

INTRODUCTION À LA SÉCURITÉ INFORMATIQUE SÉANCE 12

Marc-Olivier Killijian

UQAM, CNRS

INF4471

PROGRAMME DE LA SÉANCE

- Chiffrement de disque dur
- Sécurité réseau
 - Rappels réseau, tcp/ip, etc.
 - Attaques (DOS, Spoofing, Hijacking, ...)
 - Défenses (Parefeux, Détection d'intrusion)

CHIFFREMENT DE DISQUE DUR

Marc-Olivier Killijian

UQAM, CNRS

INF4471

DONNÉES AU REPOS

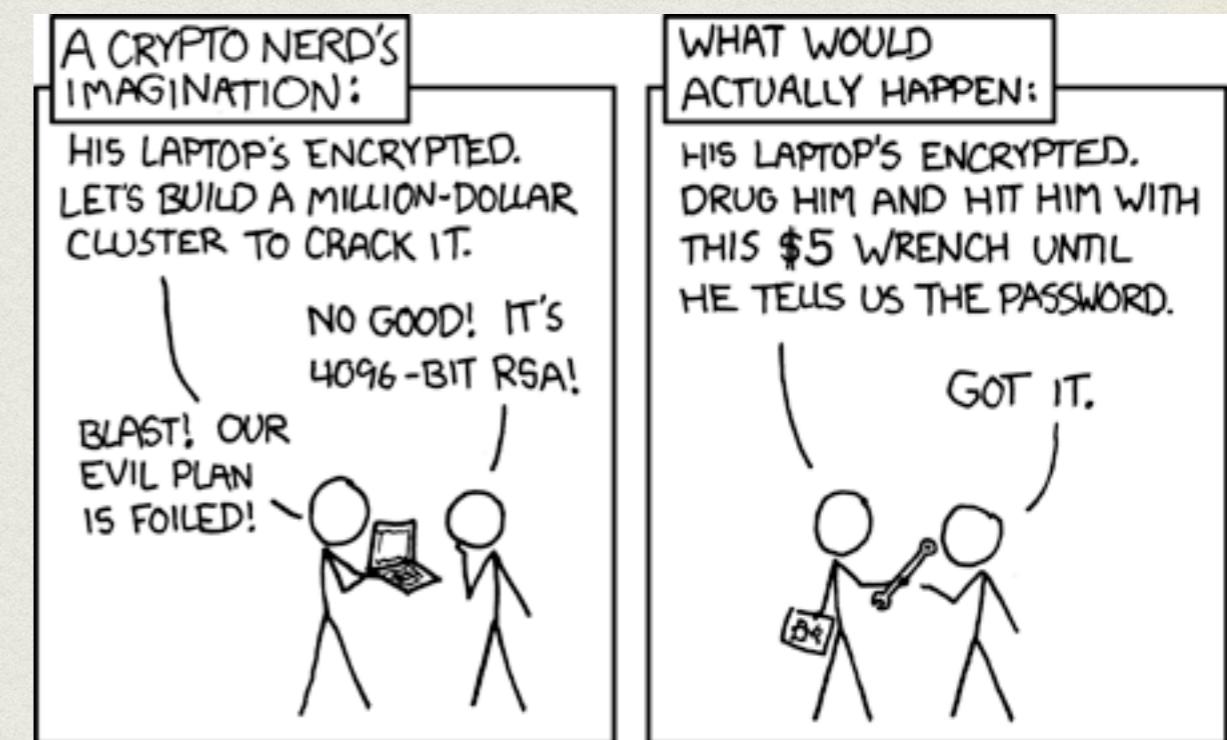
- On parle ici de chiffrer les données au repos (*data-at-rest*)
 - Disques dur, clés, SSD, cartes mémoires, téléphones, backups, bases de données, archives, etc.
- A l'inverse des
 - Données en cours d'utilisation (*in use*) : actives et en changement constant
 - Données en déplacement (*in motion*) : sur le réseau ou en mémoire pendant écriture

PROTÉGER CONTRE

- Accès aux données, à l'ordinateur, en son absence
- Vol ou perte du support (ordinateur, portable, clé, etc.)
- Envoi en réparation
- Mise au rebut
- (Installation de maliciel/keylogger en son absence)

MAIS PAS CONTRE

- Intrusion sur un ordinateur allumé et/ou en ligne
- Accès à un ordinateur allumé ou tout juste éteint (*cold boot*)
- Injonction du gouvernement (ou police) de révéler un mot-de-passe
- Injonction sous la contrainte ...
- Effacement du support



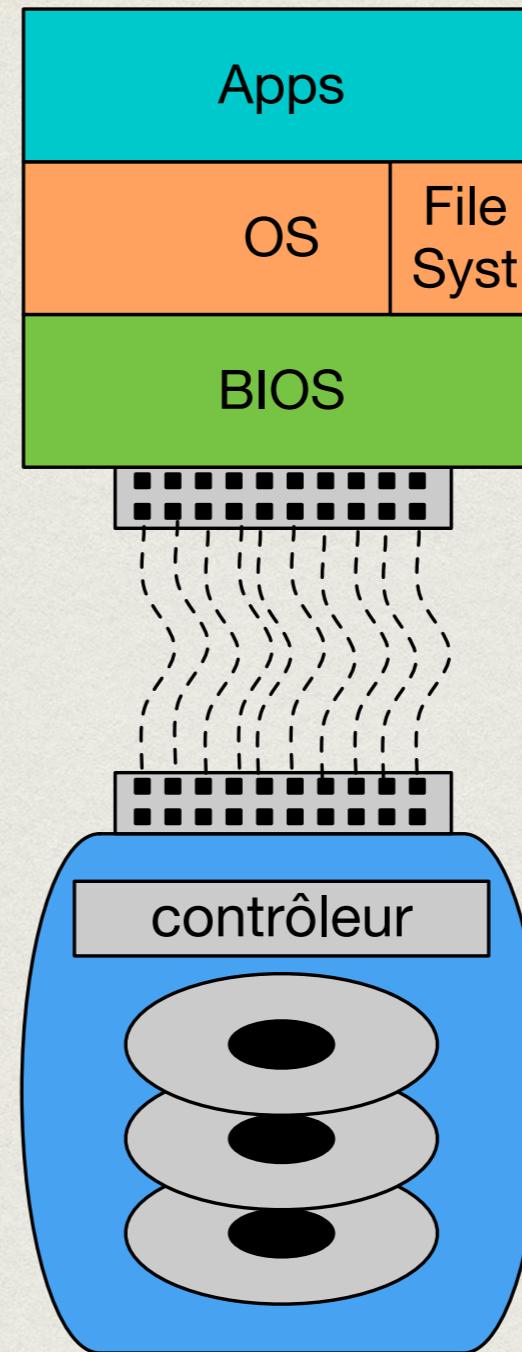
POINTS DE VUE

système de fichiers

couche logique

couche électronique

couche physique



répertoires
fichiers

partitions
blocs

secteurs
cylindres
faces

électrons

...

CHIFFREMENT...

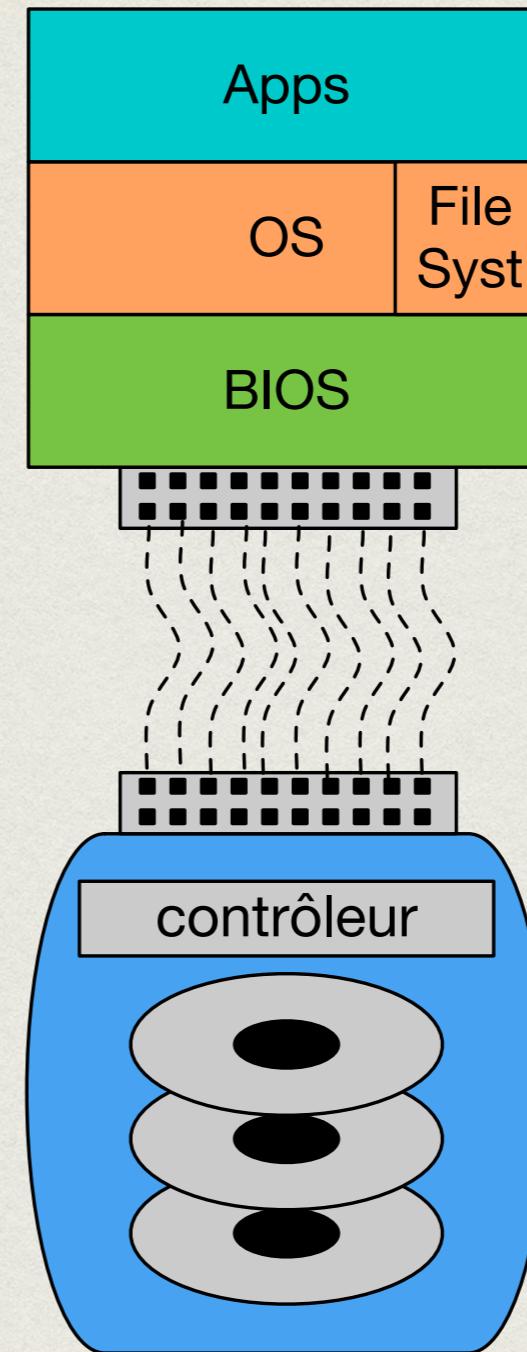
Physique
(FDE)

