Sécurité Informatique
Introduction à la sécurité

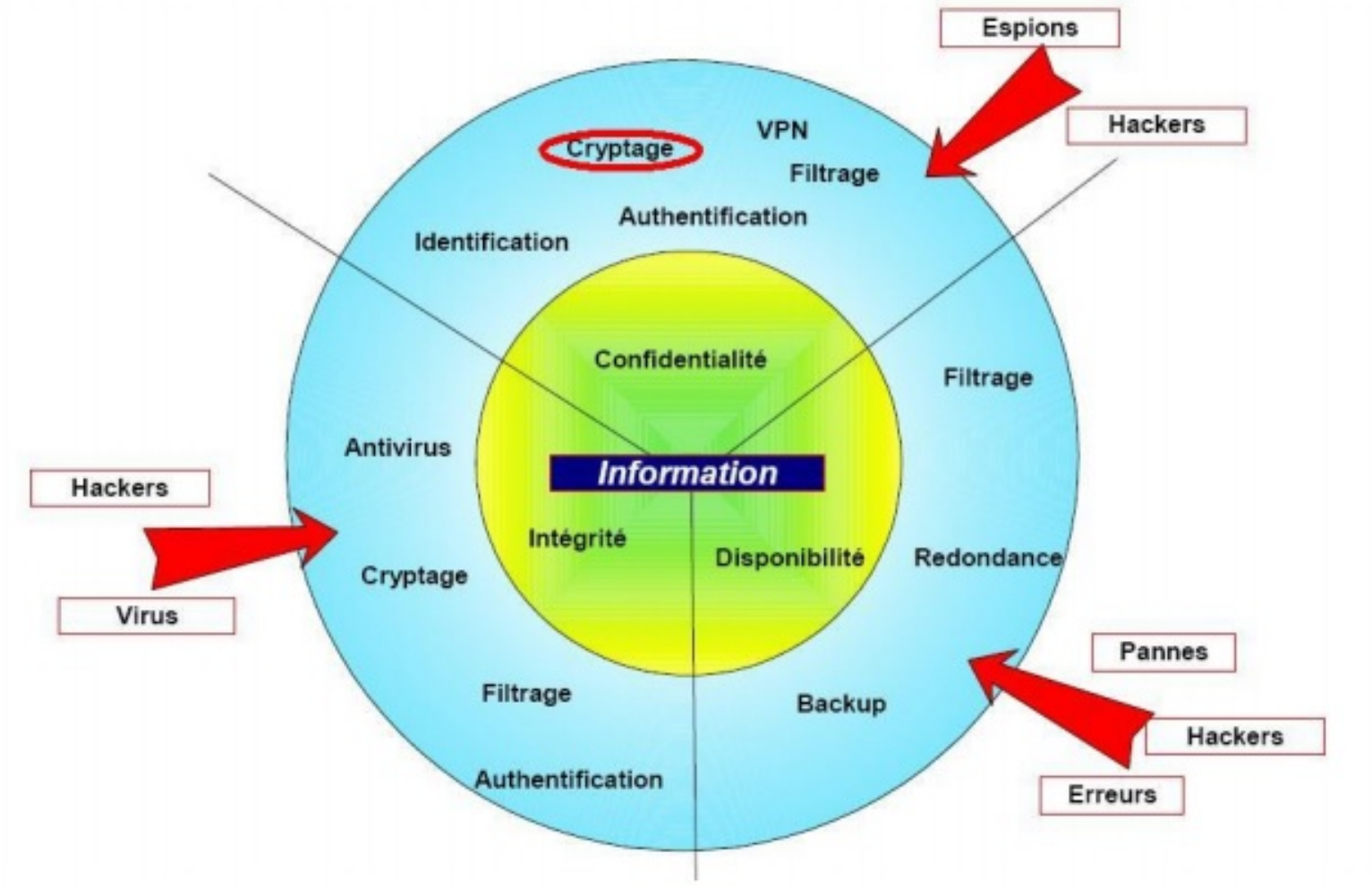
October 17, 2018

Houcemeddine HERMASSI
houcemeddine.hermassi@enit.rnu.tn

École Nationale d'Ingénieurs de Carthage ENI-CARTHAGE
Université Carthage
Tunisie

Plan de cour

Introduction
Objectctifs de la sécurité



Introduction
Un peu d'histoire

Kevin Mitnik

- Le plus médiatisé des pirates : 3 livres et un film
- il a commencé par pirater les réseaux téléphoniques
- A attaqué les machines d'un "supercomputing" center à San Diego
- Il a fait 5 ans de prison et 2 ans d'interdiction de toucher des ordinateurs
- La force de Mitnik était l'ingénierie sociale
- Maintenant il est consultant de sécurité informatique

Evènements importants

- Fevrier 2000 : plusieurs sites sont hors services (ebay, cnn, amazon, microsoft) pendant des heures, ils ont été inondés par un trafic allant jusqu'à 1 Gbps provenant de plusieurs adresses
- Le 16 fevrier un dénommé "Mafiaboy" est suspecté d'avoir lancé ces attaques, Il a été arreté en canada, il avait 15 ans, il a été condamné à 8 mois de détention, A l'aide d'un prog automatique ; Mafiaboy a compromis 75 ordinateurs en exploitant une faille dans leurs serveurs FTP, Il a installé un prog d'attaques distribué sur ces machines.
- Melissa ne vous aime pas : premier virus planétaire instantanné, c'est un document word contenant une Macro pour envoyer le document à 50 adresses du carnet d'adresses, son auteur a été arrété dans la semaine
- Depuis "I love you", "kournikova", "sircam" ont pris la relève.

Attaque

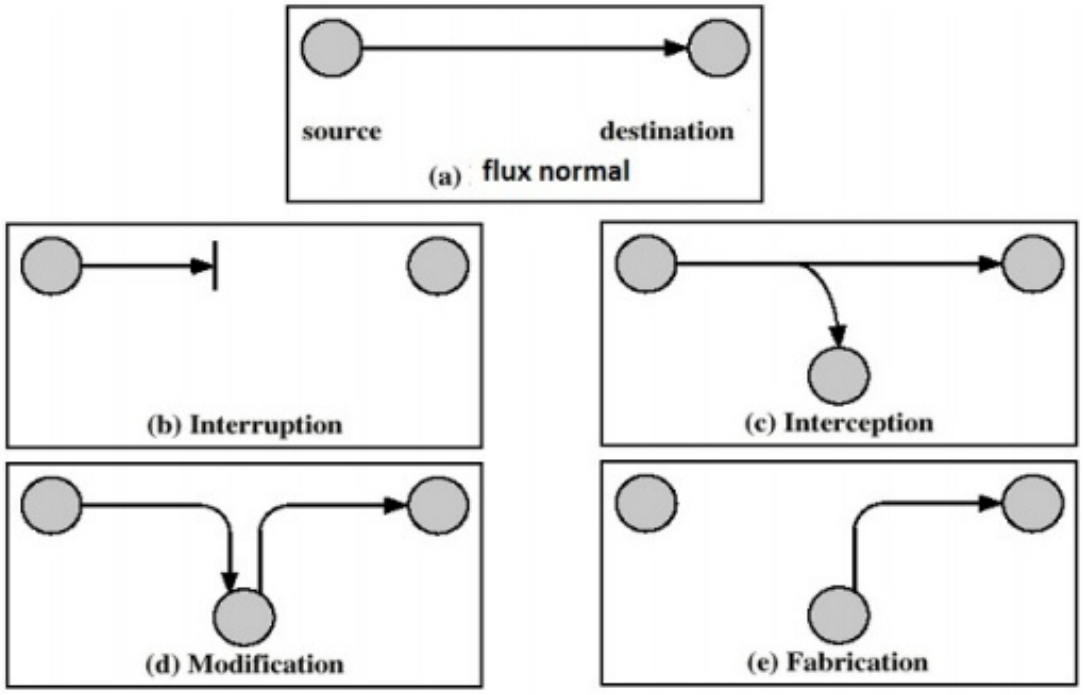
Toute action qui compromet la sécurité de l'information

Mécanisme de sécurité

Un mécanisme qui est conçu pour détecter, prévenir, ou se remettre d'une attaque de sécurité.

Service de sécurité

Un service qui améliore la sécurité des systèmes de traitement de données et les transferts d'information. Un service de sécurité fait usage d'un ou plusieurs mécanismes de sécurité



Impact

- **Interruption** : une attaque sur la disponibilité
- **Interception** : une attaque sur la confidentialité
- **Modification** : une attaque sur l'intégrité
- **Fabrication** : une attaque sur l'authenticité

Attaques passives

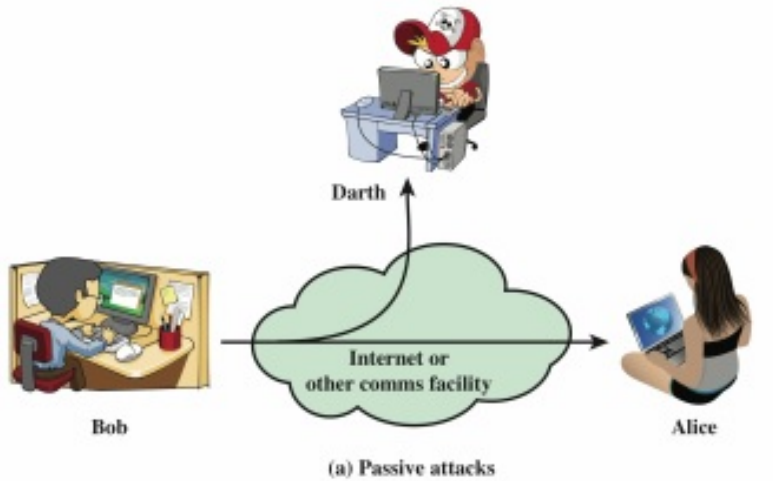
- Tente d'apprendre ou d'utiliser l'information du système, mais **n'affecte pas les ressources du système**
- Relativement difficile à détecter, mais plus facile à prévenir

Lecture du message & Analyse du trafic

Attaques actives

- Tente de **modifier** les ressources du système ou **d'affecter** leur fonctionnement
- Relativement difficile à éviter, mais plus facile à détecter

