 0

Seuil = 0.9

	^positif	^négatif	Total
positf	3	3	6
négatif	0	14	14
Total	3	17	20

TVP = 3/6 = 0.5 ; TFP = 0/14 = 0

Seuil = 0.85

	^positif	^négatif	Total
positf	3	3	6
négatif	1	13	14
Total	4	16	20

TVP = 3/6 = 0.5 ; TFP = 1/14 = 0.07

Seuil = 0

	^positif	^négatif	Total
positf	6	0	6
négatif	14	0	14
Total	20	0	20

TVP = 6/6 = 1 ; TFP = 14/14 = 1

Crédit M. Malek, Cyu

Courbe ROC : principe

Construction de la courbe ROC (2/2)

Mettre en relation
TFP (abscisse) et TVP (ordonnée)

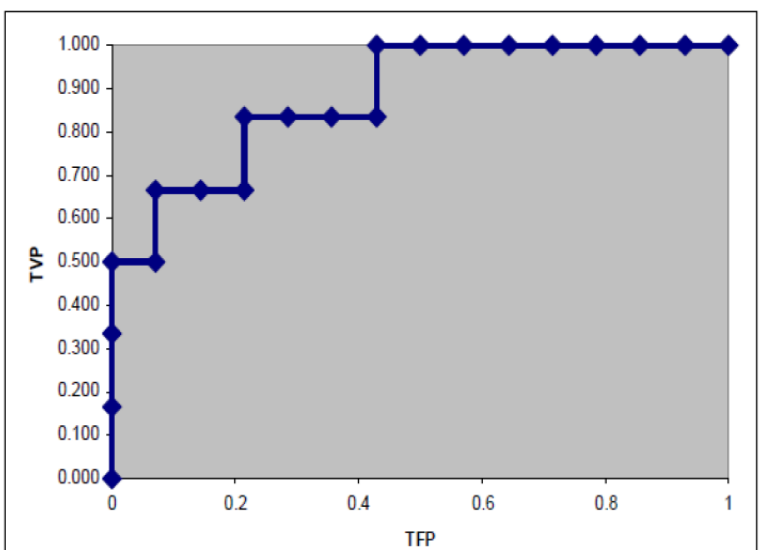
Individu	Score (+)	Classe	TFP	TVP
			0	0.000
1	1	+	0.000	0.167
2	0.95	+	0.000	0.333
3	0.9	+	0.000	0.500
4	0.85	-	0.071	0.500
5	0.8	+	0.071	0.667
6	0.75	-	0.143	0.667
7	0.7	-	0.214	0.667
8	0.65	+	0.214	0.833
9	0.6	-	0.286	0.833
10	0.55	-	0.357	0.833
11	0.5	-	0.429	0.833
12	0.45	+	0.429	1.000
13	0.4	-	0.500	1.000
14	0.35	-	0.571	1.000
15	0.3	-	0.643	1.000
16	0.25	-	0.714	1.000
17	0.2	-	0.786	1.000
18	0.15	-	0.857	1.000
19	0.1	-	0.929	1.000
20	0.05	-	1.000	1.000

Calcul pratique

TFP (i) = Nombre de négatifs parmi les « i » premiers / (nombre total des négatifs)

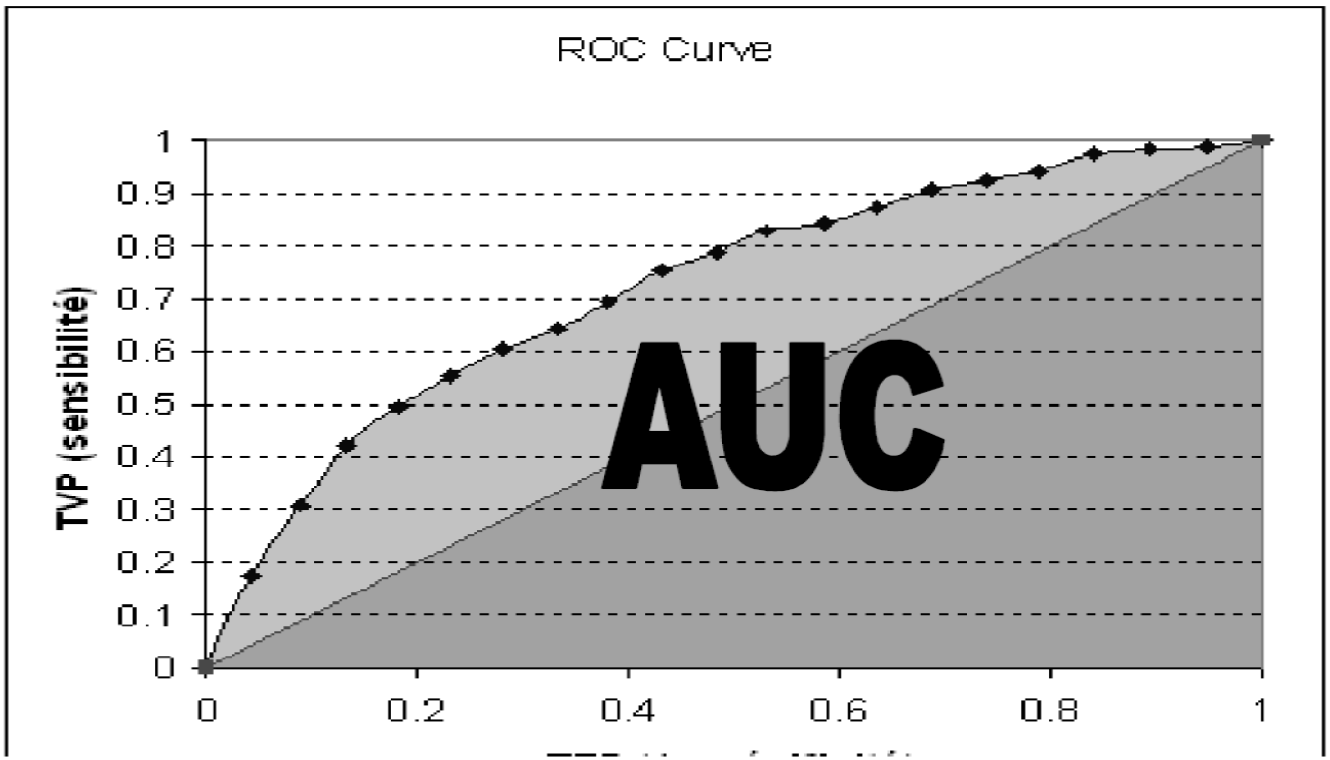
TVP (i) = Nombre de positifs parmi les « i » premiers / (nombre total des positifs)