système de fichiers

couche logique

couche électronique

couche physique



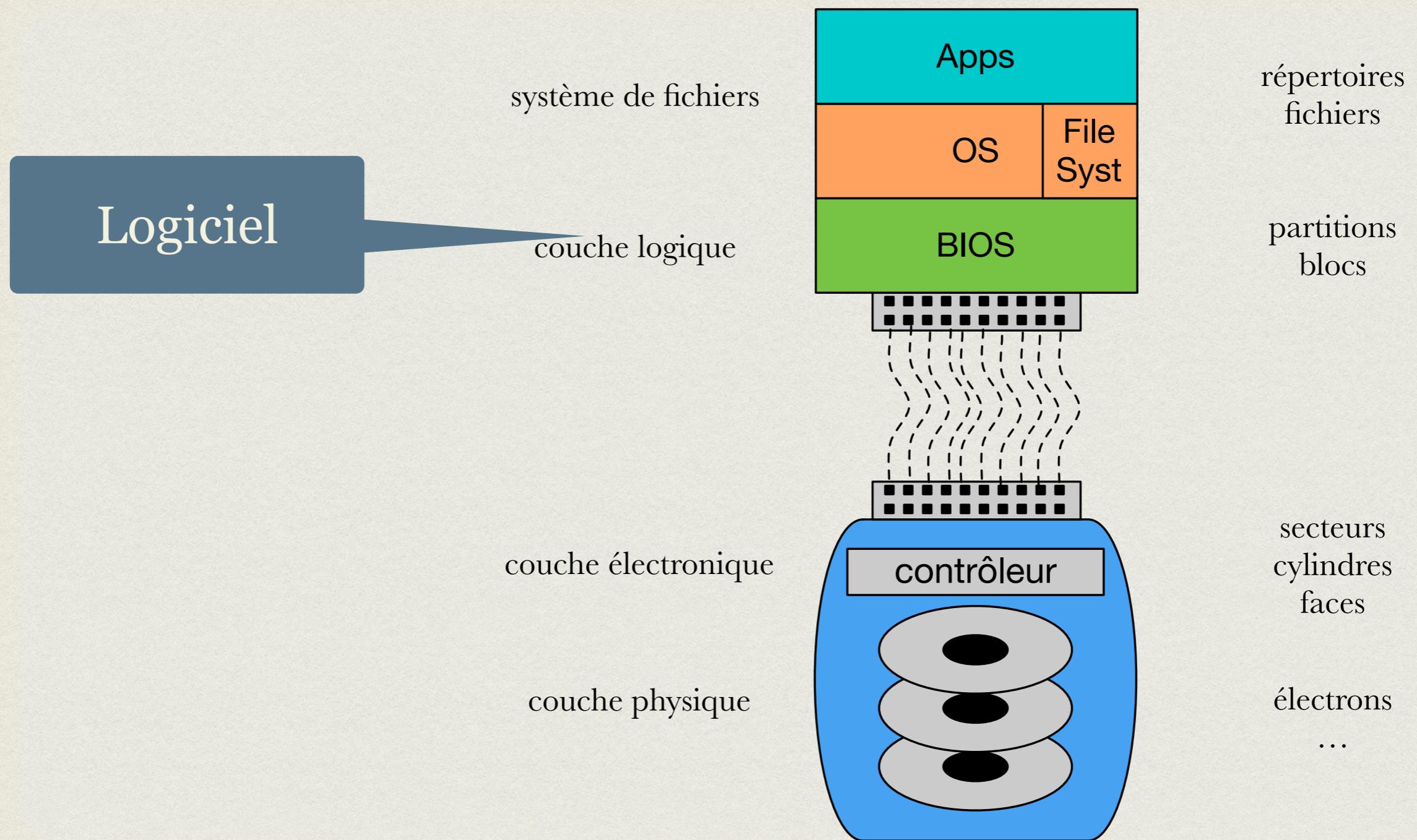
répertoires
fichiers

partitions
blocs

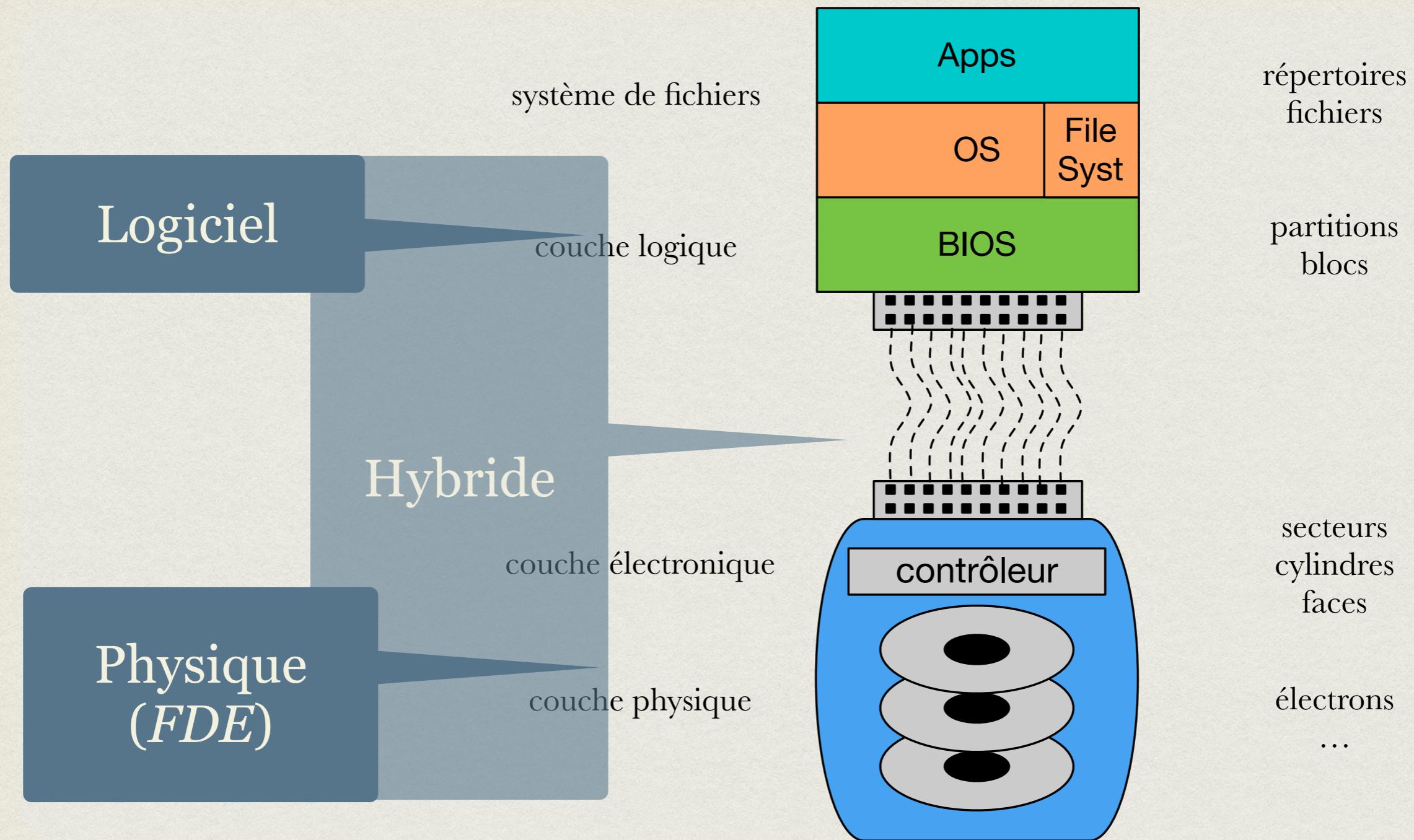
secteurs
cylindres
faces

électrons
...

CHIFFREMENT...



CHIFFREMENT...