Mascarade, Replay, Modification du message et DoS

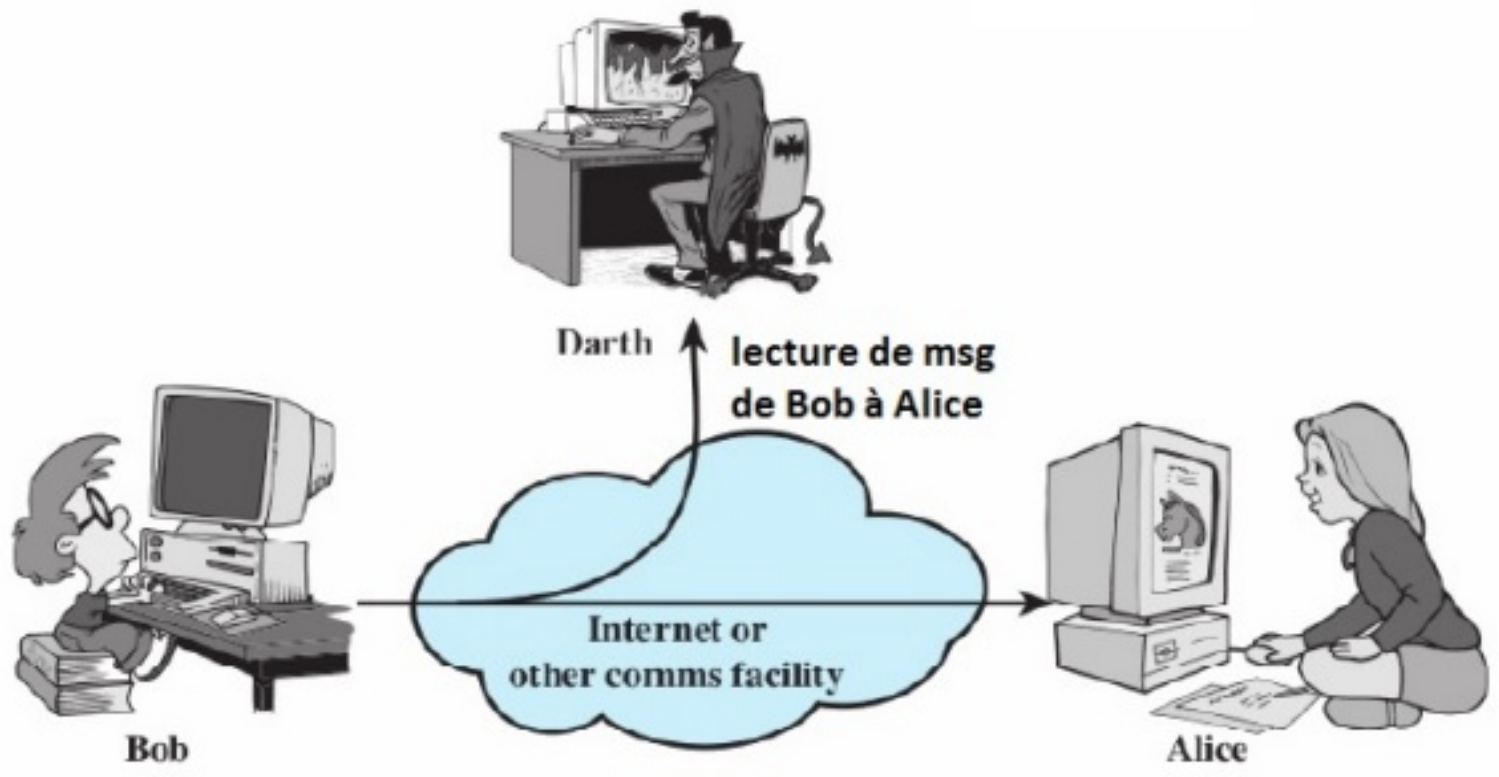


(a) Passive attacks

(b) Active attacks

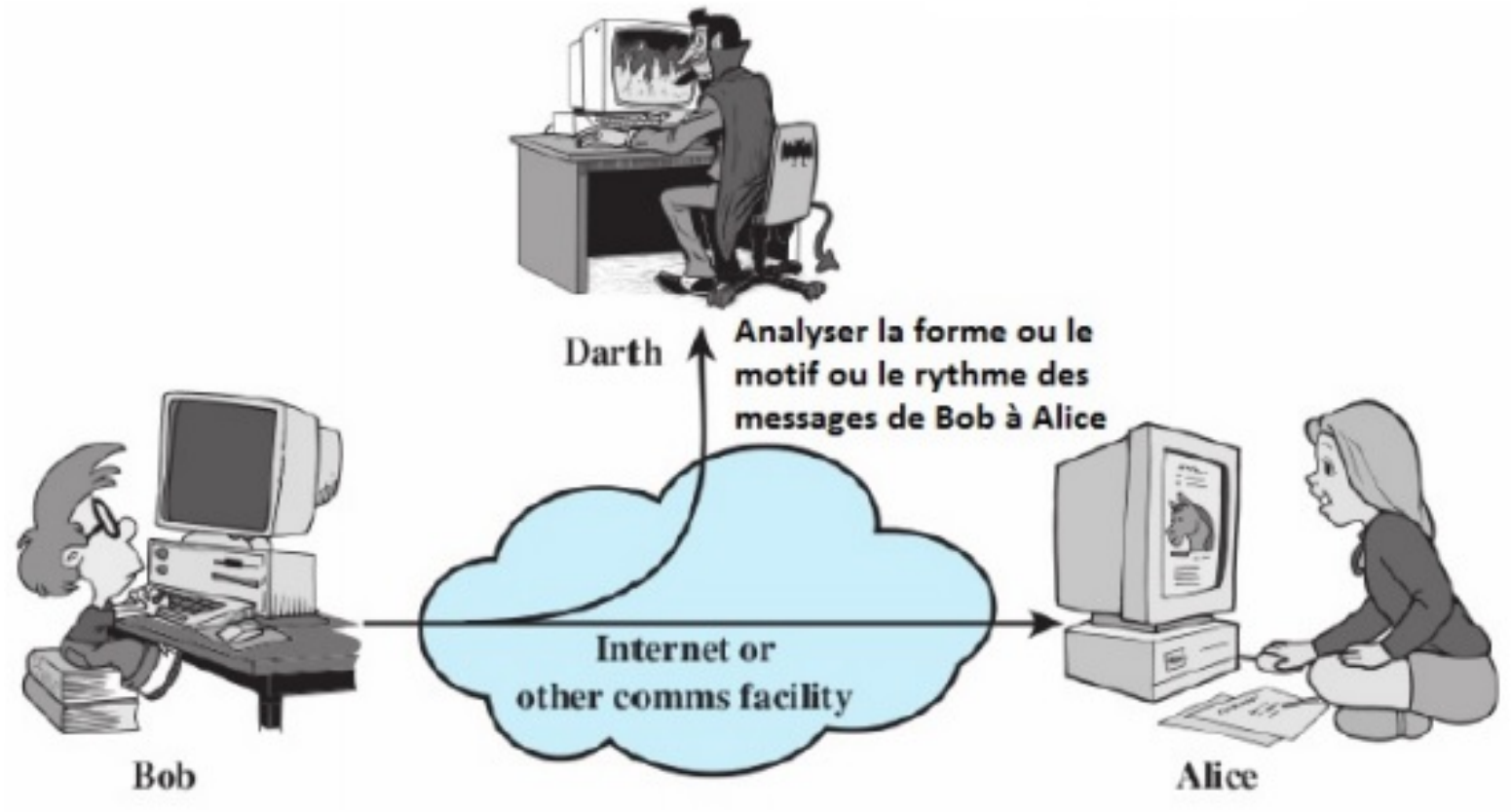
Types d'attaques
Attaques passives

Lecture du contenu du message

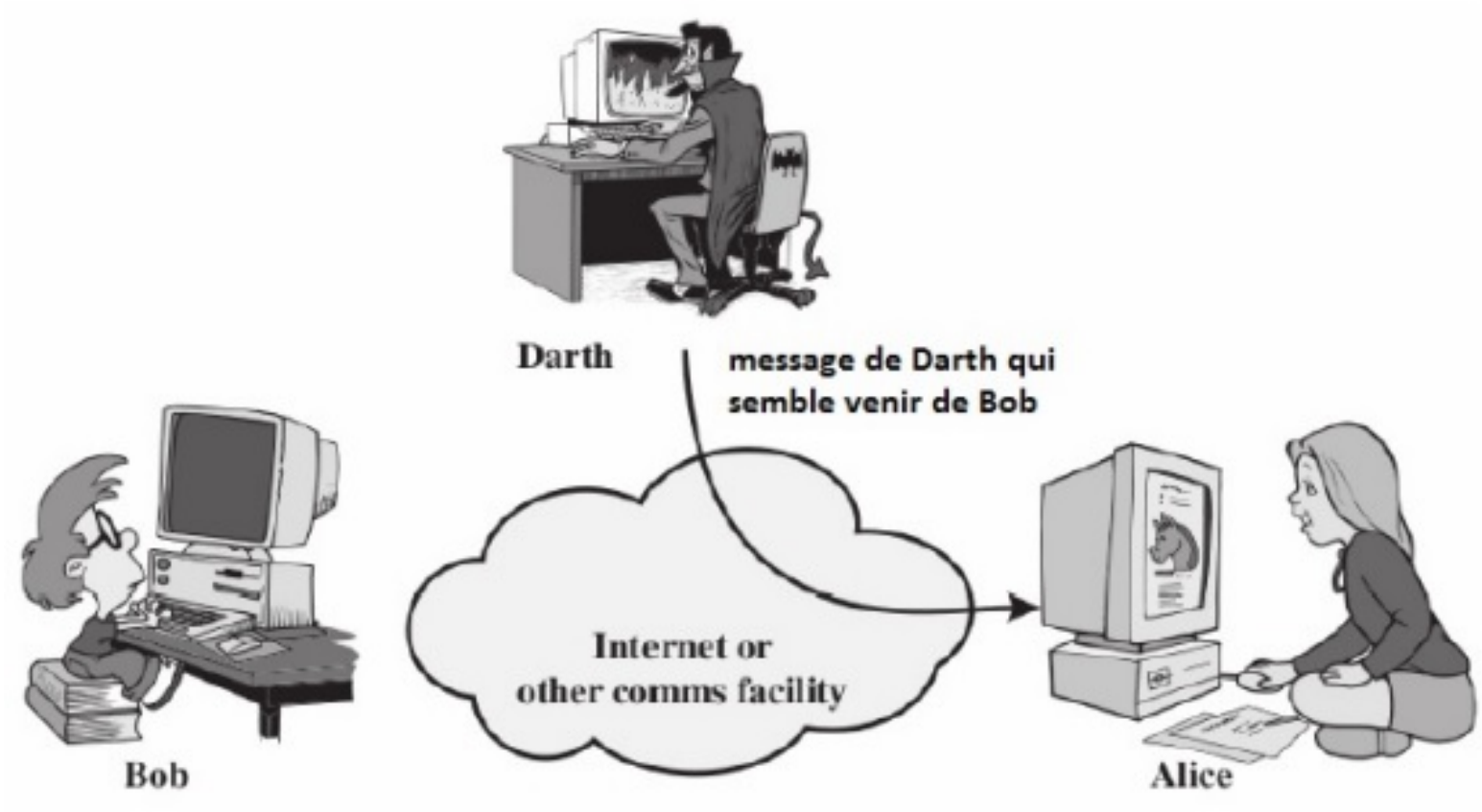


Types d'attaques
Attaques passives

Analyse du Trafic