Courbe ROC



Crédit M. Malek, Cyu

Courbe ROC : principe



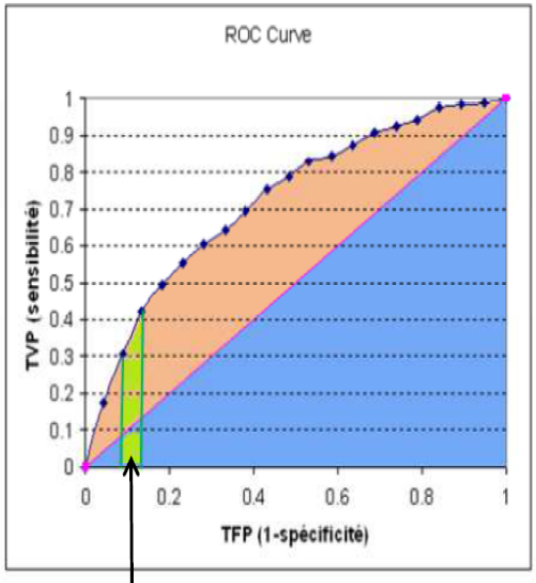
Probabilité pour que la fonction SCORE place un positif devant un négatif (dans le meilleur des cas AUC = 1)

Crédit M. Malek, Cyu

Courbe ROC :Calcul pratique 1

Dérivée directement de la définition : surface = intégrale

Individu	Score (+)	Classe	TFP	TVP	Largeur	Hauteur	Surface
			0	0.000			
1	1	+	0.000	0.167	0.000	0.083	0.000
2	0.95	+	0.000	0.333	0.000	0.250	0.000
3	0.9	+	0.000	0.500	0.000	0.417	0.000
4	0.85	-	0.071	0.500	0.071	0.500	0.036
5	0.8	+	0.071	0.667	0.000	0.583	0.000
6	0.75	-	0.143	0.667	0.071	0.667	0.048
7	0.7	-	0.214	0.667	0.071	0.667	0.048
8	0.65	+	0.214	0.833	0.000	0.750	0.000
9	0.6	-	0.286	0.833	0.071	0.833	0.060
10	0.55	-	0.357	0.833	0.071	0.833	0.060
11	0.5	-	0.429	0.833	0.071	0.833	0.060
12	0.45	+	0.429	1.000	0.000	0.917	0.000
13	0.4	-	0.500	1.000	0.071	1.000	0.071
14	0.35	-	0.571	1.000	0.071	1.000	0.071
15	0.3	-	0.643	1.000	0.071	1.000	0.071
16	0.25	-	0.714	1.000	0.071	1.000	0.071
17	0.2	-	0.786	1.000	0.071	1.000	0.071
18	0.15	-	0.857	1.000	0.071	1.000	0.071
19	0.1	-	0.929	1.000	0.071	1.000	0.071
20	0.05	-	1.000	1.000	0.071	1.000	0.071
						AUC	0.881



$$s_i = (TFP_i - TFP_{i-1}) \times \frac{TVP_i + TVP_{i-1}}{2}$$

Surface d'un trapèze

$$AUC = \sum s_i$$

Crédit M. Malek, Cyu

COURBE ROC : CALCUL PRATIQUE 2

Test de Mann-Whitney : montrer que deux distributions sont différentes (décalées).
Statistique basée sur les rangs.
Dans notre contexte, montrer que les « + » présentent en moyenne des scores plus élevés que les « - ».
On peut en dériver un test statistique.

Individu	Score (+)	Classe	Rangs	Rangs +
1	1	+	20	20
2	0.95	+	19	19
3	0.9	+	18	18
4	0.85	-	17	0
5	0.8	+	16	16
6	0.75	-	15	0
7	0.7	-	14	0
8	0.65	+	13	13
9	0.6	-	12	0
10	0.55	-	11	0
11	0.5	-	10	0
12	0.45	+	9	9
13	0.4	-	8	0
14	0.35	-	7	0
15	0.3	-	6	0
16	0.25	-	5	0
17	0.2	-	4	0
18	0.15	-	3	0
19	0.1	-	2	0
20	0.05	-	1	0

Somme (Rang +)	95
U+	74

AUC	0.881

Somme des rangs des « + »

$$S_+ = \sum_{i:y_i=+} r_i = 20+19+18+16+13+9 = 95$$

Statistique de Mann-Whitney

$$U_+ = S_+ - \frac{n_+(n_+ +1)}{2} = 95 - \frac{6\times 7}{2} = 74$$

AUC

$$AUC = \frac{U_+}{n_+ \times n_-} = \frac{74}{6\times 14} = 0.881$$

Crédit M. Malek, Cyu

COURBE ROC : CALCUL PRATIQUE 3

AUC – Calcul pratique 3 – Dénombrer les inversions

Trier les individus selon un score décroissant.
Pour chaque « + », compter le nombre de « - » qui le précède.
Dans notre contexte, on souhaite que les scores élevés soient attribués aux « + » en priorité c.-à-d. les « + » sont peu précédés de « - ».

Individu	Score (+)	Classe	Nb de "-" devant un "+"
1	1	+	0
2	0.95	+	0
3	0.9	+	0
4	0.85	-	0
5	0.8	+	1
6	0.75	-	0
7	0.7	-	0
8	0.65	+	3
9	0.6	-	0
10	0.55	-	0
11	0.5	-	0
12	0.45	+	6
13	0.4	-	0
14	0.35	-	0
15	0.3	-	0
16	0.25	-	0
17	0.2	-	0
18	0.15	-	0
19	0.1	-	0
20	0.05	-	0