PARTIEL

- Sur un DD, où sont les données confidentielles ?
- On pourrait envisager de chiffrer partiellement le DD
 - au niveau système/filesystem en ne chiffrant que les données et en conservant la structure (noms de fichiers, hiérarchie, etc.)
 - par exemple la partition /users
- Autres endroits non chiffrées où résident des données (/swap /tmp etc.)
- Certaines métadonnées peuvent être confidentielles (e.g. fichiers avec noms de clients)

CHIFFREMENT COMPLET

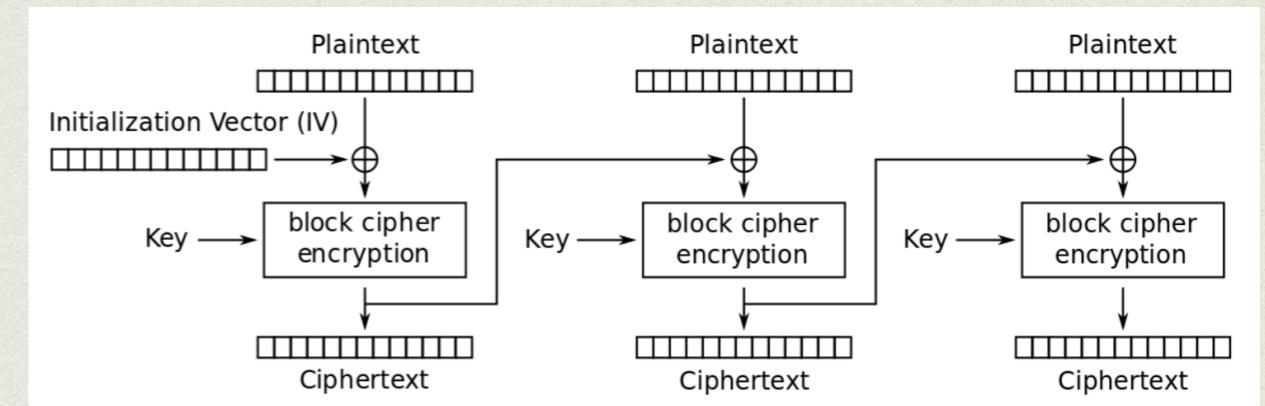
- Plus sûr de chiffrer complètement un disque ou une partition (incluant les métadonnées)
- Possible à différents niveaux
 - Logiciel (filesystem) :
un volume virtuel clair monté à partir d'un volume chiffré
 - Matériel :
le contrôleur de disque gère le chiffrement, une fois en place, l'OS ne voit qu'un volume en clair
 - Hybride :
un logiciel (e.g. BitLocker) utilise des services du contrôleur de disque pour gérer le chiffrement

BONUS: EFFACER UN DISQUE

- Que veut dire effacer une donnée ? (/forensique)
 - Apps: Enlever les données du fichier, réécrire le fichier (click-click-ctrl-S)
 - OS: Enlever le descripteur de fichier de la table du répertoire (rm data.perso)
 - Physique: écrire des 0 (ou des 1) à l'endroit de la donnée ... plusieurs fois ?
 - Disque chiffré: jeter et oublier la clé ! (*Crypto-shredding*)
e.g. OSX « Find My Mac » demande au chip T2 du Mac d'oublier la clé

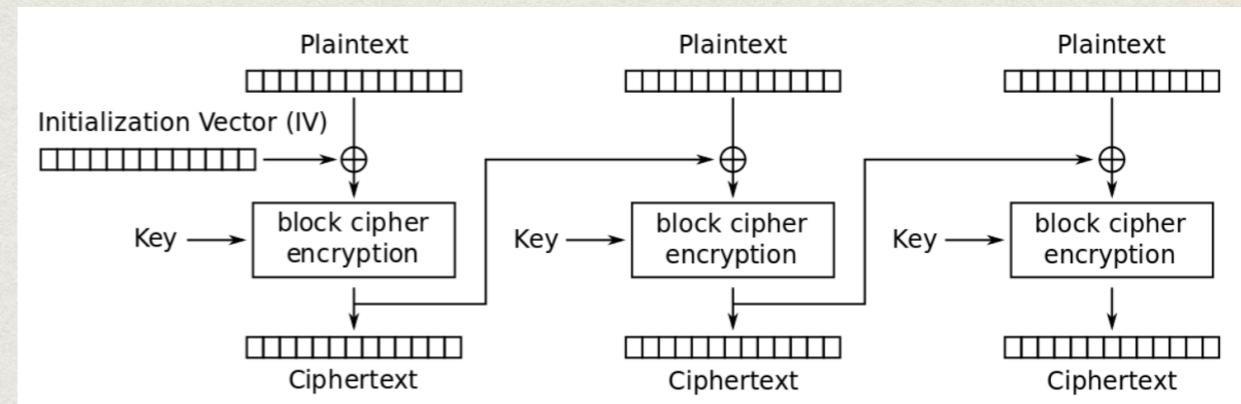
AES-CBC

- $c_i = ENC(c_{i-1} \oplus m_i, k)$
avec $c_{-1} = IV$
- simple, efficace
- mais ...



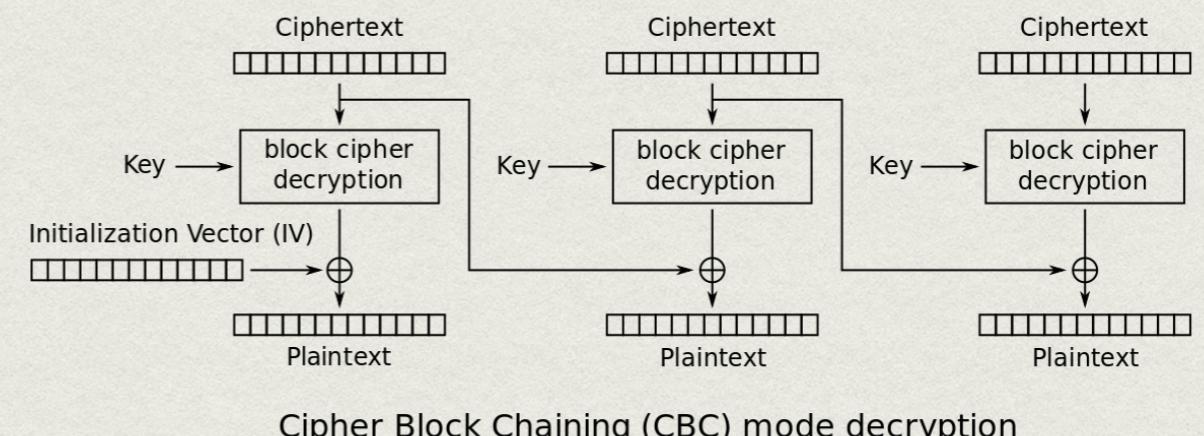
AES-CBC WATERMARKING

- Si IV est prévisible, créer un fichier spécifique qui sera sauvegardé sur plusieurs blocs
 - premiers blocs de chaque secteur b_1 et b_2 (voire plus b_i) tq
$$b_1 \oplus IV_1 = b_2 \oplus IV_2$$
 - donc $ENC_k(b_1, IV_1) = ENC_k(b_2, IV_2)$
 - peut servir de tatouage à un attaquant qui sera capable de détecter la présence du fichier sans connaître la clé de déchiffrement
- Mitigé par CBC-ESSIV où
$$IV = f(\#sector, \text{hash}(k))$$



AES-CBC MALLÉABLE

- « injection de code » CBC
- Adv connaît p_i, c_i, c_{i-1}, x_i
$$p_i = DEC_k(c_i) \oplus c_{i-1}$$
$$\Rightarrow DEC_k(c_i) = c_{i-1} \oplus p_i$$
on veut que $p'_i = x_i$
$$\Rightarrow c'_{i-1} = DEC_k(c_i) \oplus x_i$$
$$= c_{i-1} \oplus p_i \oplus x_i$$
écrire c'_{i-1} pour contrôler p_i