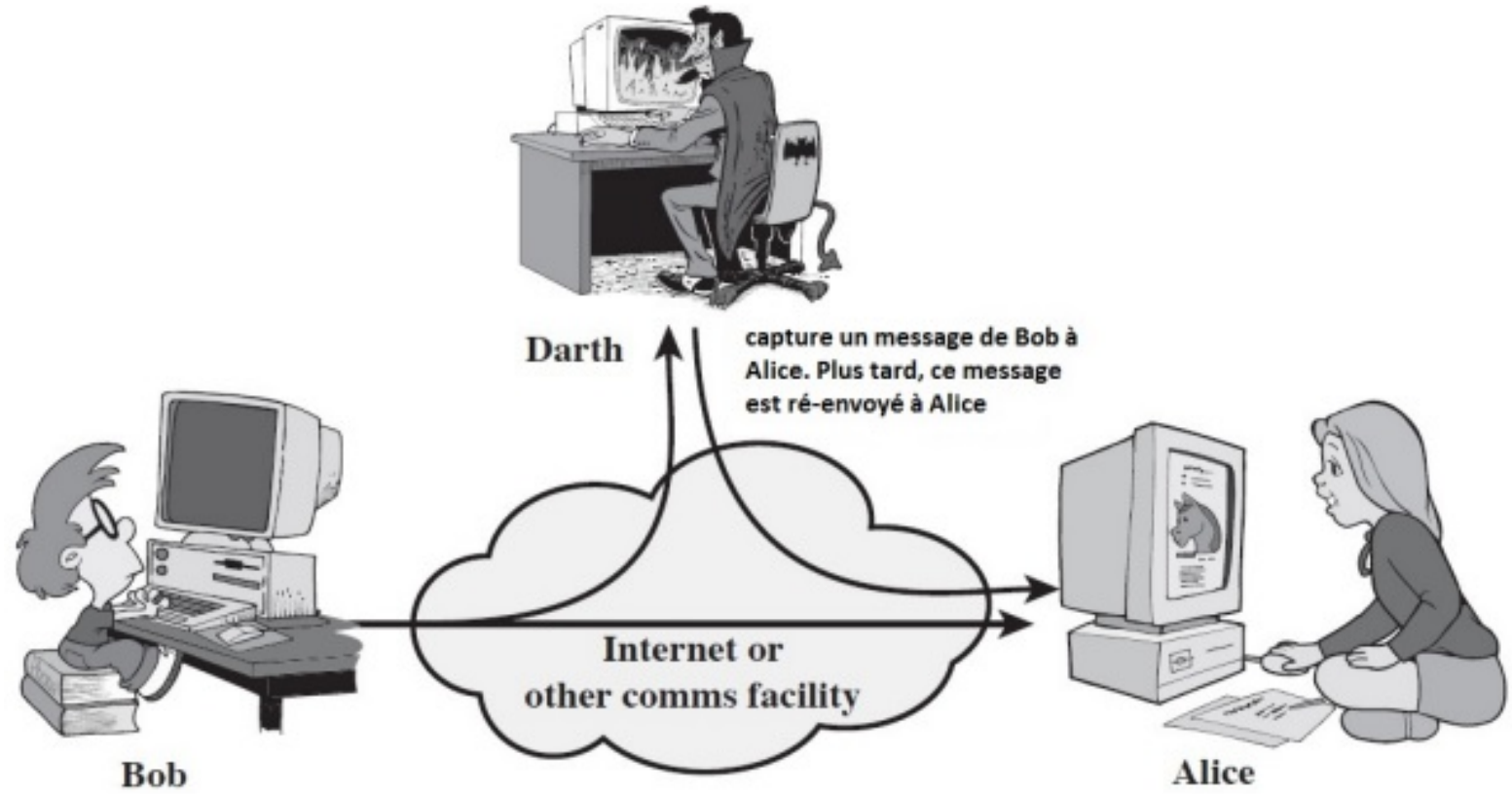


Mascarade

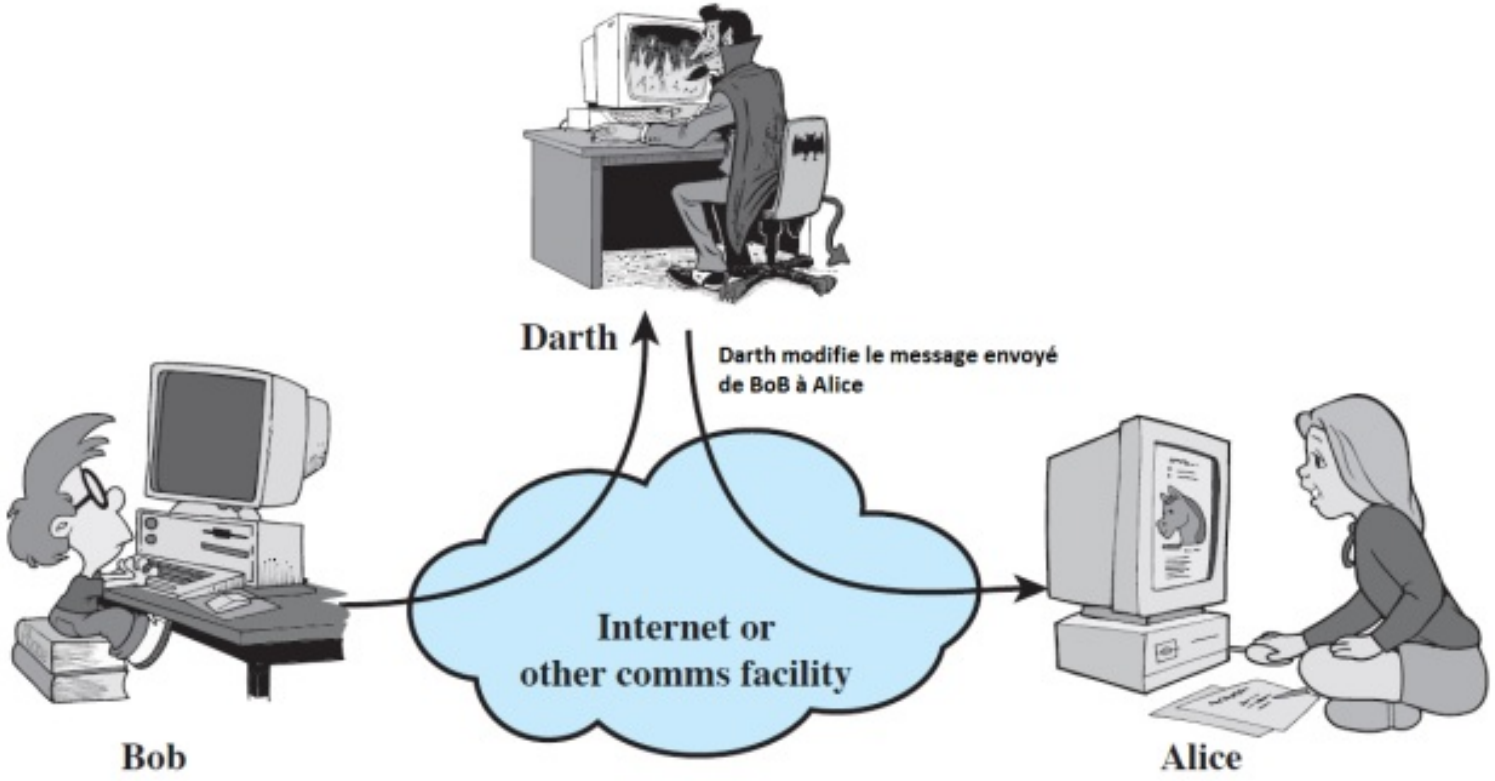

Darth
message de Darth qui
semble venir de Bob
Internet or
other comms facility
Bob
Alice

Types d'attaques
Attaques actives

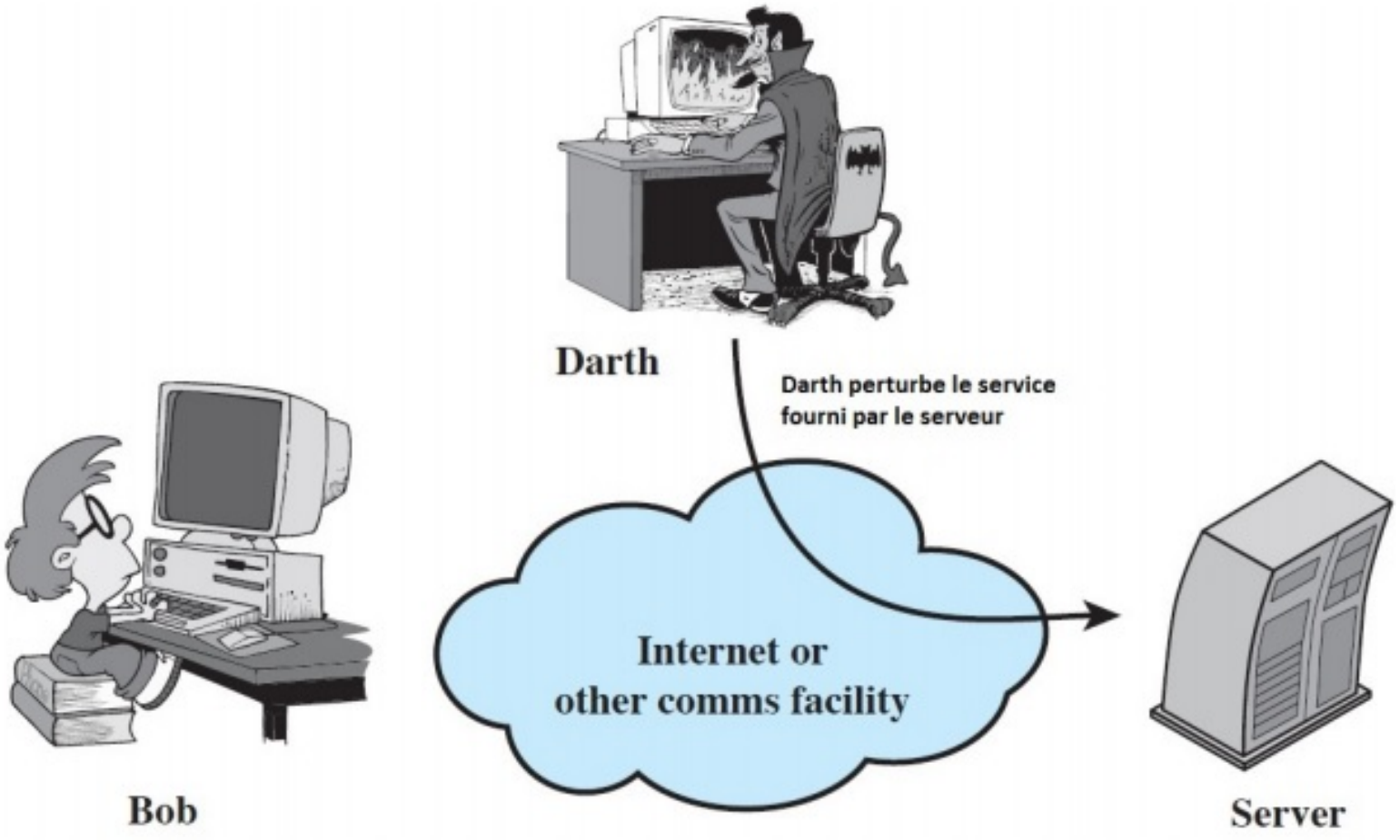
Replay attack



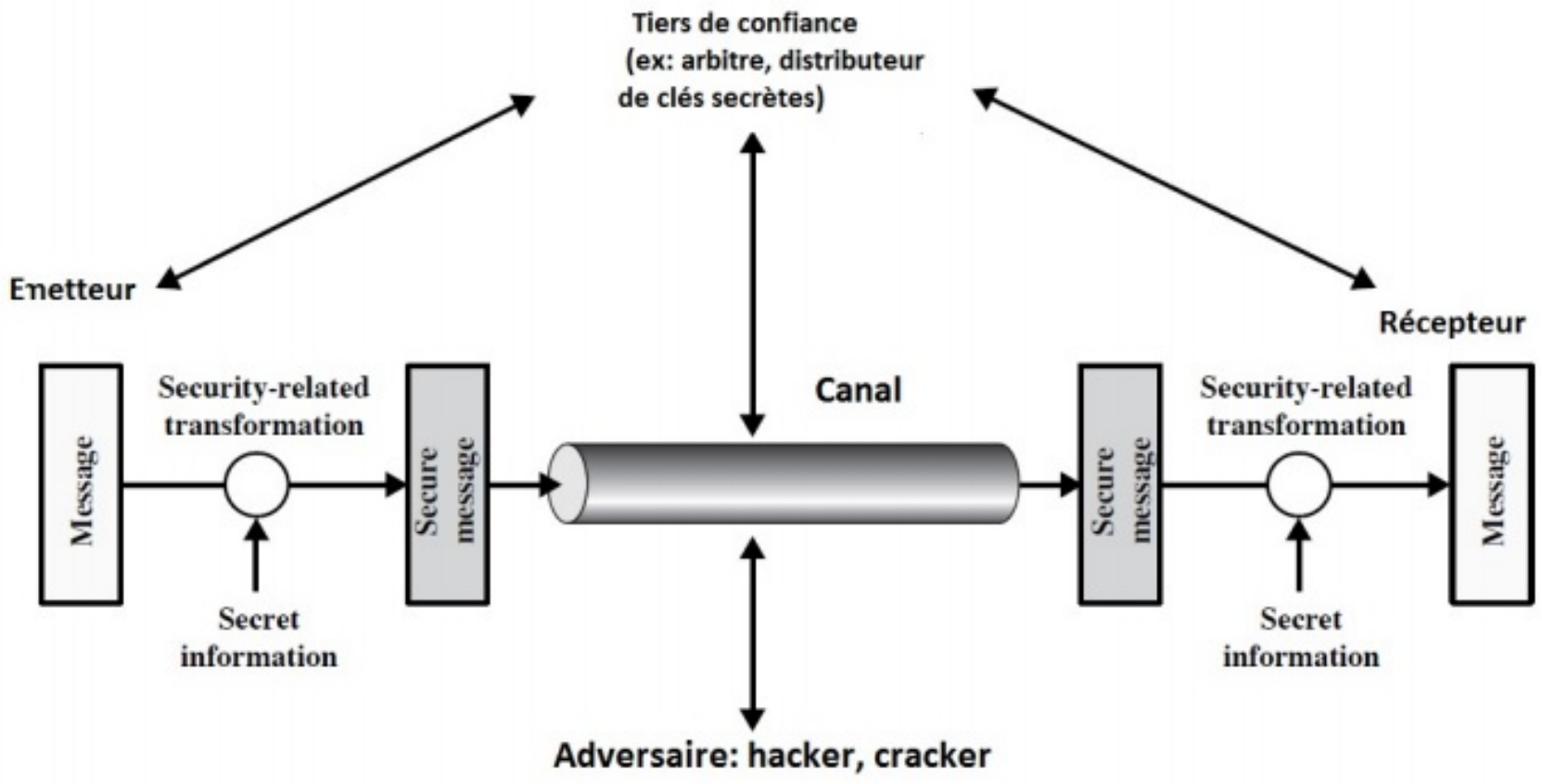
Modification



DoS (Denial of Service)