Swaps : somme de l'indicateur ci-dessus

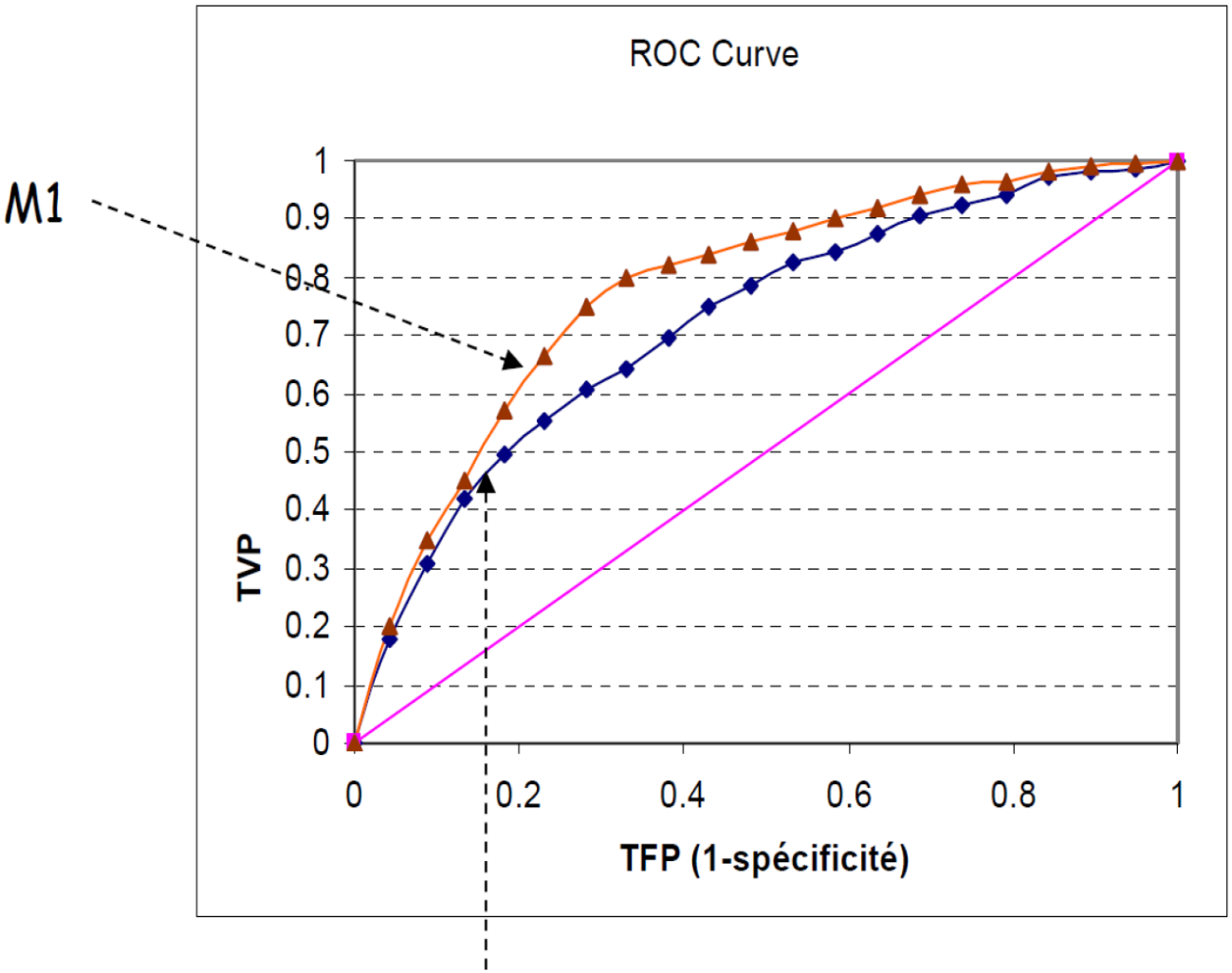
$$Swaps = \sum_{i:y_i=+} c_i = 0+0+0+1+3+6 = 10$$