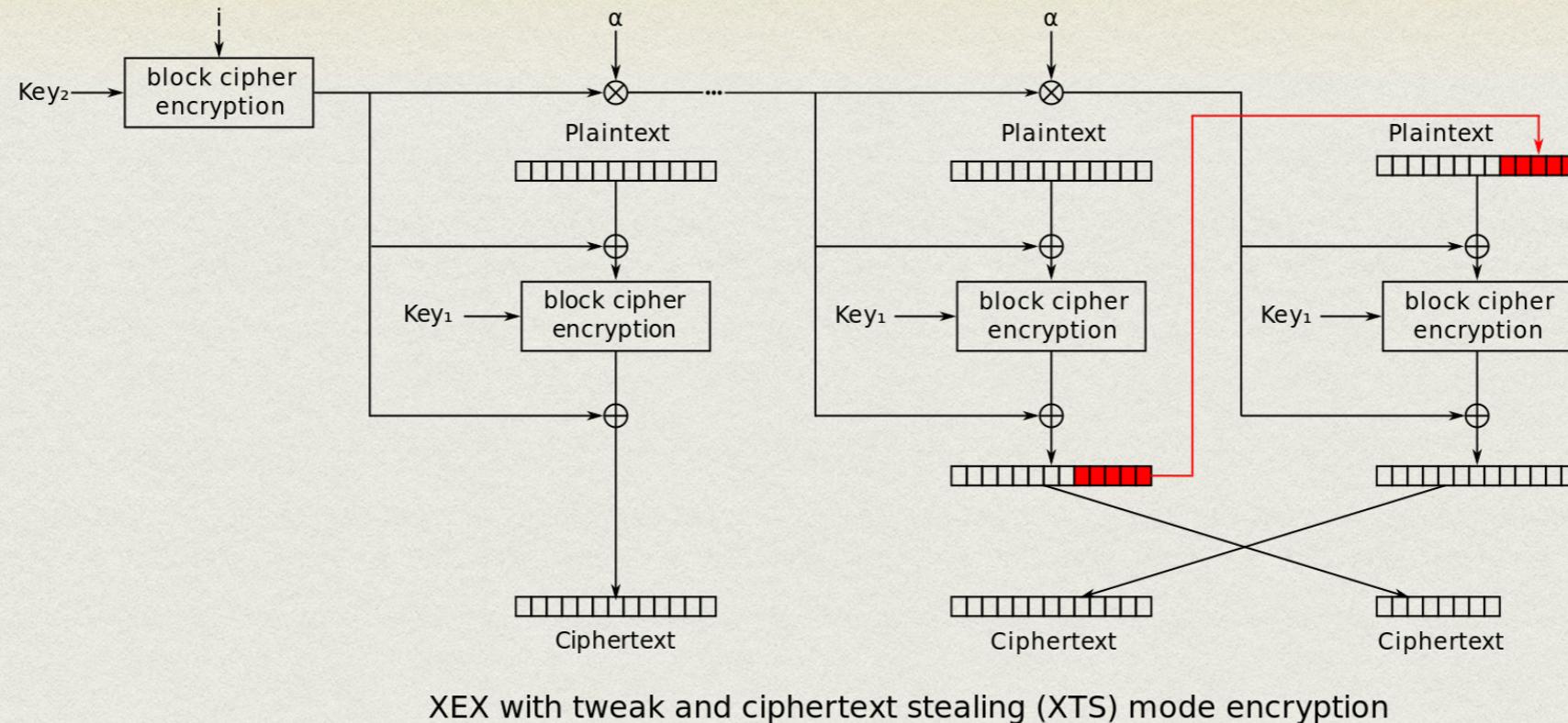


- Peut contrôler 1 bloc sur 2 avec un *jmp* en fin de bloc installation de code arbitraire

LRW, XEX

- Mode Liskov, Rivest, and Wagner (LRW)
 - 2 clés K et F : $x_i = f \otimes i$ et $c_i = \text{ENC}_k(p_i \oplus x_i) \oplus x_i$
 - Mais fuite détection d'écriture : si 1 bloc/secteur est modifié alors 1 chiffré change
- Mode XEX : α un générateur $GF(2^{128})/x = 2$
 $X_{i,j} = \text{ENC}_k(i) \otimes \alpha^j$ et $c_i = \text{ENC}_k(p_{i,j} \oplus X_{i,j}) \oplus X_{i,j}$
avec i le secteur et j le numéro du bloc
- Implémentation matérielle rapide et compacte
- Non sécuritaire avec certains paramètres [Minematsu 2006]

XEX+CTS=XTS



- Standard NIST actuel (SP800-38E) taille de bloc/secteur limitée à 2^{20} blocs AES
- Utilisé dans la majorité des solutions SW et hybrides actuelles : BitLocker, FileVault2, dm_crypt
- Attention, une forme de malléabilité subsiste → utiliser des codes détecteurs d'erreurs au niveau filesystem

ATTENTION

- Comme d'habitude rien n'est jamais totalement sécurisé
- Les fuites *Equation Group* ont montré que la NSA avait des backdoor qui permet de flasher les firmwares de DD
- Certaines implémentations HW sont insécuré et certaines solutions hybride (BitLocker) se reposent sur le HW [Meyer & van Gasten 2018]
- Depuis octobre 2020, sécurité du Apple T2 compromise (besoin d'un accès physique)
- ...

FORENSIQUE ANTI DISK ENCRYPTION

- Retrouver la clé dans les fichiers de recouvrement, d'hibernation, le gestionnaire de mots de passe, etc.
- Brute forcer la clé
- Retrouver des copies des données non-chiffrées dans des backups, emails, fichier de swap, etc.
- Installer un keylogger matériel et intercepter le mdp ou la clé
- Extraire la clé de la RAM avec une *cold boot attack* ou une *DMA attack*
 - Anti-*coldboot* : stocker la clé dans les registres et pas dans la RAM

SÉCURITÉ RÉSEAU

Marc-Olivier Killijian
UQAM, CNRS
INF4471

RAPPELS TCP/IP

Marc-Olivier Killijian
UQAM, CNRS
INF4471

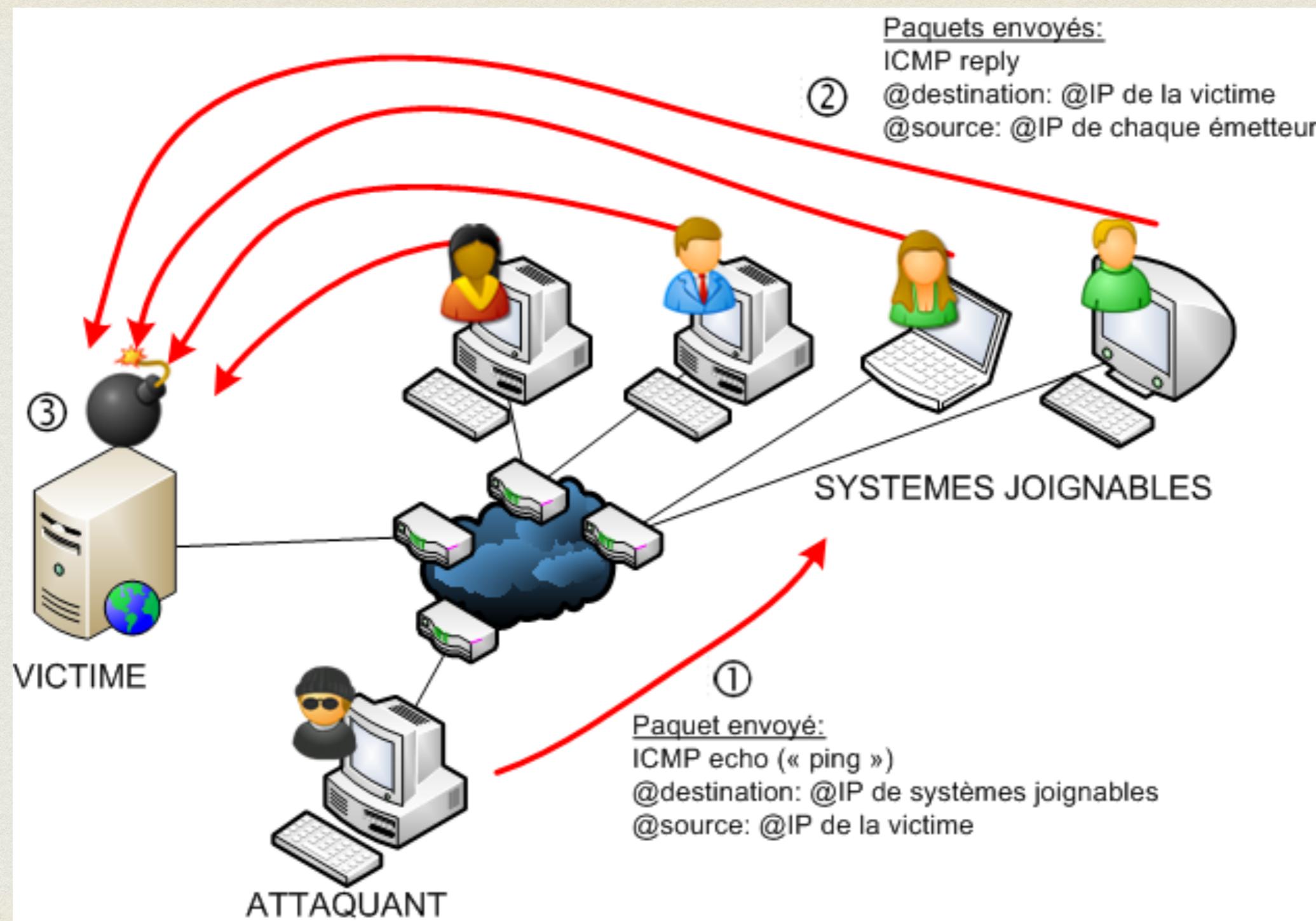
PRÉAMBULE

TCP/IP	ISO	Protocoles
Application	Application Presentation Session	SMTP, HTTP
Transport	Transport	TCP, UDP
Internet	Network	IP, X25 PLP
Network Access	Data Link Physique	Ethernet, PPP, X25 ALPB