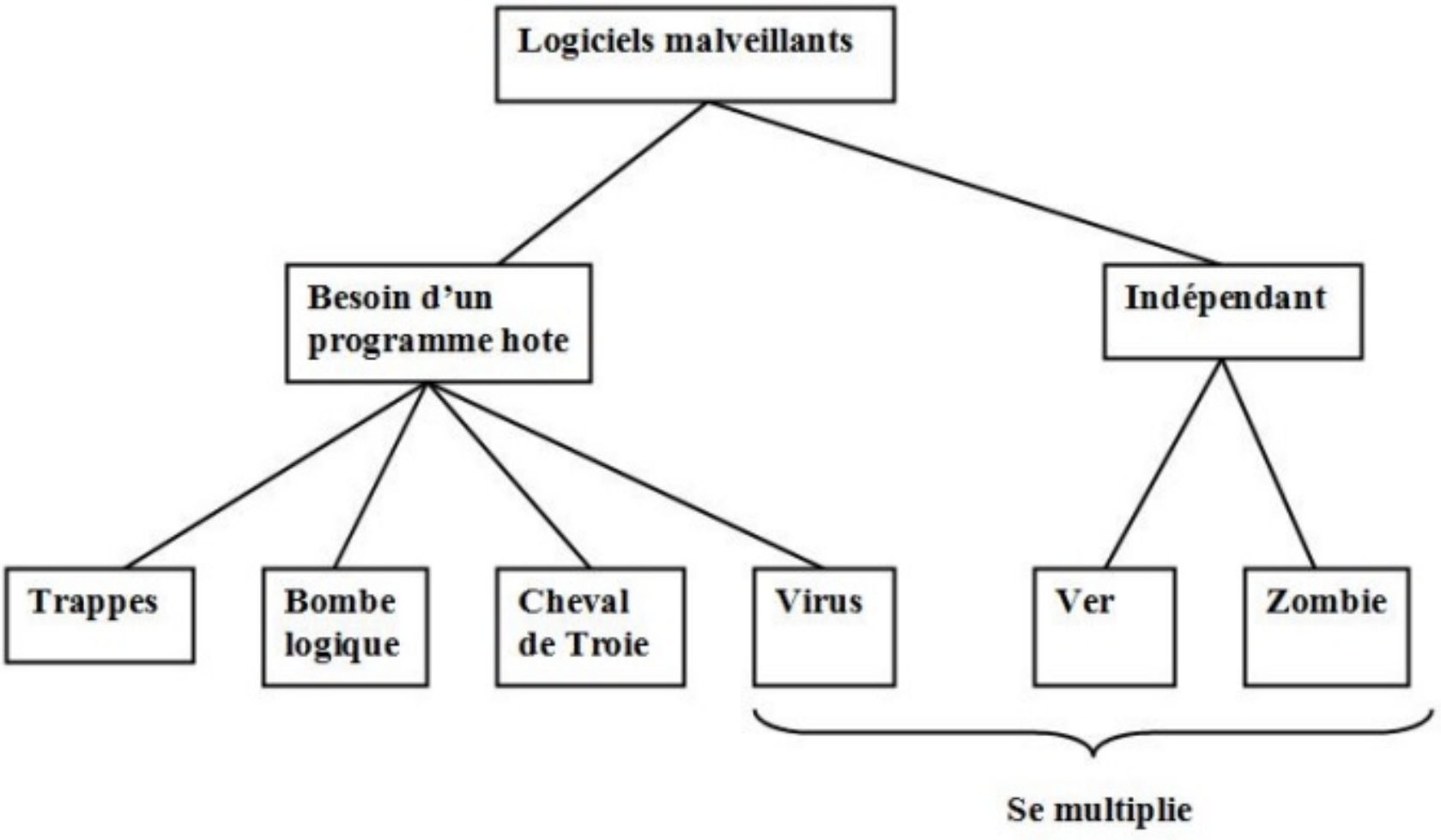


	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			


Tiers de confiance
(ex: arbitre, distributeur
de clés secrètes)
Enetteur
Récepteur
Message
Security-related
transformation
Secure
message
Canal
Secure
message
Security-related
transformation
Message
Secret
information
Secret
information
Adversaire: hacker, cracker

Méthodes de défense

- **Chiffrement de données**
- **Contrôle d'accès software** : limiter l'accès aux bases de données, protéger chaque utilisateur des autres utilsateurs
- **Contrôle d'accès hardware** : ex Cartes à puce
- **Politiques de sécurité** : changer fréquemment les mots de passes
- Utiliser **les Firewalls**, **les systèmes de détection d'intrusion**, les **anti-virus**
- **Utiliser les réseaux VLAN** pour cacher les différentes parties des réseaux
- **Pour accès distant utiliser les VPN** : Virtual Private Network


Logiciels malveillants
Besoin d'un programme hote
Indépendant
Trappes
Bombe logique
Cheval de Troie
Virus
Ver
Zombie
Se multiplie

Trappes (Trapdoors or backdoors)

- Point d'entrée secrète dans un programme
- Permet de surpasser les mécanismes de sécurité surtout d'authentification.
- Ont été couramment utilisé par les développeurs
- C'est une menace sérieuse lorsque un programme de production est infiltré par un adversaire pour laisser des trapdoors.
- Très difficile à trouver dans les systèmes d'exploitation
- Seule remède : faire des mises à jour des programmes soft pour éliminer ces trapdoors ds les programmes anciens

Bombe Logique

- Le plus ancien type des logiciels malveillants
- Code inséré dans un programme légitime
- Activée lorsque des conditions spécifiques se reproduit :
  - ex : prsence/absence de quelque fichiers
  - une date particulière
  - un utilisateur particulier
  - une série particulière de frappes de clavier
- Une fois déclenché, le système est endommagé
- modifie/supprime des fichiers/disques

Cheval de Troie

- Programmes qui semblent avoir une fonction mais en fait effectuer une autre.
- Il ressemble à un programme que l'utilisateur est attiré à l'exécuter. ex : jeu ; mise à jour d'un software
- Lorsqu'il est exécuté, il performe d'autres taches qu'annoncées. Ex : laisse un adversaire d'avoir un accès au système.
- Souvent utilisé pour propager un virus/ver ou pour installer un trapdoor
- ou simplement pour détruire les données.

Zombie

- Programme qui, secrètement, prend le contrôle sur un autre ordinateur du réseau
- Puis il l'utilise pour lancer des attaques indirectement
- Utilisé souvent pour lancer des attaques DDoS : Distributed Denial of Service
- Exploite des défauts connus dans le réseau.

Virus

- Une portion de code qui infecte les programmes
  - les modifier pour y inclure une copie du virus
  - il s'exécute en secret lorsque le programme hôte est lancé
- Chaque virus est spécifique pour un système d'exploitation et un hardware
  - profitant de leurs détails et les faiblesses
- Un virus passe par plusieurs phases
  - dormant
  - propagation
  - déclenchement
  - Exécution

Structure d'un virus

- Composants :
  - **Mécanisme d'infection** : pour la réplication
  - **Gâchette** : évènement causant le déclenchement de la charge (payload)
  - **Payload (charge)** : l'effet malveillant du virus
- **Propagation** :
  - Méthode par laquelle le virus se propage
  - Autrefois : un virus sur un PC, transféré à d'autres hôtes par des disquettes.
  - De nos jours : l'Internet est son moyen de propagation, les flash USB.

Classification des virus

- **Parasitaire** : se joint à l'exe, infecte et cause des dommages lorsqu'il est exécuté
- **Virus résident à la mémoire** : se charge en mémoire, infecte chaque application exécutée
- **Virus du secteur boot** : infecte les fichiers de démarage, et se multiplie en démarrage
- **virus furtif** : conçu pour se cacher d'un antivirus
- **virus polymorphe** : mute à chaque infection, difficile à détecter sa signature
- **virus métamorphique** : se réécrit complètement à chaque fois et change son comportement

Les antivirus

- Fonctions basiques :
  - **Détection** : détermine que l'infection par un virus s'est produite
  - **Identification** : identifie le virus spécifique relié à l'infection
  - **suppression** : supprimer les virus de programmes infectés
- Antivirus de Première Génération :
  - exiger la signature de virus pour identifier les virus
  - signature : structure, modèle binaire, les caractères génériques
  - mémorise la longueur des programmes, recherchez les changements
- Antivirus de deuxième génération :
  - utiliser des règles heuristiques, la recherche de l'infection probable
  - Cherche des portions cryptée de codes, détermine les clés privées
  - vérification d'intégrité, utiliser les empreintes digitales, les hash codes.
- Antivirus de troisième génération : réside dans la mémoire, identifie les virus par leurs actions et non signature
- Antivirus 4eme génération : package contenant des Techniques AV multiples, limite la capacité d'infection des virus

Ver

- Code actif Autonome qui peut se répliquer à des hôtes distants sans déclenchement
- Réplication mais sans infection des programmes
- Parce qu'ils se propagent de manière autonome, ils peuvent se propager beaucoup plus rapidement que les virus !
- Sa Vitesse de propagation fait que les vers constituent les menaces les plus importantes

Les attaques des vers récentes

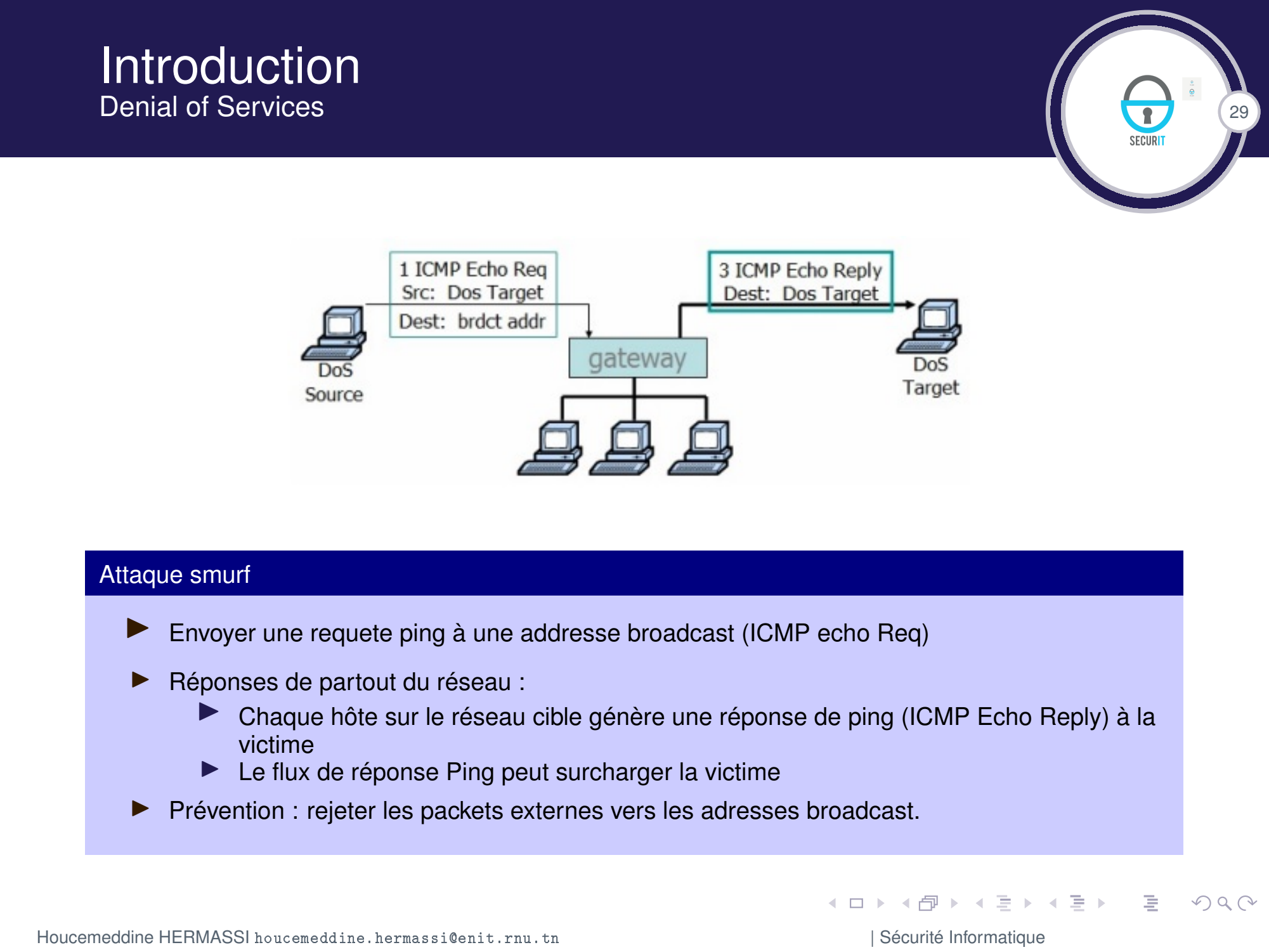
- **Code Red**
  - Juillet 2001 expolitant un bug système
  - choisi un adresse IP aléatoire et lance une attaque DDoS
- **Code Red II** : une variante qui installe aussi un trapdoor
- **SQL SLammer**
  - début 2003, attaques MS SQL Server
- **Mydoom**
  - en 2004, un ver qui envoie une quantité de mails énorme
  - installe des backdoor dans les systèmes infectés
- **Warezov** : scanne des adresses mails, transmet en pièce jointe