AUC

$$AUC = 1 - \frac{Swaps}{n_+ \times n_-} = 1 - \frac{10}{6 \times 14} = 0.881$$

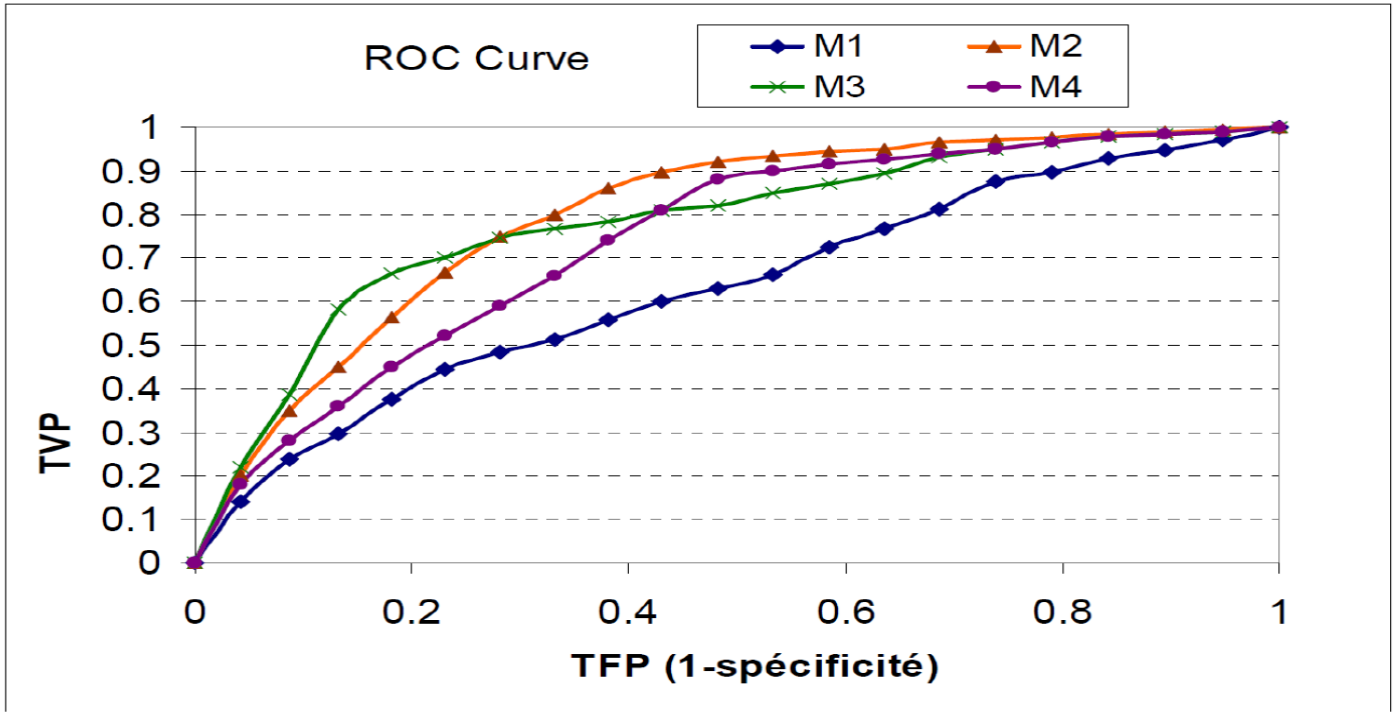
Crédit M. Malek, Cyu

COURBE ROC : COMPARISON



Crédit M. Malek, Cyu

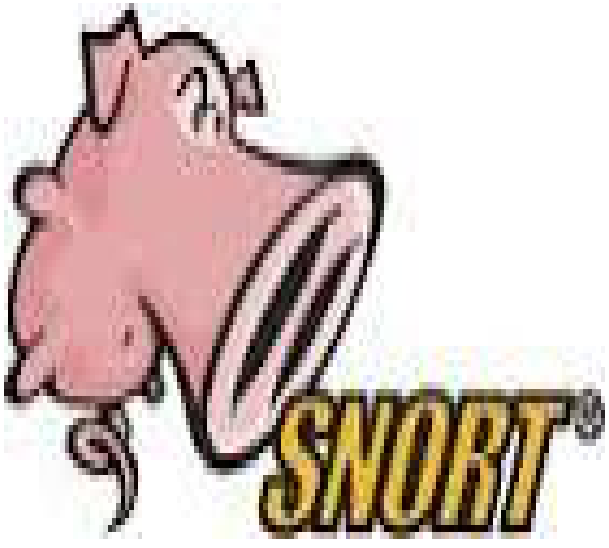
Courbe ROC : Enveloppe convexe



- formée par les courbes qui n'ont aucune courbe ≪ au-dessus ≫ d'elles.
- Exemple : enveloppe convexe est formée par les courbes de M3 et M2.

Crédit M. Malek, Cyu

Outil IDS



- Snort: logiciel libre compatible avec les principaux OS (linux, UNIX, MAC OS X, windows)
- `https://www.snort.org`
- Type: NIDS
- détection en temps réel

SNORT: FONCTIONS

- Opère au niveau 3 et 4 (IP, ICMP, UDP et TCP)
- Détection d'anomalies

  paquets ICMP invalides
- Pré-porcessuer HTTP
- Détection d'attaques de type dénis de service, saturation
- Langage de règles simple
- Règles paramétrables (utilisation de variables de substitution).
- Importation de règles

SNORT: LES RÈGLES

Syntaxe

```
action protocole @IP-src sport direction @IP-dest dport options
```

- Action : alert, log, pass
- protocole : tcp udp icmp.
- Options : **msg, flags, ttl, offset, seq, ack, minfrag, content, . . . ,**

  `minfrag` : permet de fixer un seuil de taille minimale pour un fragment

  `content` : permet de rechercher un contenu spécifique dans le champ donnée

SNORT: EXEMPLES DE RÈGLES

- `alert tcp any any -> 192.168.1.0/24 any (flags:SF; msg:"Scan SYN FIN");`
- `alert tcp any any -> 192.168.1.0/24 21 (content: "USER root"; msg: "Tentative d'accès au FTP pour l'utilisateur root";)`
- `log udp any any -> 192.168.1.0/24 any`
- `log 193.50.60.0/24 any <> 194.78.45.0/24 any`

SNORT: RÈGLES AVANCÉS

- Variables de substitution :

  `var Mynetwork 192.168.1.0/24`

- Inclusion de fichiers de règles externes

  `include:<fichier>`

- Sites publiques pour règles snort.

  voir `www.snort.org`

AUTHENTIFICATION

- **Définition** : Vérification de l'identité d'une *entité* afin de lui autoriser l'accès à des ressources.
- Entités à authentifier: utilisateurs, processus, machines
- Types d'authentification :

  Simple : Exiger un seul élément d'authentification (ex. mot de passe)

  Forte : Exiger au moins deux éléments (ex. carte à puce).

  Mutuelle : exiger une authentification dans le deux sens.

Robustesse des mots de passe

- **Robustesse** = Nombre d'essaies nécessaires pour retrouver le mot par force brute
- On estime la robustesse par l'**entropie** (E) du mot de passe
- Soit $\mathcal{A}$ l'alphabet utilisé. $N = |A|$ le nombre d'éléments de $\mathcal{A}$. $l(m)$ la longueur du mot de passe m. On a

$$E(m) = log_2(N^{l(m)}) = l(m) \times log_2(N)$$

- Exercice : Quelle est la longueur minimale d'un mot de passe composé uniquement de chiffres pour que sa robustesse soit de l'ordre de 2^{64} ?

Mots de passe : Règles classiques

- utiliser un alphabet étendu : caractères alphabétique majuscules et minuscules + chiffres + caractères spéciaux
- Eviter les répétitions et les suites bien connus
- Eviter d'utiliser des informations publiques
- Utiliser un générateur de nombres aléatoires
- `dd if=/dev/random bs =1 count =8 2>/dev/null | xxd -ps`

Cryptographie

Vocabulaires

- **Cryptographie** : science de secret
- **Message en clair** : message originale
- **Chiffrement** : transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement
- **Cryptogramme** : message chiffré

Cryptographie : services

- Confidentialité
- Authentification de l'origine des données
- Intégrité
- Non-répudiation
- Authenticité = Authentification + Intégrité

CRYPTOGRAPHIE: PRINCIPES

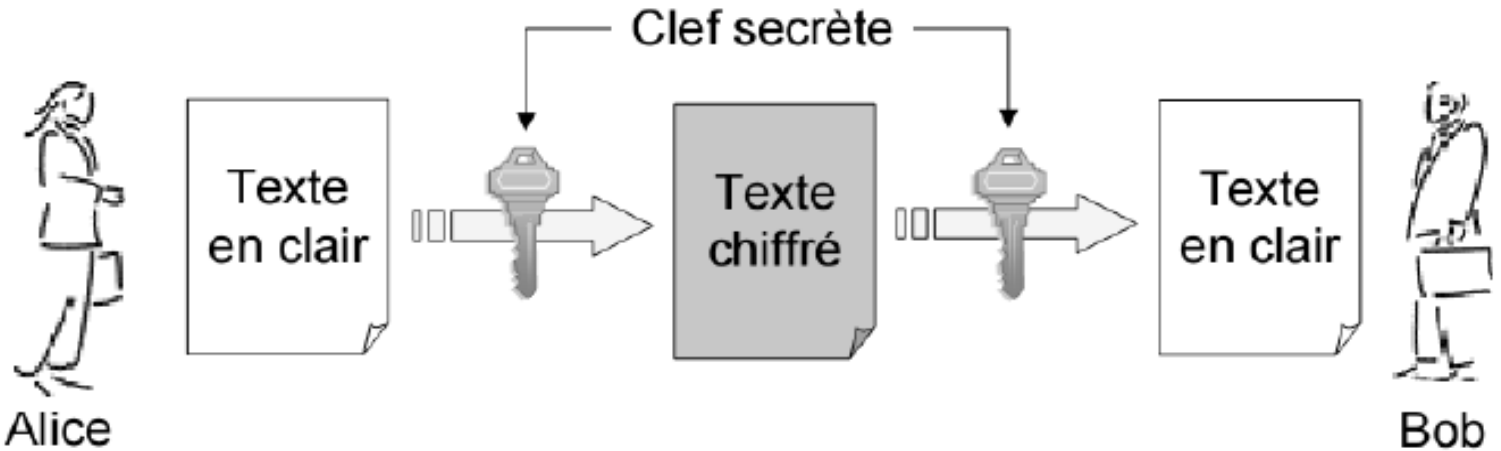
- Deux grandes approches :

  Cryptage symétrique : utilisation d'un clé de cryptage partagé

  Cryptage asymétrique : Codage avec deux clés : une privée et l'autre publique.