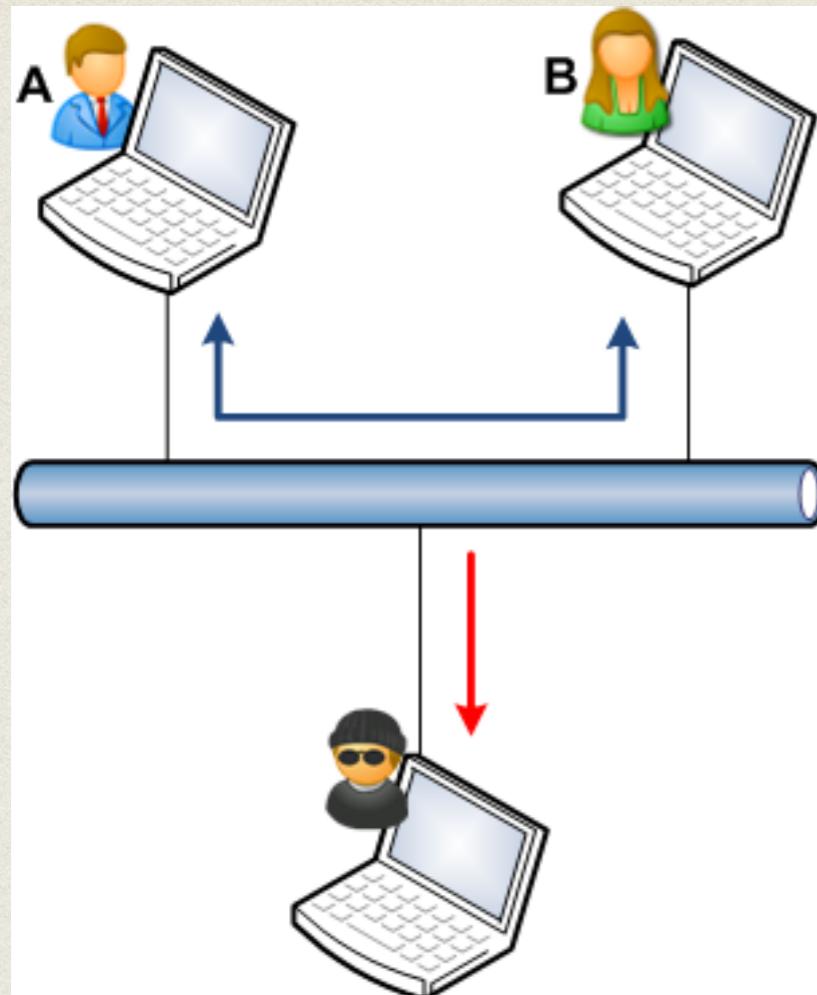
PRÉAMBULE

- A leur création, IP et les protocoles associés (TCP, UDP, ICMP)
 - n'ont pas pris en compte la sécurité
 - le concept de sécurité n'existe pas
 - aucun mécanisme de sécurité dans ces protocoles
- Exemples de faiblesses (pas toujours applicables)
 - Pas d'authentification de l'émetteur d'un message (usurpation d'IP possible)
 - Pas de chiffrement des données (écoute possible)
 - Le routage peut être modifié en route (pb disponibilité et confidentialité)

EX: ATTAQUE PAR RÉFLEXION

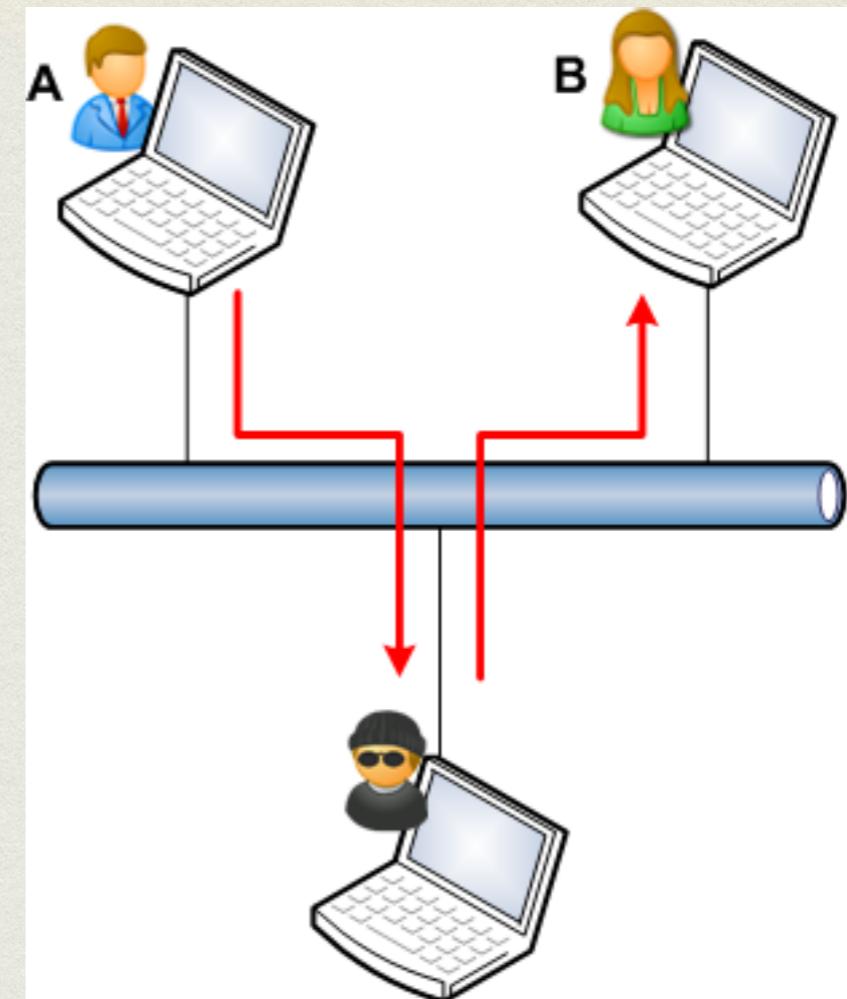


EX: ÉCOUTE



Ecoute passive

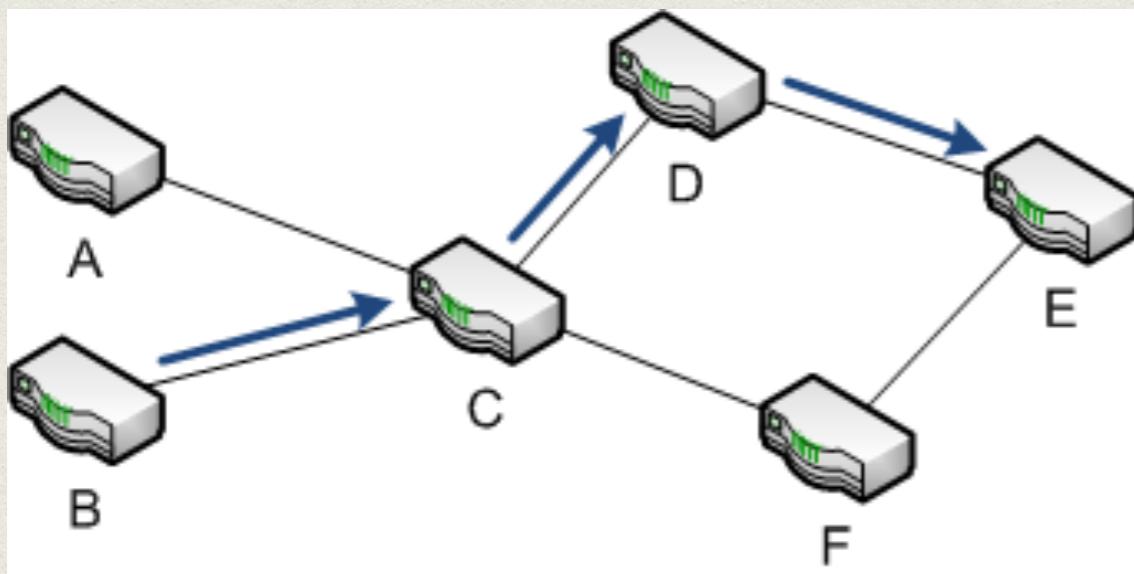
L'attaquant est en mesure d'écouter les conversations entre A et B (atteinte à la **confidentialité** des échanges).