Les Vers de téléphones mobiles

- des vers apparus sur les mobiles en 2004
- ciblent les smartphones qui peuvent installer des softwares
- communiquent en utilisant le blutooth et MMS
- désactive le téléphone, supprime des données du téléphone, ou envoyer des messages
- **CommWarrior**, lancé en 2005 :
  - se réplique via blutooth aux smartphones proches
  - et via MMS en utilisant le carnet d'adresse

Denial of Service

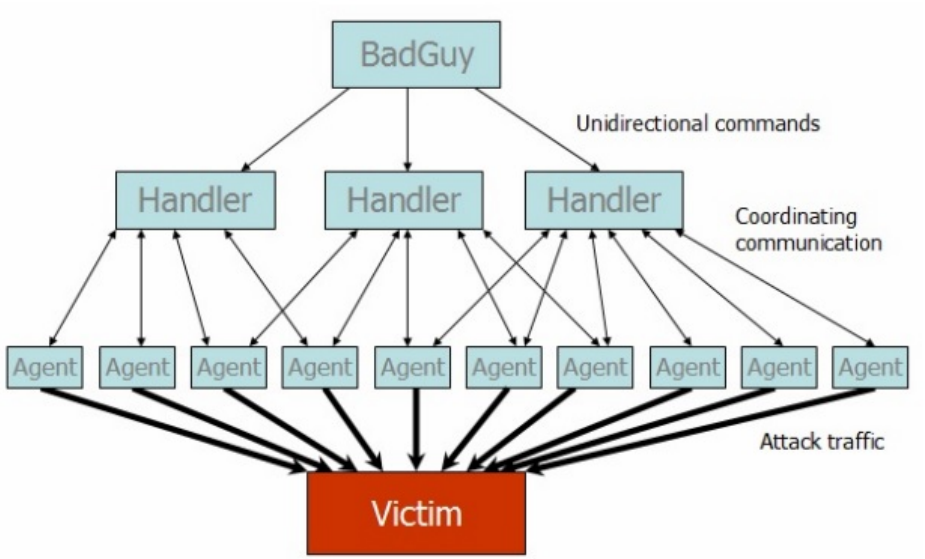
- Une tentative par des attaquants afin d'empêcher les utilisateurs légitimes d'un service d'utiliser ce service
- Modèle de la menace DoS :
  - La consommation de connectivité et / ou la bande passante réseau
  - La consommation d'autres ressources, par exemple file d'attente, CPU
  - La destruction ou l'alternance de la configuration de l'information : Paquets malformés peuvent mettre une application en confusion et l'amener à geler
  - Destruction physique ou alternance des composants de réseau
- Consomme la mémoire système : un script de programme se fait des copies
- consomme la mémoire disque : générer beaucou d'emails,générer beaucoup d'erreurs, placer des fichiers dans des zones partagées de la mémoire



Attaque smurf

- Envoyer une requete ping à une addresse broadcast (ICMP echo Req)
- Réponses de partout du réseau :
  - Chaque hôte sur le réseau cible génère une réponse de ping (ICMP Echo Reply) à la victime
  - Le flux de réponse Ping peut surcharger la victime
- Prévention : rejeter les packets externes vers les adresses broadcast.

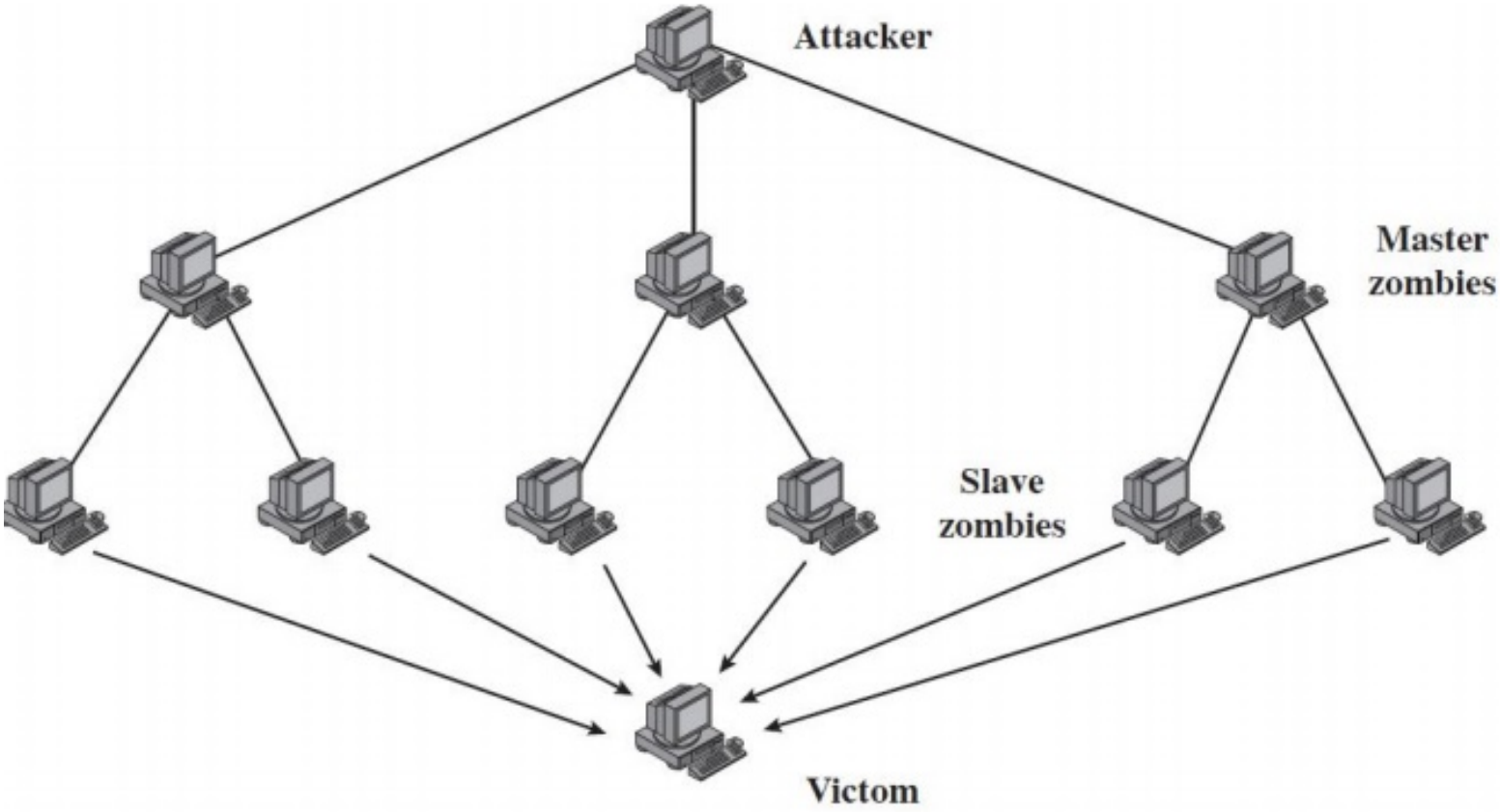
Distributed DoS



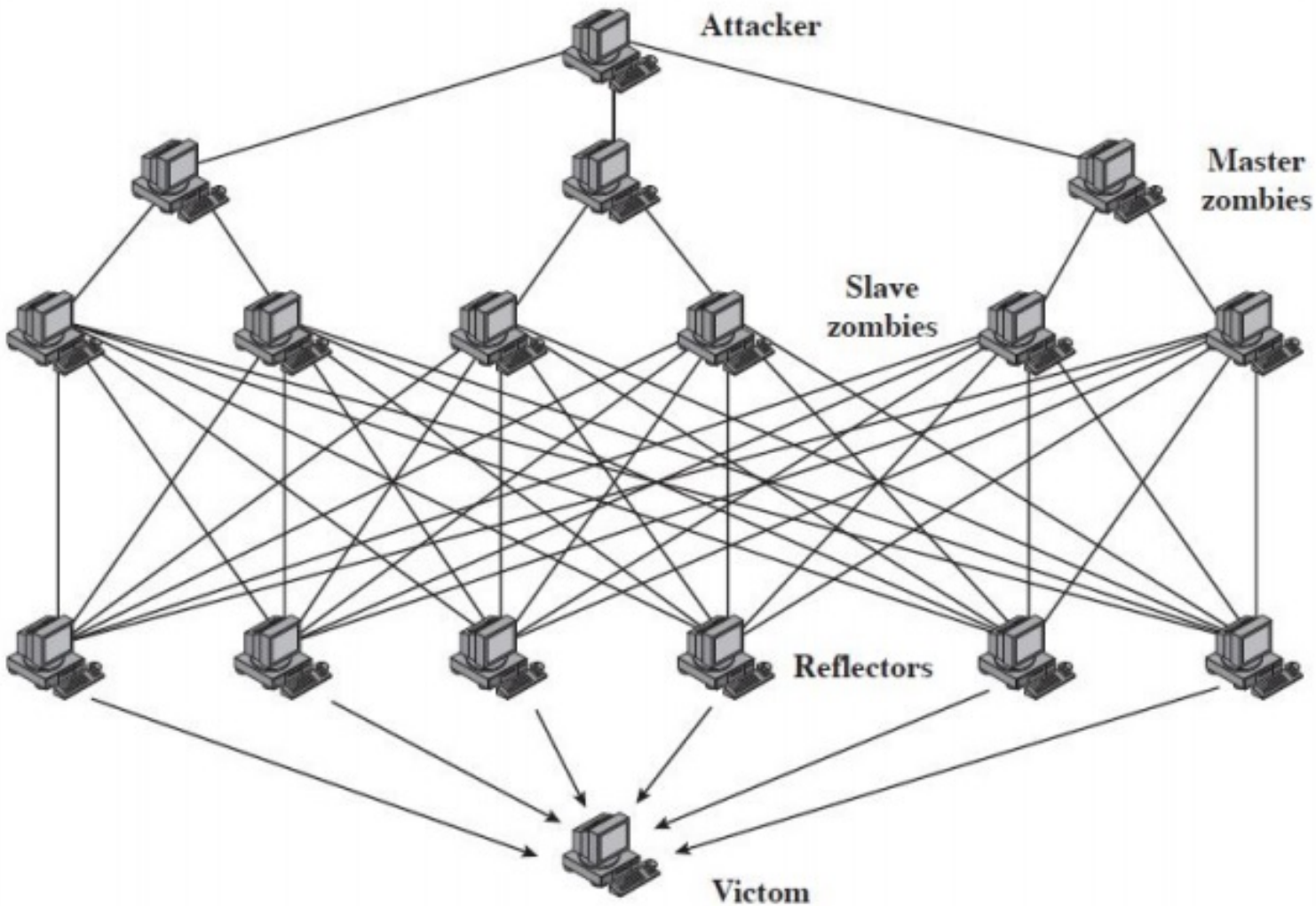
Pourquoi DDoS

- Peut-on trouver BadGuy ? celui qui a initié l'attaque ?
  - l'initiateur de l'attaque a utilisé les handlers (gestionnaires)
  - l'initiateur n'est pas actif lorsque l'attaque DDoS se produit
- on peut essayer de trouver les agents
- il faut une nalyse de trafic sur différents points du réseau