- **Principe de Kerckhoffs**: (*Maxime de Shanon*) : L'ennemi connaît l'algorithme utilisé, donc le secret repose sur le secret de clé et non sur le secret de l'algorithme.

CHIFFREMENT SYMÉTRIQUE

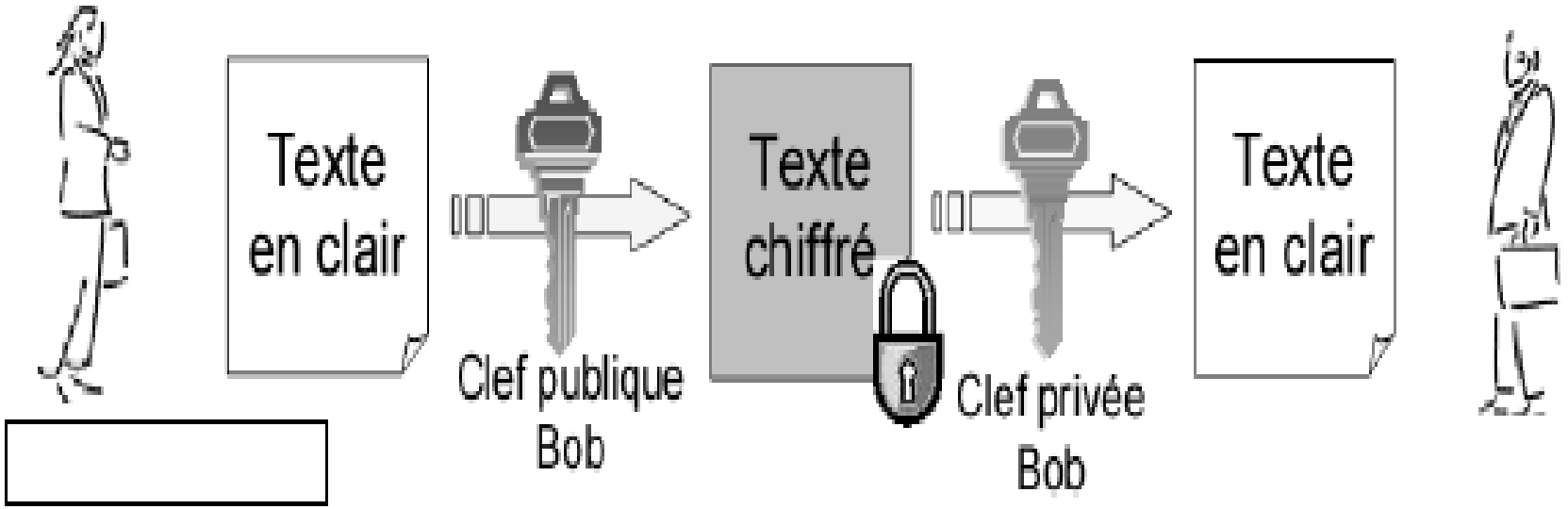


Problème

Comment communiquer la clé ?

Chiffrement asymétrique

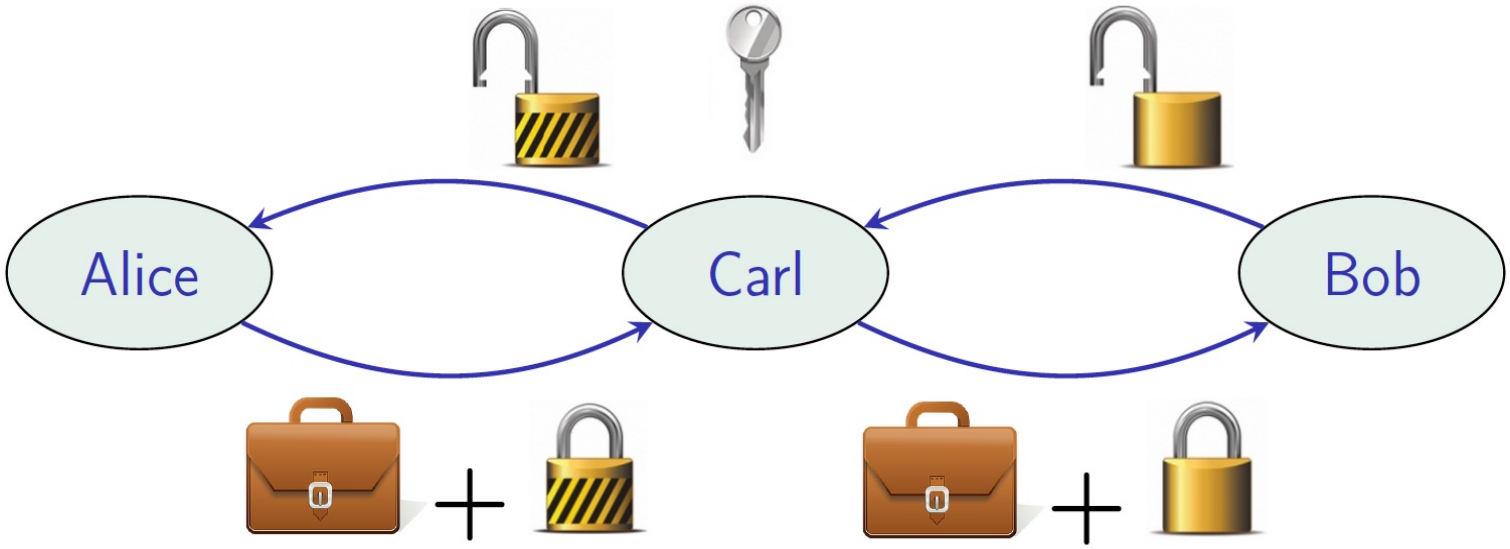
Confidentialité



Problème

Attaque : Man in the Middle !