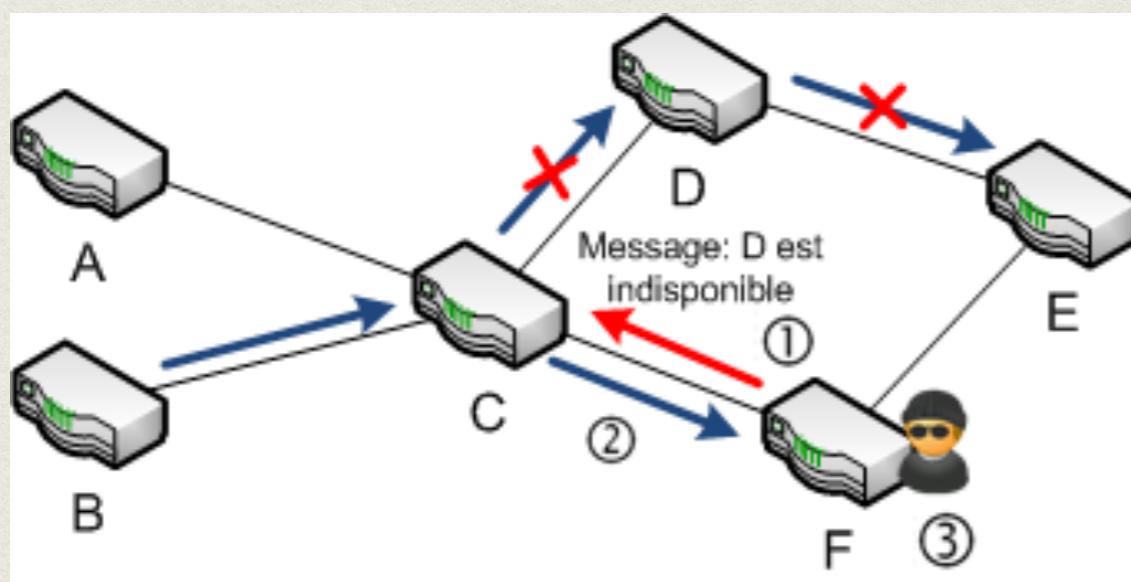
Ecoute active

L'attaquant est en mesure de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent (atteinte à la **confidentialité** et à l'**intégrité** des échanges).

EX: MODIFICATION DU ROUTAGE



Chaque routeur possède une table de routage qui indique vers quel routeur voisin transmettre les datagrammes. Cette table peut être mise à jour dynamiquement en fonction des événements réseaux (protocoles BGP, RIP, OSPF, etc.).



But de l'attaque : **dérouter les paquets** à destination du réseau E, vers le réseau F maîtrisé par l'attaquant.

Méthode :

- ① L'attaquant utilise une faiblesse du protocole de routage pour indiquer au routeur C que le routeur D est indisponible, et que le routeur F peut router les paquets vers E ;
- ② le routeur C transfère donc à F les paquets pour E, afin qu'ils puissent être routés à destination ;
- ③ Selon le but visé par l'attaquant, celui-ci peut décider de router ou non les paquets vers E.

RAPPELS RÉSEAU

Marc-Olivier Killijian

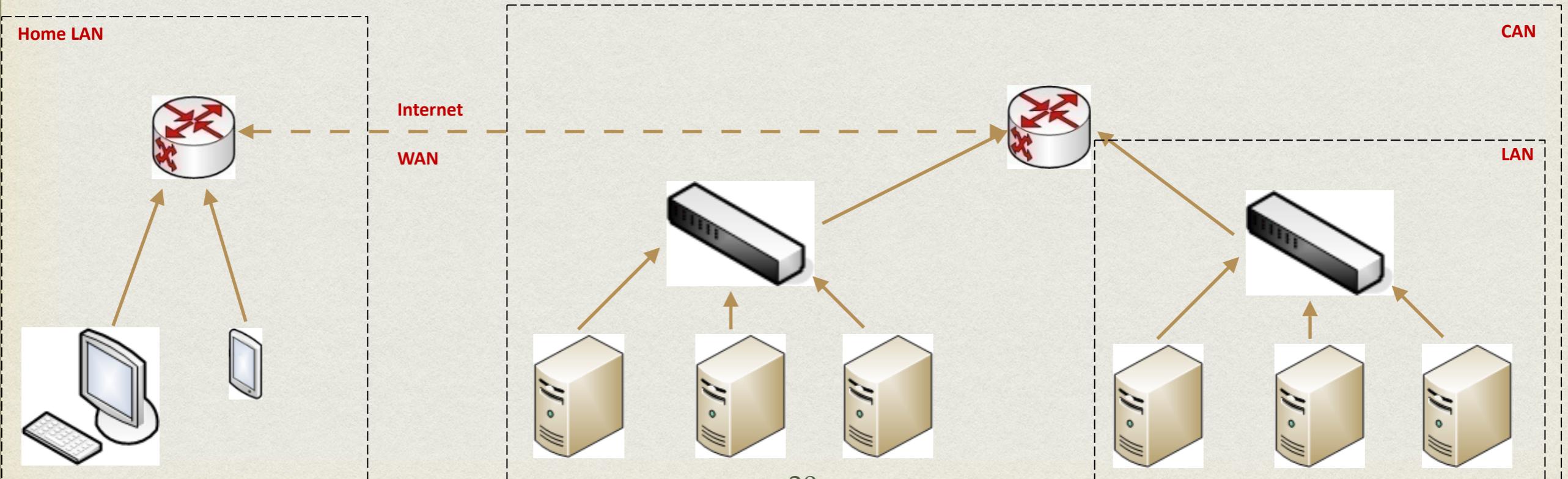
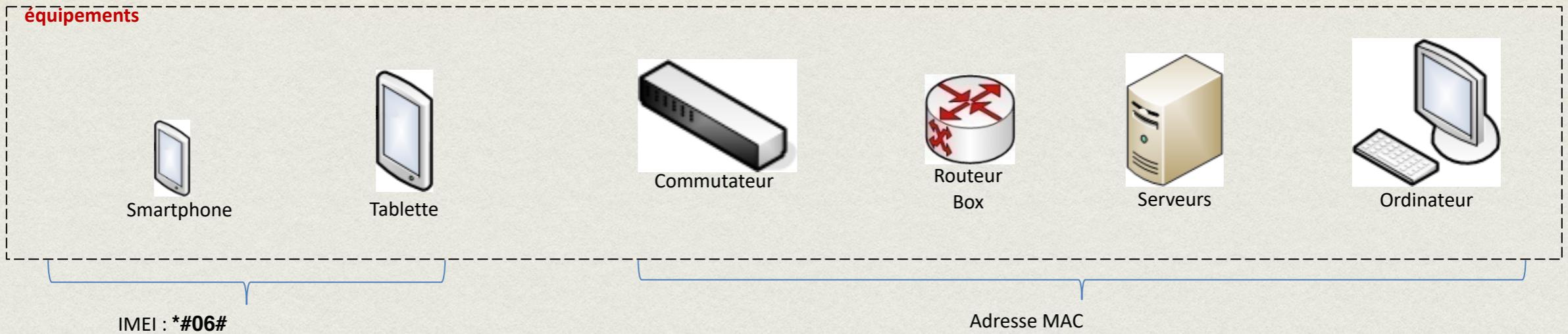
UQAM, CNRS