Reflector DDoS



Direct DDoS



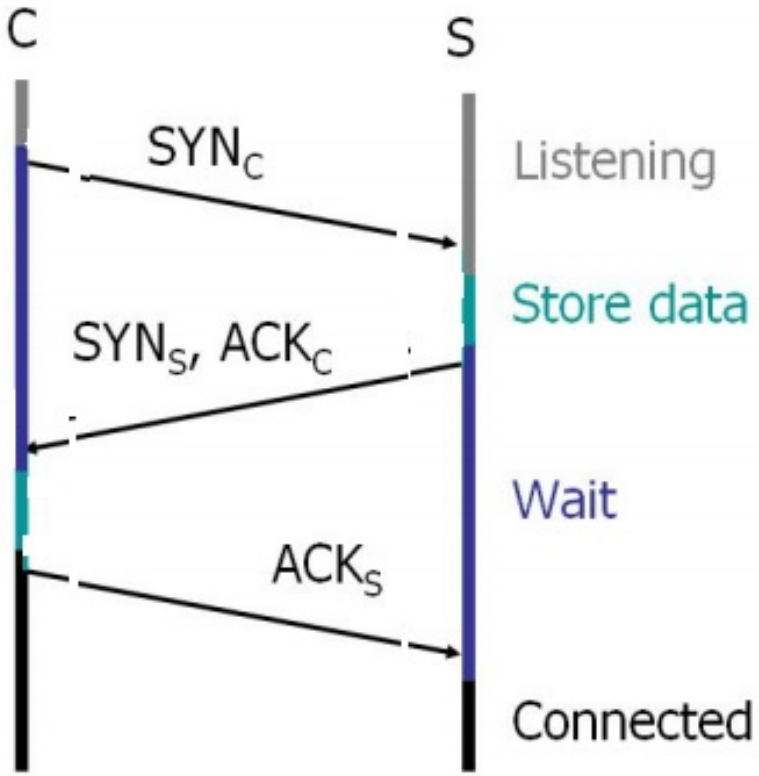
SYN flooding attack

- 90% des attaques DoS ont pour origine TCP SYN folooding
- exploite une vulnérabilité dans l'établissement de la connection TCP
- le serveur commence des connexions "semi-ouverte"
- Ces demandes de connexions se multiplient jusqu'à la file d'attente est pleine et les requêtes additionnelles sont bloqués.

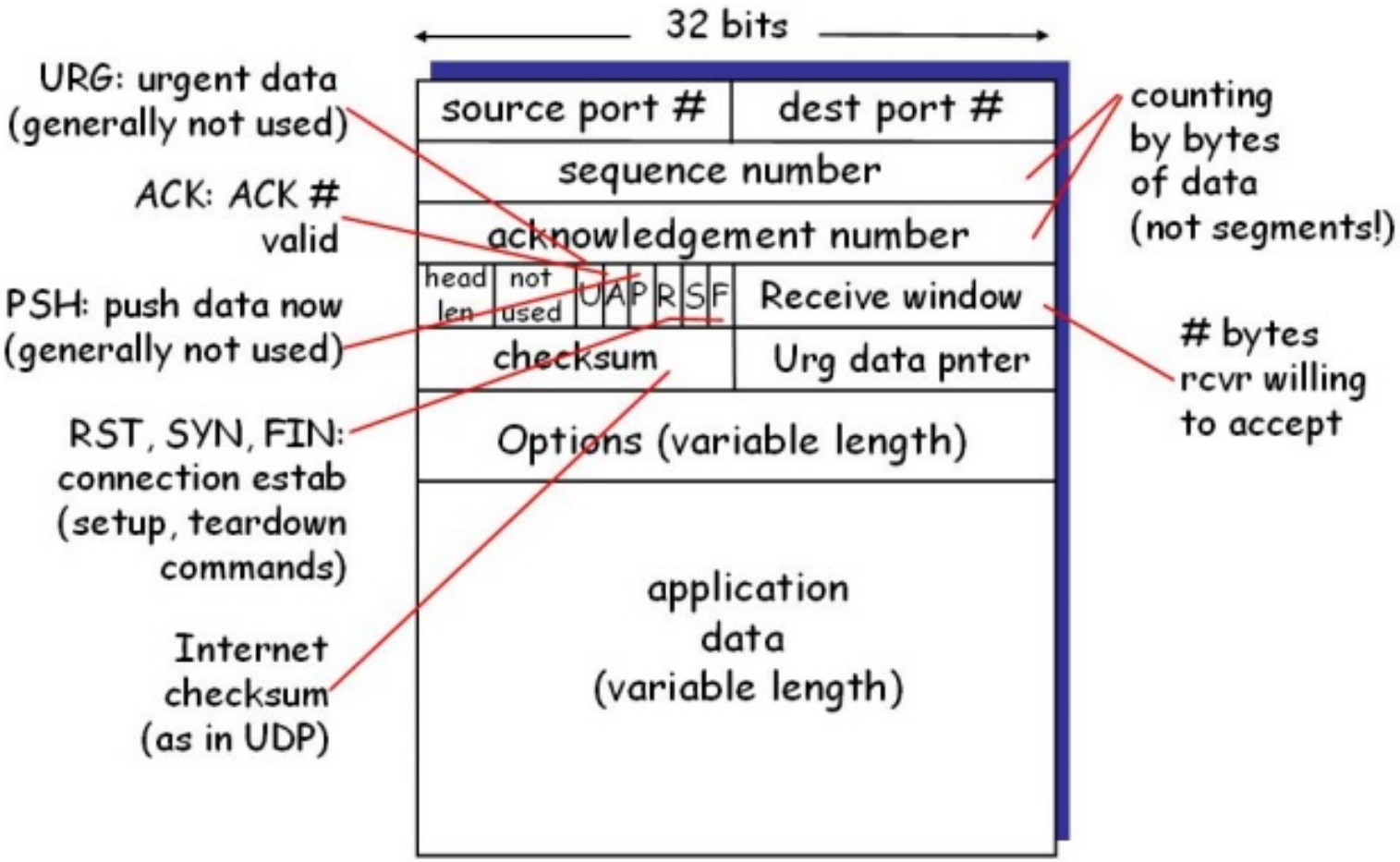
Rappel: connexion TCP

Émetteur (client) et récepteur (Serveur) établissent une "connexion" avant d'échanger des données

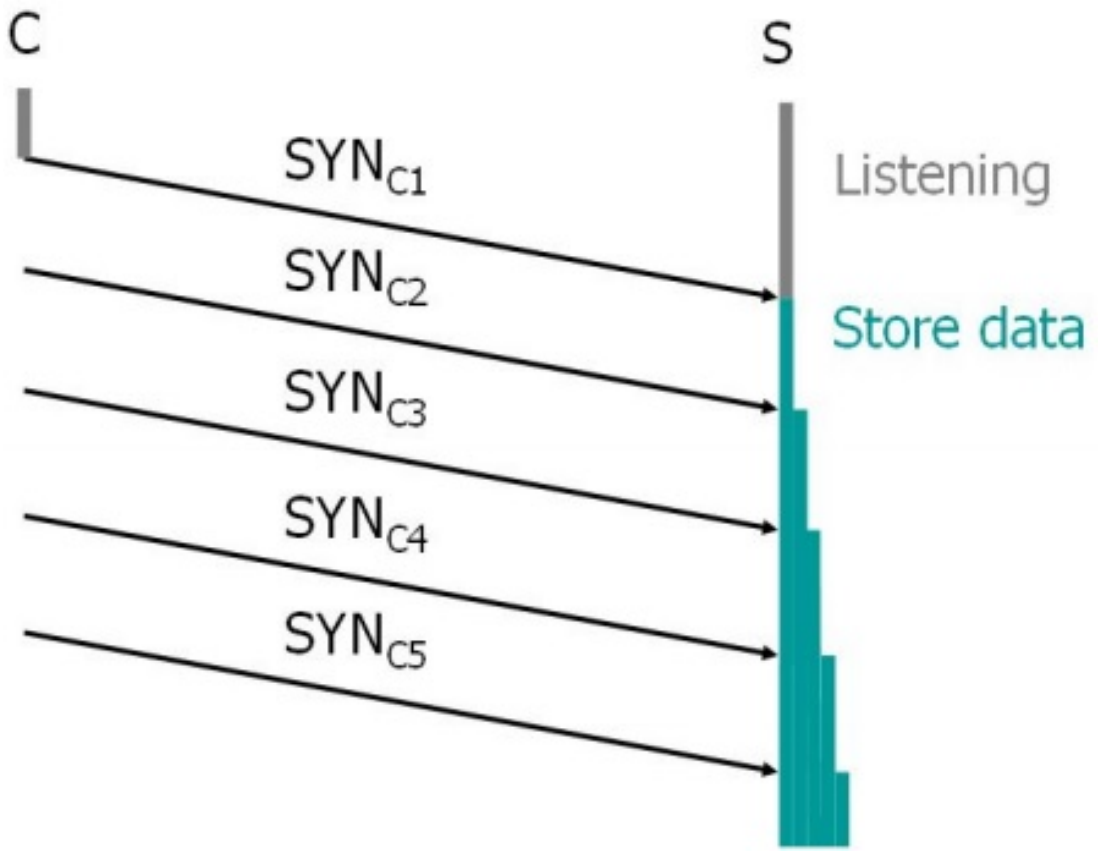
- le client envoie un segment TCP SYN au serveur :
  - spécifie une sequence initiale seq#
  - pas de données
- serveur reçoit SYN et répond par sagement SYNACK
  - Serveur alloue des buffers
  - spécifie la séquence de serveur initiale seq#
- Le client reçoit SYNACK du serveur et répond par ACK qui peut contenir des données