CHIFFREMENT ASYMÉTRIQUE : ATTAQUE



Crédit Y. Legrandgérard - IRIF

Solution

Alice doit authentifier la clé de Bob : utilisation de **certificat**

CERTIFICAT

- Un certificat = un document numérique **signé** contenant une **clé publique** et l'identification du porteur de cette clé
- **Signature** par :
  - **autorité de certification**
  - membre d'un **réseau de confiance**

AUTORITÉ DE CERTIFICATION : EXEMPLES

Structure d'un certificat

Données	`Version:`	Version du type de certificat X.509
	`Serial number:`	Numéro de série au sein de l'AC
	`Signature algorithm:`	Algorithme de signature utilisé
	`Issuer:`	Identité de l'AC (*Distinguished Name*) qui a émis ce certificat

	`Validity`
	` Not before: xx`
	` Not after : xx`
		Période de validité du certificat : dates de début et de fin

	`Subject:`	Identité du propriétaire (*Distinguished Name*) du certificat
	`Subject Public Key Info:` ` Public Key Algorithm:`	Informations sur la clé publique et les paramètres de celle-ci

	`X509v3 extensions:`
	` Extension name:`
	`  Extension value`
	` ...`
		Extensions optionnelles propres à la version 3

Signature	`Signature algorithm:`	Algorithme utilisé pour la signature
	`Signature`	Signature du certificat

Crédit Y. Legrandgérard - IRIF

Autorité de certification

- Une AC possède son propre couple (clé privée, clé publique) associé à un certificat qui peut être, soit **auto-signé** ou signé par une autre AC.
- L'AC est garante des informations contenues dans les certificats qu?elle délivre.
- N'importe qui peut se déclarer AC !
- La confiance accordée à une AC est héritée par toutes les ACs filles
- **Confiance croisée** : Deux ACs peuvent s'entendre afin de signer chacune le certificat de l?autre.

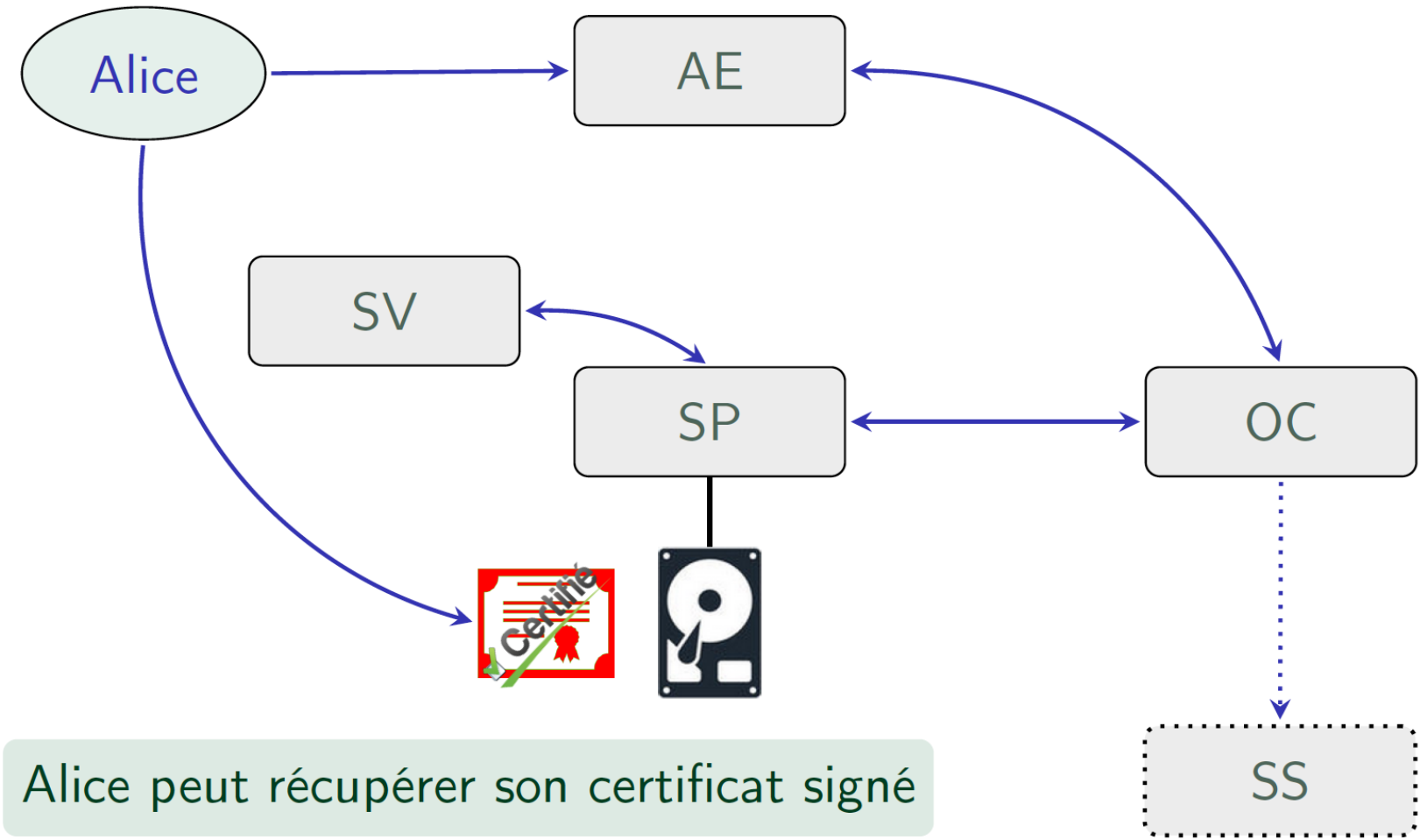
Infrastructure de Gestion de Clés

- IGC : Infrastructure de Gestion de Clés
- PKI : Public Key Infrastructure
- Services :
  - Enregistrement de utilisateurs
  - Génération et renouvellement des certificats
  - Révocation des certificats
  - Publication des certificats et des révocations
  - Service de séquestre et de recouvrement des clés privées ! (rare à mettre en place)

Composition d'un IGC

- Autorité d?Enregistrement (AE) : reçoit et traite les demandes de création, renouvellement et révocation de certificats. Elle doit notamment s'assurer de l'identité des demandeurs.
- Opérateur de Certification (OC) : effectue toutes les opérations demandées par l'AC nécessitant la clé privée de celle-ci. Il n?est en principe **pas connecté** au réseau.
- Service de Publication (SP) : met à disposition de tous, via un annuaire , les certificats issus de l'IGC, le certificat de l'AC et éventuellement les listes de révocation (CRL).
- Service de Validation (SV) : permet à tout utilisateur de vérifier la validité d'un certificat
- Service de Séquestre (SS) : stocke les couples (clé privée, clé publique) des certificats produits !!

Circuit de demande de certificat



Crédit Y. Legrandgérard - IRIF

SIGNATURE DE CERTIFICAT

- Utilisation de fonction de **hachage** (ou condensation)
- Une fonction de hachage est une fonction à **sens unique** qui prend en entrée des données de longueur quelconque et rend une valeur de taille fixe
- Une fonction à sens unique est facile à calculer mais difficilement inversible
- Soit $\mathcal{A}$ un alphabet limité. $A^* = \cup_k A^K$. Une fonction d'hachage est

$$f : A^* \rightarrow \{0,1\}^n$$

- $f(x)$ est appelé l'empreinte (ou aussi : condensé, condensat, haché, hash) de x.

Fonctions d'hachage : applications

- Stockage des mots de passe.
- Signature
- Garantir l'intégrité des données transmises
- ...

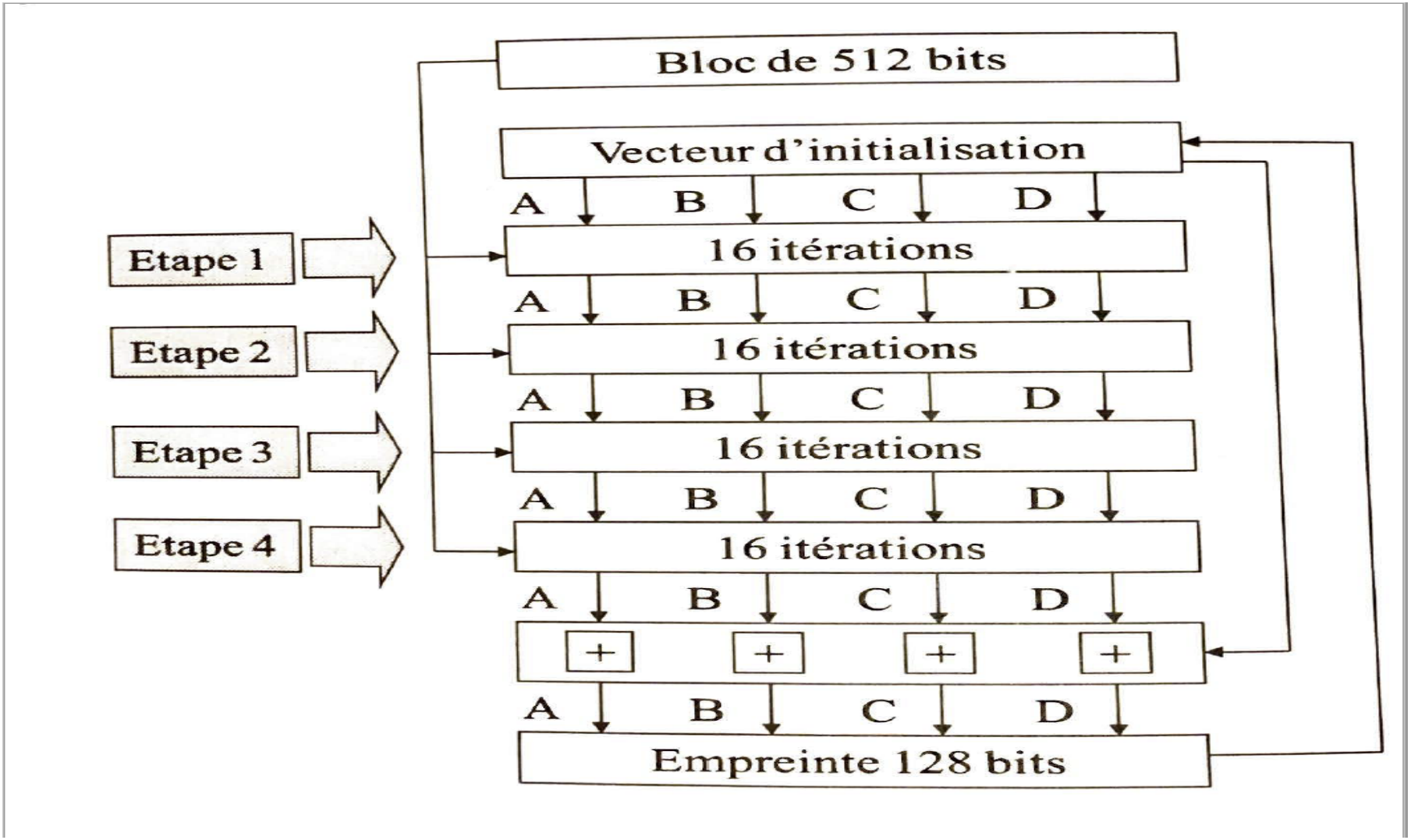
EXEMPLE : L'ALGORITHME MD5

- MD5 (Message Digest) 5 étapes.
- Calcule une empreinte de 128 bits
- Utilisation de 4 registres de 32 bits : A, B, C, D
- Valeurs initiales des registres :

  A : 67452301
  B : EFCDAB89
  C : 98BADCFE
  D : 10326476

- Donnée divisé en bloc de 512 bits : Les données sont toujours complétée pour avoir un taille égale 448 modulo 512 (par une suite de 0 se terminant par 1. Puis ajouter un champs de 64 bits codant la longuer des données

EXEMPLE : L'ALGORITHME MD5



EXEMPLE : L'ALGORITHME MD5

- Étape 1 : `F(X,Y,Z) = (X ET Y) OU ((NON X) ET Z)`
- Étape 2 : `F(X,Y,Z) = (X ET Y) OU (Y ET (NON Z)))`
- Étape 3 : `F(X,Y,Z) = X XOR Y XOR Z`
- Étape 4 : `F(X,Y,Z) = Y XOR (X OU (NON Z))`