Structure du segment TCP



SYN flooding



SYN flooding: analyse

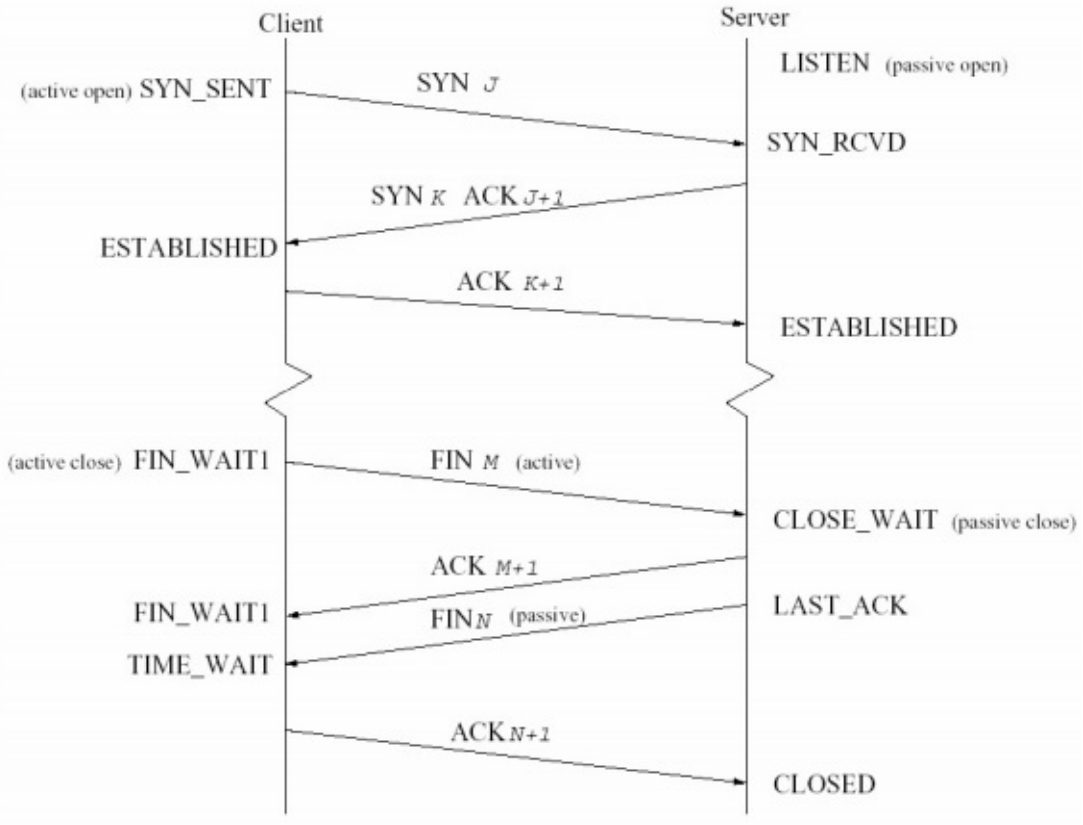
- l'adversaire a envoyé plusieurs segments TCP/syn

No. .	Time	Source	Destination	Protocol	Info
9987	27.842666	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9988	27.845329	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9989	27.847992	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9990	27.850654	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9991	27.854647	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9992	27.857310	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9993	27.859973	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9994	27.862635	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9995	27.865297	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9996	27.867960	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9997	27.870621	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9998	27.873284	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
9999	27.875931	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le
10000	27.878618	211.23.45.69	192.168.1.10	TCP	45873 > http [SYN] Seq=0 Win=0 Le

SYN flooding

- Attaquant envoie de nombreuses demandes de connexion avec des adresses sources usurpées (Adress spoofing)
- Victime alloue des ressources pour chaque demande
- Une fois les ressources épuisées, les demandes des clients légitimes se voient refuser
- c'est la DoS classique : ça ne coûte rien à l'initiateur TCP pour envoyer une demande de connexion, mais le récepteur doit reserver des ressources pour chaque demande

TCP connexion

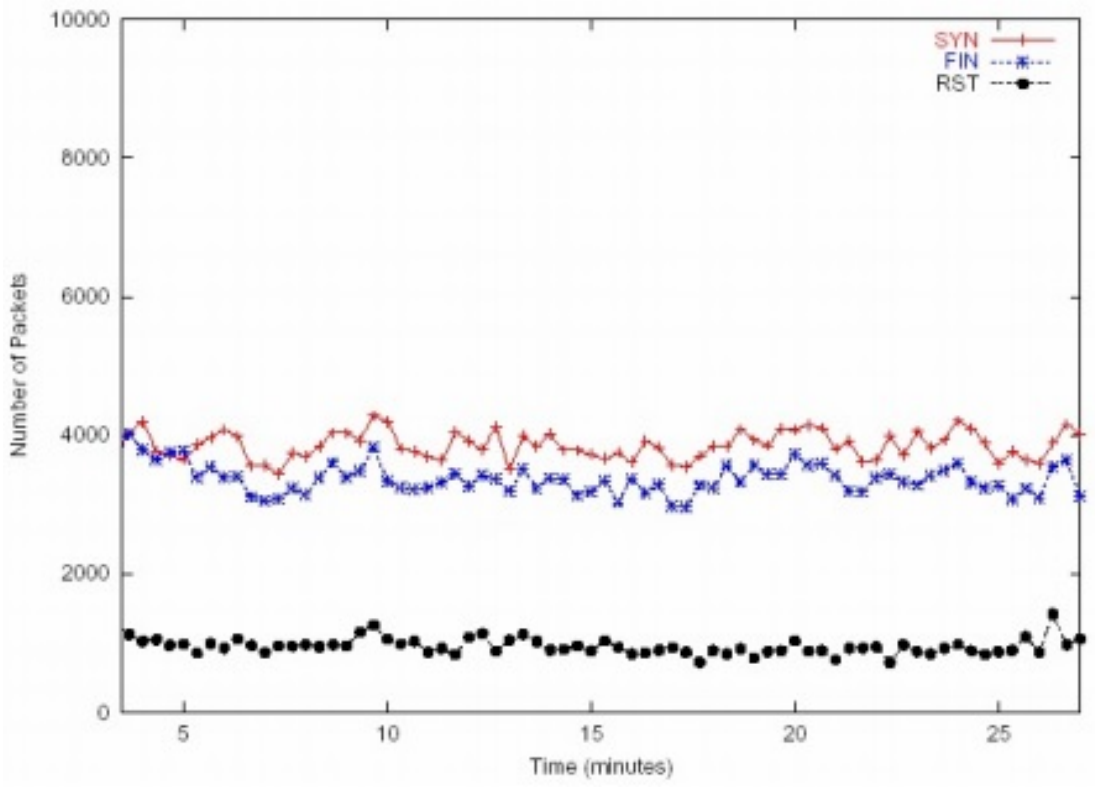


Détection de DoS

- Analyser le comportement des paires **SYN-FIN**
- ou analyser le comportement des paires **SYNACK-FIN**
- Mais RST viole la regle **SYN-FIN**
  - Passive **RST**: transmise après l'arrivé d'un packet à un port fermé (par le serveur)
  - Active **RST**: initié par le client pour abondonner une connexion TCP
- donc les paires **SYN-RST** active sont aussi normales

Paires SYN-FIN

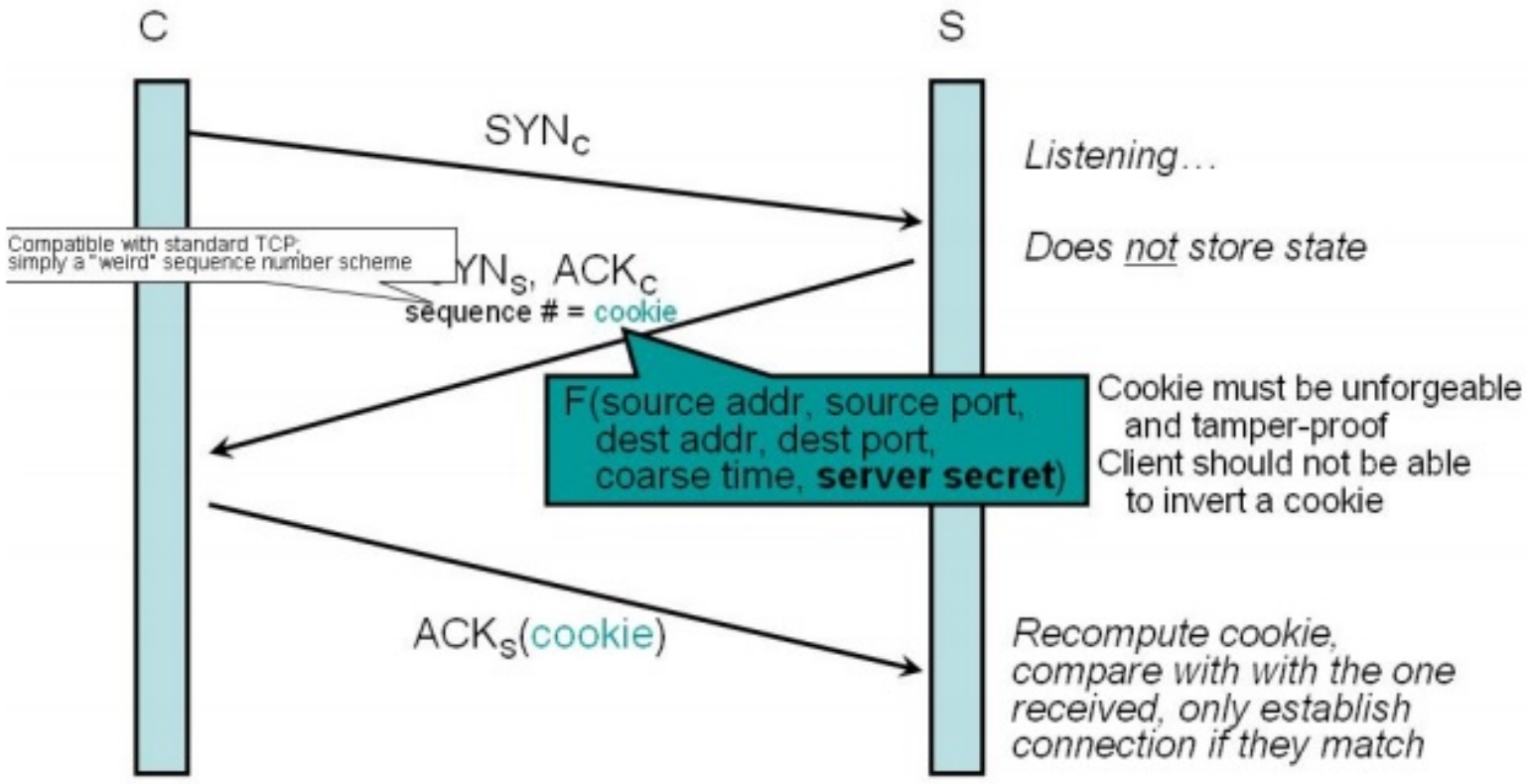
- Généralement chaque **SYN** a un **FIN**
- on ne peut dire si les RST sont active ou passive
- généralement 75% des RST sont actives



Prévention de DoS

- DoS est causée par une allocation asymétrique des ressources
- Si le récepteur alloue des ressources pour chaque connexion, l'adversaire peut initier des milliers de connnexions à partir des adresses usurpées et trafiquées
- Les Cookies assurent que le récepteur n'alloue des ressources que si l'incitateur a envoyé au moins deux messages
- L'etat du récepteur est enregistré dans une cookie et envoyé à l'initiateur

SYN cookies


C
S
SYN$_C$
Listening…
Does not store state
Compatible with standard TCP;
simply a "weird" sequence number scheme
YN$_S$, ACK$_C$
sequence # = cookie
F(source addr, source port,
dest addr, dest port,
coarse time, server secret)
Cookie must be unforgeable
and tamper-proof
Client should not be able
to invert a cookie
ACK$_S$(cookie)
Recompute cookie,
compare with with the one
received, only establish
connection if they match

ARP spoofing

- ARP (Adress Resolution Protocol) : il permet de trouver une adresse niveau 2 (Ethernet) à partir d'une adresse niveau 3 (IP).
- fonctionnement :
  - client : who has 10.1.2.3 ? ?
  - n'importe qui : 10.1.2.3 is at 09 :0A :0B : :0C :0D :0E
- c'est fait de forger des réponses, même non-sollicités, pour rediriger le trafic

ARP flooding

- le hacker change a chaque fois son adresse MAC et diffuse ensuite la paquet ARP