Fonction d'hachage : autres algorithmes

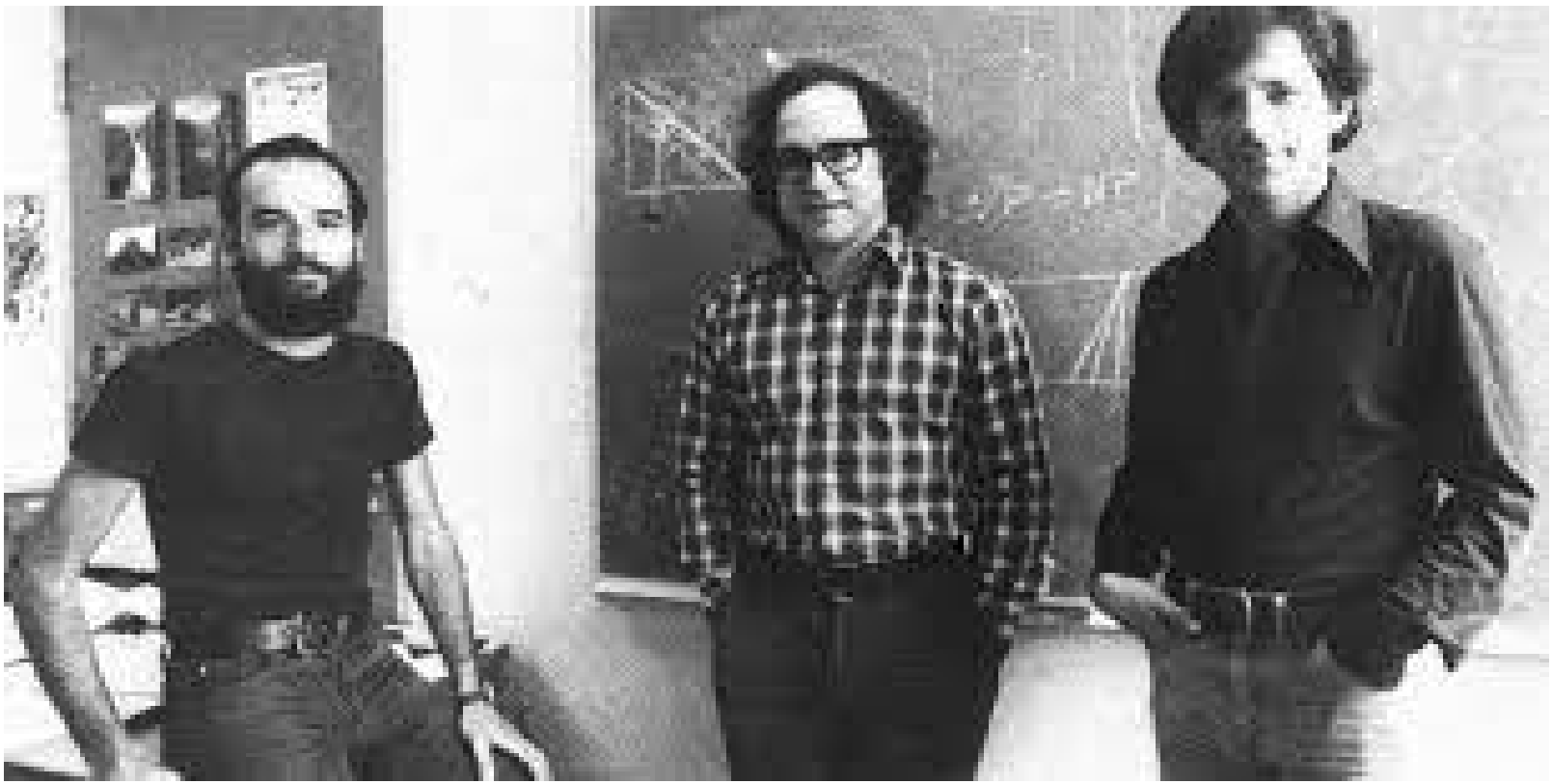
- SHA : Secure Hash Algorithm
- SHA-1 : empreinte de 160 bits. Encore très utilisé
- SHA-2 : empreinte de 224, 256, 384 ou 512 bits
- SHA-3 : empreinte de 224, 256, 384, 512 ou arbitraire bits. Les fonctions de hachage précédentes, étant construites à partir des mêmes heuristiques, sont sensibles aux mêmes attaques. Il a donc été decidé (NIST) de fournir une alternative fondée sur des principes complètement différents. C?est SHA-3 normalisée en 2015

Fonction d'hachage : attaque

- Est-ce qu'une fonction d'hachage peut être injective ?
-
- Quelle est la probabilité d'avoir $x_i, x_j \in A^*, x_i \neq x_j : f(x_i) = f(x_j)$?
-
- Indice : Calculer combien de personnes faut il réunir pour avoir plus de 50% de chance d'avoir au moins deux personnes nées le même jour de l'année !

CHIFFREMENT ASYMÉTRIQUE : L'EXEMPLE DE RSA

1978 : Par Rivest, Shamir & Adleman



RSA

- Alice veut recevoir un message d?une autre personne Bob.
- Le crypto-système RSA comprend 3 étapes :
  - Choix de la clé et sa publication par Alice
  - Chiffrement du message par Bob et envoi
  - Déchiffrement du message par Alice par clé privée.

RSA : Choix de la clé

- Alice génère deux très grands entiers naturels **premiers** p et q.
- $p = 59, q = 71$
- Elle calcule $n = p \times q$ et $w = (p-1) \times (q-1)$
- $n = 4189, w = 4060$
- Elle choisit e premier avec w
- $e = 671$
- En appliquant le théorème de Bachet-Bézout : e est premier avec w donc il existe deux entiers d, k : $(e \times d) + (k \times w) = 1$. On a $d \times e = 1 \bmod w$
- $d = 1791$
- Elle envoie la clé publique (n, e) et garde la clé privée (n, d)

RSA : Chiffrement de message

- Bob veut envoyer $M = 010100100101001101000001$
- M est découpé en bloc de $k$bits : $2^K < n < 2K + 1$
- $K = 12$
- Deux blocs à chiffrer :
  $010100100101 = (1317)_{10}, 0011010000001 = (833)_{10}$
- Bob envoie $b^e \bmod n$
- $1317^{671} \bmod 4189 = 3530$
- $833^{671} \bmod 4189 = 3050$

RSA : Déchiffrement

- Alice reçoit c et calcule $c^d \bmod n$
- $3530^{1791} \bmod 4189 = 1317$
- $3050^{1791} \bmod 4189 = 833$

RSA : Principe

- Il est facile de multiplier deux grands nombres premiers
- Il est très difficile de factoriser un très grand nombre.
- La factorisation en nombres premiers croit exponentiellement avec la longueur de n
- Les experts estiment des clés de 4096 bits sont sures, mais pas de garantie !

RSA : REMAQRUES

- RSA comme les autres algorithme asymétriques sont gourmands en temps de clacul.
- souvent utilisé pour transporter une clé secret de chiffrement symétrique.

CHIFFREMENT SYMÉTRIQUE : ÉCHANGE DE LA CLÉ

- Approche 1 : échanger la clé en utilisant un algorithme de chiffrement asymétrique
- Approche 2 : Génération de clé secrète : Mécanisme Diffie-Hellman :

  Alice et Bon choisissent un nombre premier p et un générateur g modulo p
  Alice choisit un nombre secret a : $1 \leq a \leq p-1$
  Bob choisit un nombre secret b : $1 \leq b \leq p-1$
  Alice envoie à Bob $A = g^a[modp]$
  Bob envoie à Bob $B = g^b[modp]$
  Clé secrète : $(B[modp])^a = B^a[modp] = g^{ba}[modp] = (A[modp])^b$