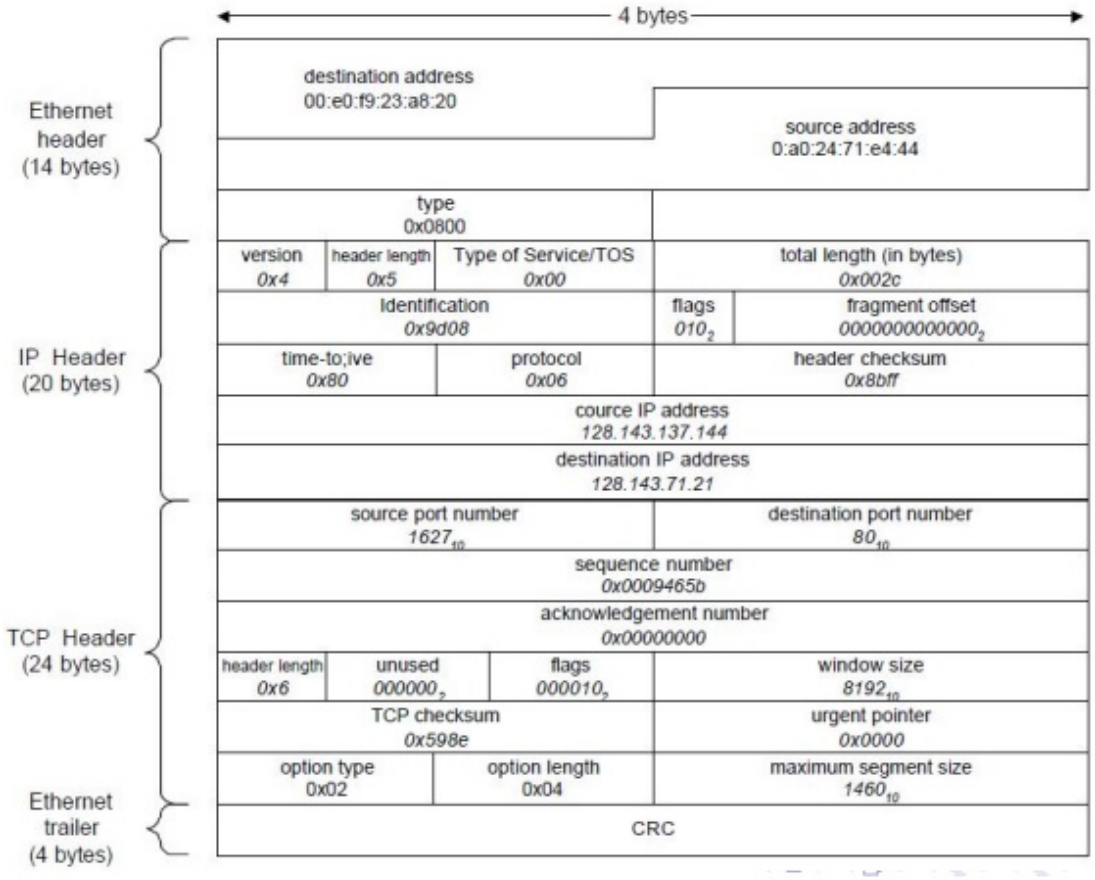
o.	Time	Source	Destination	Protocol	Length	Info
2	0.122161	da:8d:ea:26:6d:d3	Broadcast	ARP	57	Who has 201.175.168.237? Tell 178.151.202.185
3	0.122487	ff:cd:41:7a:84:f7	Broadcast	ARP	57	Who has 47.239.178.21? Tell 204.13.62.128
4	0.122635	db:e1:2b:ec:c1:28	Broadcast	ARP	57	Who has 123.8.148.134? Tell 169.32.42.234
5	0.122772	5f:6b:6a:33:f9:f8	Broadcast	ARP	57	Who has 83.40.96.62? Tell 165.58.203.219
6	0.122907	00:ce:91:6d:5b:3c	Broadcast	ARP	57	Who has 28.15.255.6? Tell 134.98.23.76
7	0.123046	de:3c:56:9a:84:54	Broadcast	ARP	57	Who has 182.101.178.106? Tell 116.188.186.238
8	0.123180	57:7a:bf:97:05:07	Broadcast	ARP	57	Who has 211.33.98.84? Tell 20.207.202.130
9	0.123322	d1:0b:2e:82:bf:0b	Broadcast	ARP	57	Who has 139.99.131.213? Tell 179.114.127.47
10	0.123456	bc:a0:8c:b1:79:aa	Broadcast	ARP	57	Who has 210.122.153.41? Tell 227.133.125.43
11	0.123591	1e:f8:25:9f:9a:23	Broadcast	ARP	57	Who has 1.230.152.3? Tell 247.239.111.104
12	0.123726	2c:9b:fb:80:f6:b8	Broadcast	ARP	57	Who has 137.151.187.147? Tell 64.110.1.38
13	0.123858	af:18:8d:51:08:8c	Broadcast	ARP	57	Who has 148.190.141.236? Tell 1.62.122.158
14	0.123989	58:a5:6f:ac:13:b8	Broadcast	ARP	57	Who has 28.222.44.183? Tell 104.166.143.25
15	0.124121	24:5a:27:a2:fa:45	Broadcast	ARP	57	Who has 174.12.18.84? Tell 20.230.25.54

DHCP Starvation

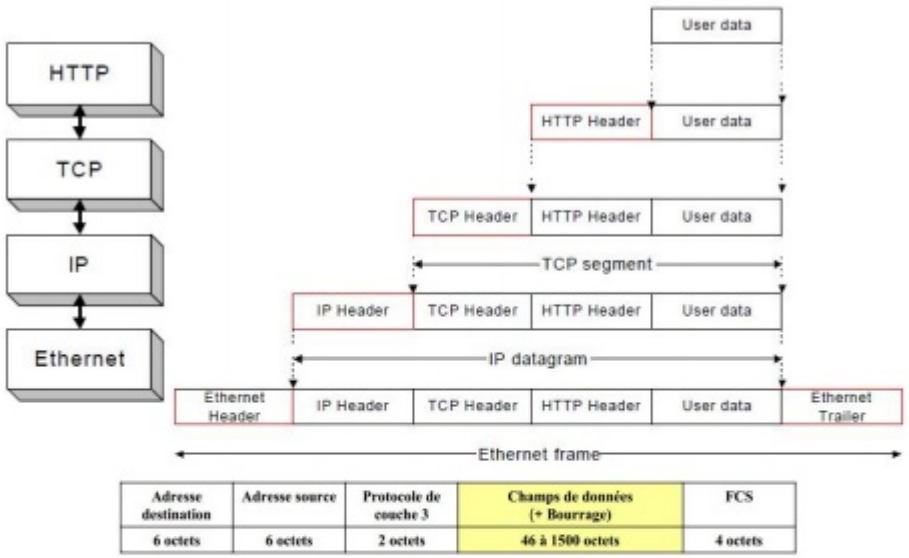
- le hacker change son MAC et demande une configuration IP

No.	Time	Source	Destination	Protocol	Length	Info
56	24.16095	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x7c957961
58	26.11032	192.168.1.1	192.168.1.11	DHCP	320	DHCP Offer - Transaction ID 0x7c957961
59	26.11137	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0x7c957961
60	26.14777	192.168.1.1	192.168.1.11	DHCP	320	DHCP ACK - Transaction ID 0x7c957961
61	26.14877	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xad3c806b
63	28.14041	192.168.1.1	192.168.1.12	DHCP	320	DHCP Offer - Transaction ID 0xad3c806b
64	28.14143	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0xad3c806b
65	28.16074	192.168.1.1	192.168.1.12	DHCP	320	DHCP ACK - Transaction ID 0xad3c806b
66	28.16184	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x3e9c6137
70	30.11740	192.168.1.1	192.168.1.13	DHCP	320	DHCP Offer - Transaction ID 0x3e9c6137
71	30.11836	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0x3e9c6137
72	30.14190	192.168.1.1	192.168.1.13	DHCP	320	DHCP ACK - Transaction ID 0x3e9c6137
73	30.14288	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xdf599404
75	31.56000	192.168.1.1	192.168.1.14	DHCP	320	DHCP Offer - Transaction ID 0xdf599404
76	31.56311	0.0.0.0	255.255.255.255	DHCP	304	DHCP Request - Transaction ID 0xdf599404
77	31.60755	192.168.1.1	192.168.1.14	DHCP	320	DHCP ACK - Transaction ID 0xdf599404

Exemple de snifer ethernet



Snifer : analyse d'une trame Ethernet



Adresse destination	Adresse source	Protocole de couche 3	Champs de données (+ Bourrage)	FCS
6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

- 0x0800 : IPv4
- 0x86DD : IPv6
- 0x0806 : ARP
- 0x8035 : RARP
- 0x809B : AppleTalk
- 0x88CD : SERCOS III
- 0x0600 : XNS
- 0x8100 : VLAN

- type de protocole selon
- et pour le protocol transport : (6 -> TCP, 1 -> ICMP, UDP -> 17)

Introduction

Snifer : analyse d'une trame Ethernet

Analyser la trame ethernet suivante :

```
08 00 20 0A 70 66 08 00
20 0A AC 96 08 00 45 00
00 28 A6 F5 00 00 1A 06
75 94 C0 5D 02 01 84 E3
3D 05 00 15 0F 87 9C CB
7E 01 27 E3 EA 01 50 12
10 00 DF 3D 00 00 20 20
20 20 20 20 9B 52 46 43
```

Introduction

Snifer : analyse d'une trame Ethernet

Solution

```
08 00 20 0A 70 66          -> @mac destinataire (constructeur = 080020)
08 00 20 0A AC 96          -> @mac émetteur (même constructeur)
08 00                      -> Type (ici IP). Si < à 1500 c'est une longueur
---------- 46 <= contenu (ici datagramme IP)<= 1500 ----------
4                          -> Version IP (Ipv4)
5                          -> Longueur de l'en-tête (5*32bit = 160bit ou 5*4 octets = 20 octets)
00 00 28 A6 F5 00 00  1A   06   75 94 C0 5D 02 01 84 E3 3D 05 -> en tête
 |  |___|  |___|  |___|  |_|  |_|  |____| |_________| |_________|
||    |      |      |      |    |     |          |              |_ @IP destinataire 132.227.61classe B
||    |      |      |      |    |     |          |_ @IP émetteur 192.92.2.1 classe C [pas dans le même
réseau !]
||    |      |      |      |    |     |_Bloc de contôle d'erreur (sur l'en-tête du datagramme
seulement)
||    |      |      |      |    |_ Protocole (ici TCP)
 |    |      |      |      |_ TTL (ici 1A = 1*16+10=26 routeurs ou secondes)
 |    |      |      |_ Drapeau + Déplacement (0=inutl, 0=DF(fragmentation autorisée) 0=MF (pas
de fragments à suivre, donc dernier fragment) 0000000000000=déplacement soit place du 1er octet
transporté, ici 1er fragment) [Il s'agit d'un datagramme non fragmenté]
 |    |      |_Id du datagramme (numéro quelconque, ne sert que si le datagramme est amené à
être fragmenté )
 |    |_ Longueur totale (ici 28 en hexadécimal vaut 2*16=8 en décimal soit 40 octets)
 |_ pas de qualité de service
---------- contenu = segment TCP d'une longueur de 20 octets (40-20) ----------
```

Solution(suite)

00 15 -> port source, ici 21 donc serveur ftp
0F 87 -> port destination 3975, port quelconque du client
9C CB 7E 01 -> Numéro de séquence (n° du 1er octet transporté émis (tiré au hasard))
27 E3 EA 01 -> Numéro de séquence (n° du 1er octet attendu en réception)
5 -> Longueur de l'en-tête du segment (20 octets) :
on peut donc en déduire que ce segment ne contient pas de données
0 12 = 0000 0001 0010 -> Drapeaux (ici réponse 'ok' d'ouverture de connexion)
|____||| |||_FIN (Clôture de la connexion)
| || |||_SYN (Ouverture (ou réponse d'ouverture) de connexion)
| || ||_RST (réinitialisation de la connexion)
| || |_PSH (Livraison immédiate)
| ||_ACK (accusé de réception)
| |_URG (urgent)
|_6 bits réservés
10 00 -> Taille de la fenêtre, ici 4096 octets. Quantité de données que l'émetteur est autorisé à envoyer sans accusé de réception
DF 3D -> BCE (Bloc de contrôle d'erreur sur le segment entier)

Solution(suite)

```
00 00                          -> Pointeur vers les données urgentes (inutile ici puisqu'il n'y
                                  a pas de données urgents bit URG =0)
------------------------- fin du segement TCP (sans données) ----------------------------------------
---
------------------------- fin des données du datagramme IP ------------------------
20 20 20 20 20 20          -> 6 octets de bourrage pour amener la trame Ethernet à la
                                  longueur MINIMALE autorisée
9B 52 46 43                -> Bloc de contôle d'erreur de la trame Ethernet
------------------------- fin de la trame Ethernet ---------------------------------------------
```

Merci pour votre attention!