INF4471

TYPES DE RÉSEAUX

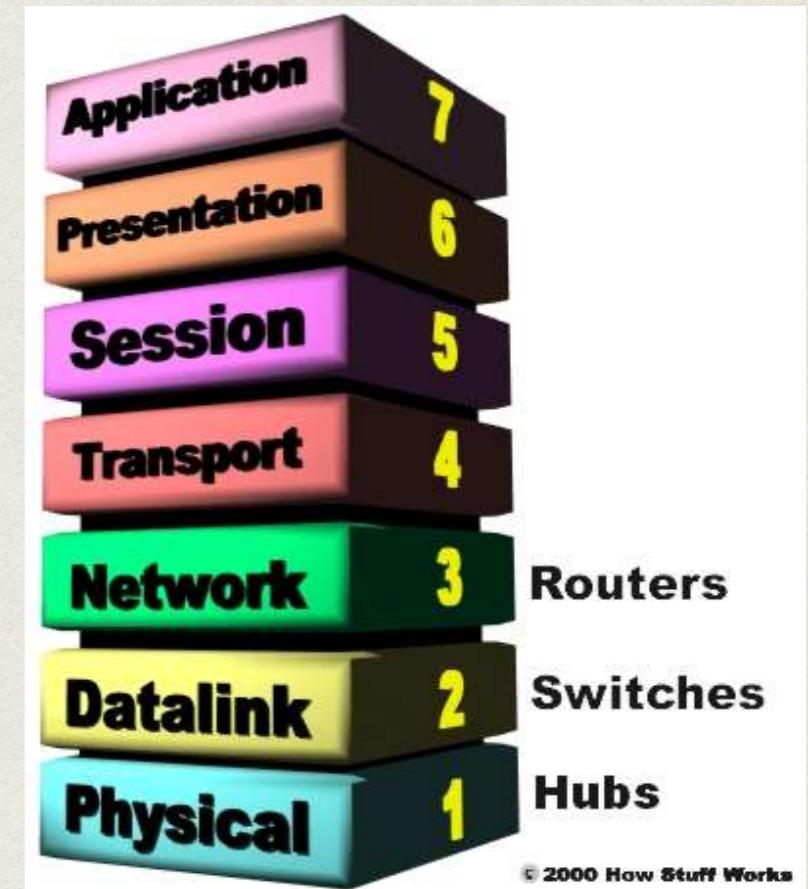
- BAN (Body Area Network) : réseau composé de télé transmetteur utilisé dans le domaine de la santé
- PAN (Personal Area Network) : réseau centré autour d'une personne interconnectant ordinateur, téléphone, tablette, voiture... (moins de 10m)
- WPAN (Wireless PAN) : réseau PAN sans fil utilisant des technologies telles que : IrDA, ZigBee, Bluetooth, Wireless USB
- LAN (Local Area Network) : Réseau local interconnectant plusieurs périphériques et permettant l'échange d'informations entre plusieurs individus
- MAN (Metropolitan Area Network) : réseau plus large qu'un LAN et étendu par exemple sur une ville
- CAN (Campus Area Network) : réseau s'étendant sur plusieurs LAN, et de la taille d'une université
- WAN (Wide Area Network) : réseau d'une étendue nationale ou internationale. Exemple : Internet.

INTERNET



HUB, SWITCH, ROUTER

- Hub : connecte les segments d'un LAN - broadcast des paquets reçus sur tous ses ports - bande passante partagée
- Switch : connecte les segments d'un LAN - filtre (@MAC) et transmet les paquets entre les segments
- Router : interconnecte 2 LANs ou 1 LAN et un ISP - localisé à des passerelles - détermine la meilleure route (tables de routage) - communiquent avec ICMP



SNIFFING

Marc-Olivier Killijian

UQAM, CNRS

INF4471 A2O

CAPTURE RÉSEAU

- Nombreux protocoles avec authentification en clair
 - POP, FTP, Telnet, HTTP, etc.
- Ecouter le trafic sur un réseau permet d'obtenir de nombreuses données, dont login/password
- Avec ces identifiants, un attaquant peut accéder à une machine distance et répéter l'opération ...

EX: FTP

The screenshot shows a Wireshark capture window titled "eth1 [Wireshark 1.6.7]". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. A filter bar at the top has a "Filter:" input field, an "Expression..." button, a "Clear" button, and an "Apply" button. The main pane displays a list of network frames. Frame 13 is highlighted in orange and expanded below. The expanded view shows the raw hex and ASCII data for the frame.

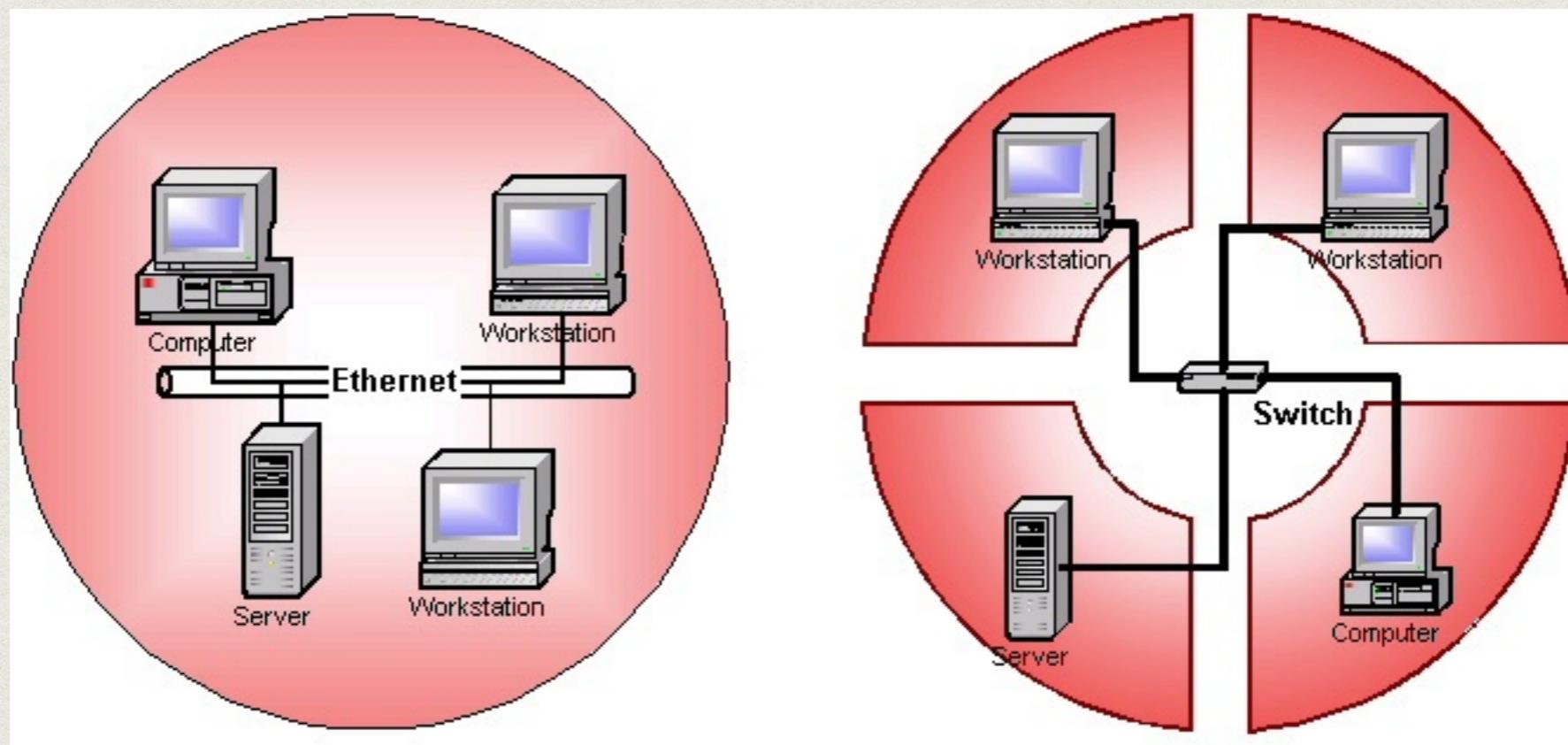
No.	Time	Source	Destination	Protocol	Length	Info
8	0.008705	192.168.1.22	212.27.63.3	TCP	74	38834 > ftp [SYN] Seq=1416128761 Win=1
9	0.036853	212.27.63.3	192.168.1.22	TCP	60	ftp > 38834 [SYN, ACK] Seq=801175440 A
10	0.036897	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128762 Ack=8
11	0.062993	212.27.63.3	192.168.1.22	FTP	140	Response: 220 Serveur de mise a jour d
12	0.063054	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128762 Ack=8
13	3.292595	192.168.1.22	212.27.63.3	FTP	74	Request: USER gildas.avoine
14	3.319677	212.27.63.3	192.168.1.22	TCP	60	ftp > 38834 [ACK] Seq=801175527 Ack=14
15	3.326153	212.27.63.3	192.168.1.22	FTP	96	Response: 331 Password required for gi
16	3.326259	192.168.1.22	212.27.63.3	TCP	54	38834 > ftp [ACK] Seq=1416128782 Ack=8
17	5.462989	b8:26:6c:07:d5:b4	Broadcast	ARP	60	Who has 192.168.1.11? Tell 192.168.1.
18	5.511446	b8:26:6c:07:d5:b4	Broadcast	ARP	60	Who has 192.168.1.15? Tell 192.168.1.

► Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Hex	Dec	ASCII
0000	b8 26 6c 07 d5 b4 d4 be	.&l..... .]....E.
0010	00 3c 3d d0 40 00 40 06	.<=@@. '.....
0020	27 ff c0 a8 01 16 d4 1b	?.....Th h./...P.
0030	3f 03 97 b2 00 15 54 68	9.....US ER gilda
0040	68 fa 2f c0 f7 e7 50 18	s.avoine ..
0050	45 52 20 67 69 6c 64 61	
0060	0d 0a	

SWITCH VS HUB

- Un switch limite la capture réseau par isolation



RÉSEAUX SANS-FIL

- Sans-fil = broadcast



CONCLUSION

- Ecouter un réseau est facile et difficilement détectable
- Ecouter un réseau sans autorisation de le faire est puni par la loi
- Chiffrer ses communications est hautement recommandé
- Utiliser Wireshark est pratique pour étudier ce qu'il se passe dans le réseau

DÉNI DE SERVICE -DOS

Marc-Olivier Killijian

UQAM, CNRS

INF4471

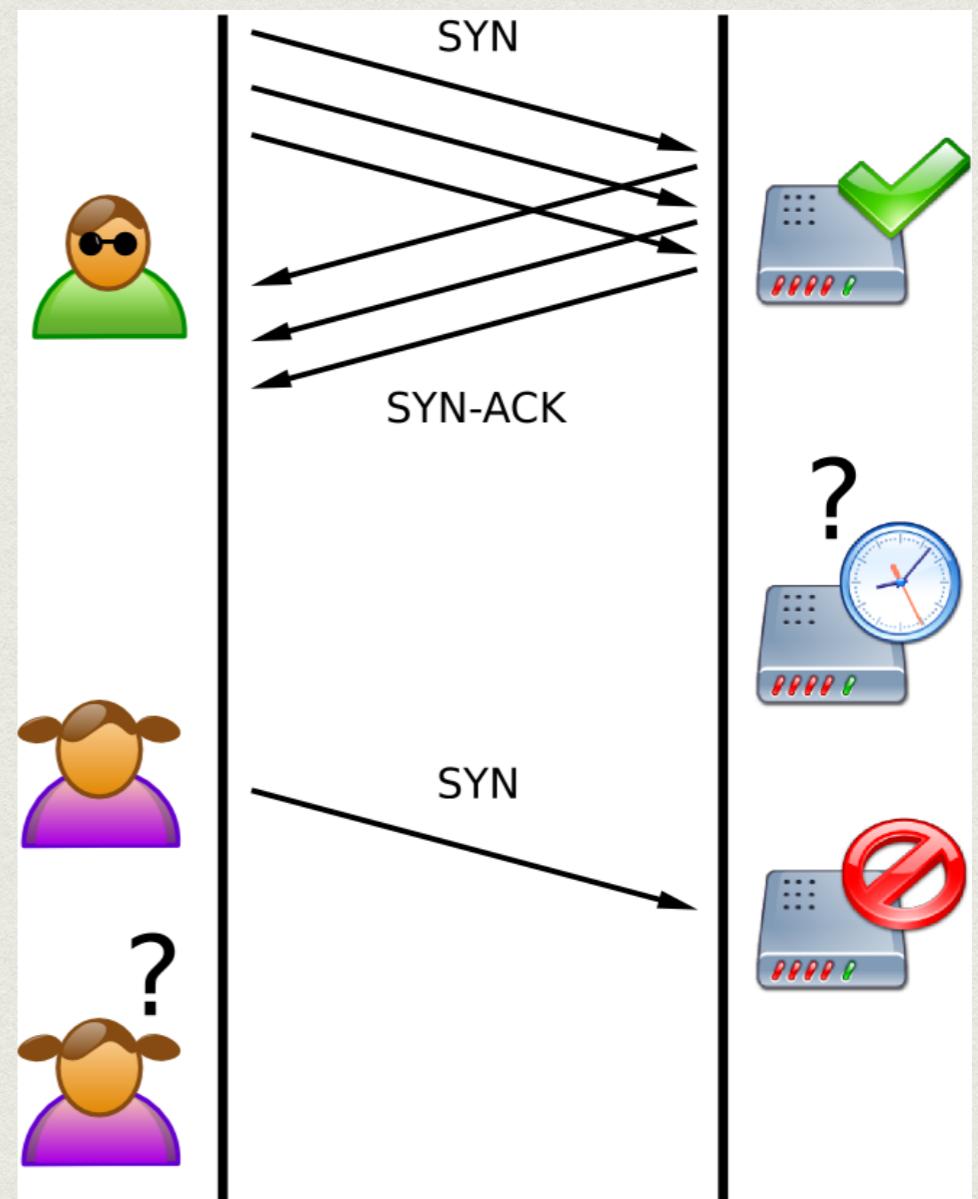
HISTORIQUEMENT

- Ping of death : parmi les premières attaque DOS
 - Unix, Linux, Mac, imprimantes et routeurs vulnérables jusqu'en 1997
 - Taille des paquets ping : 64 octets (84 avec header)
 - Envoyer des paquets IP fragmentés > 64ko
 - Mènes à différents problèmes (crash, etc.)
- Vérifier la taille des données (buffer overflows) et s'attendre à des comportements non spécifiés
- Plus d'infos : [ici](#)

INONDATIONS SYN

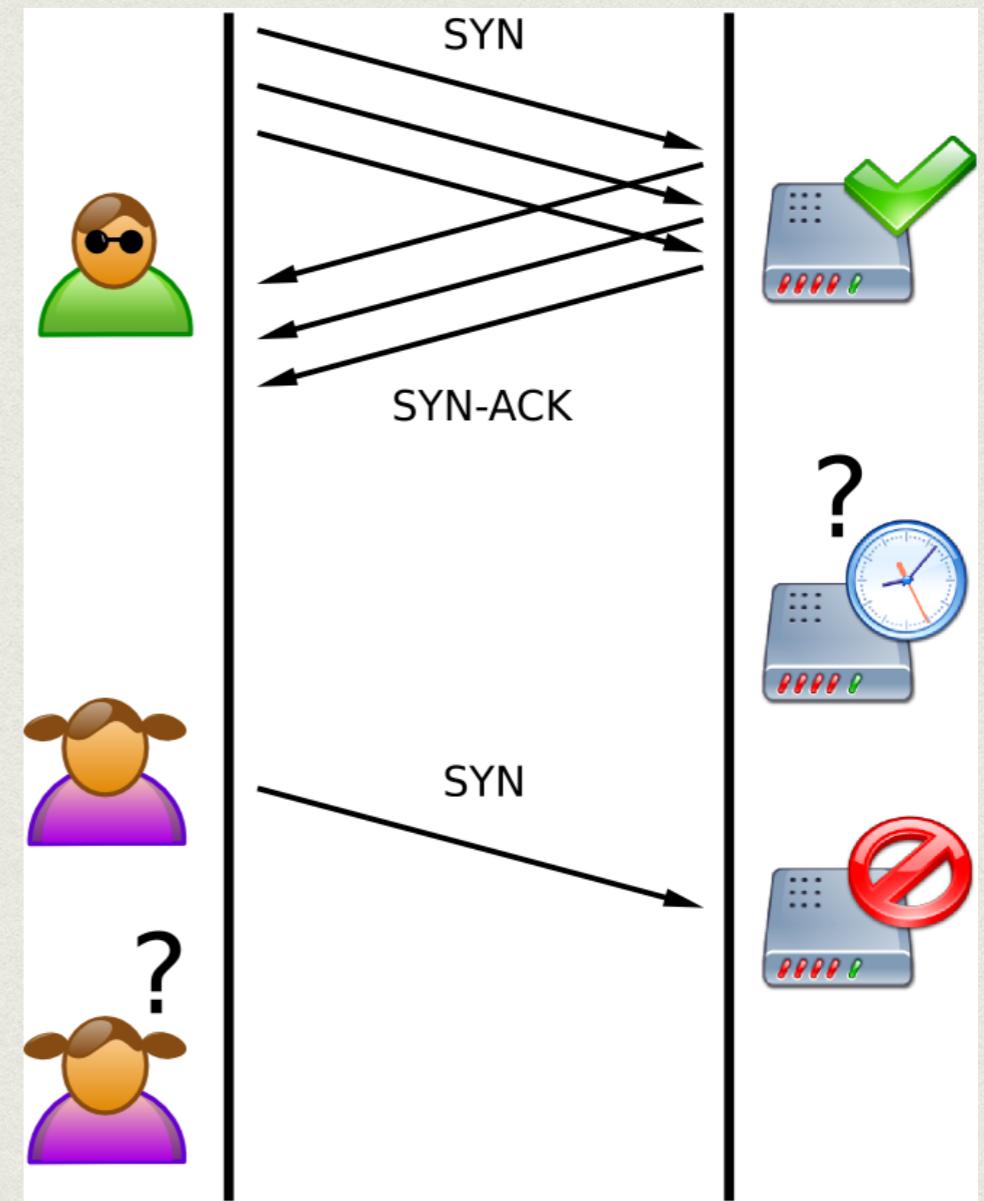
- Sur réception d'un paquet SYN

- Allocation des ressources nécessaires à l'établissement d'une connexion TCP
- File de connexions « demi-ouvertes » jusqu'à réponse au SYN ACK
- Attaquant: abuser des requêtes SYN sans réponse au STN ACK
 - Faire déborder la file des connexions
 - Fausse adresse source pour rester anonyme
- File pleine, le serveur n'accepte plus de connexions



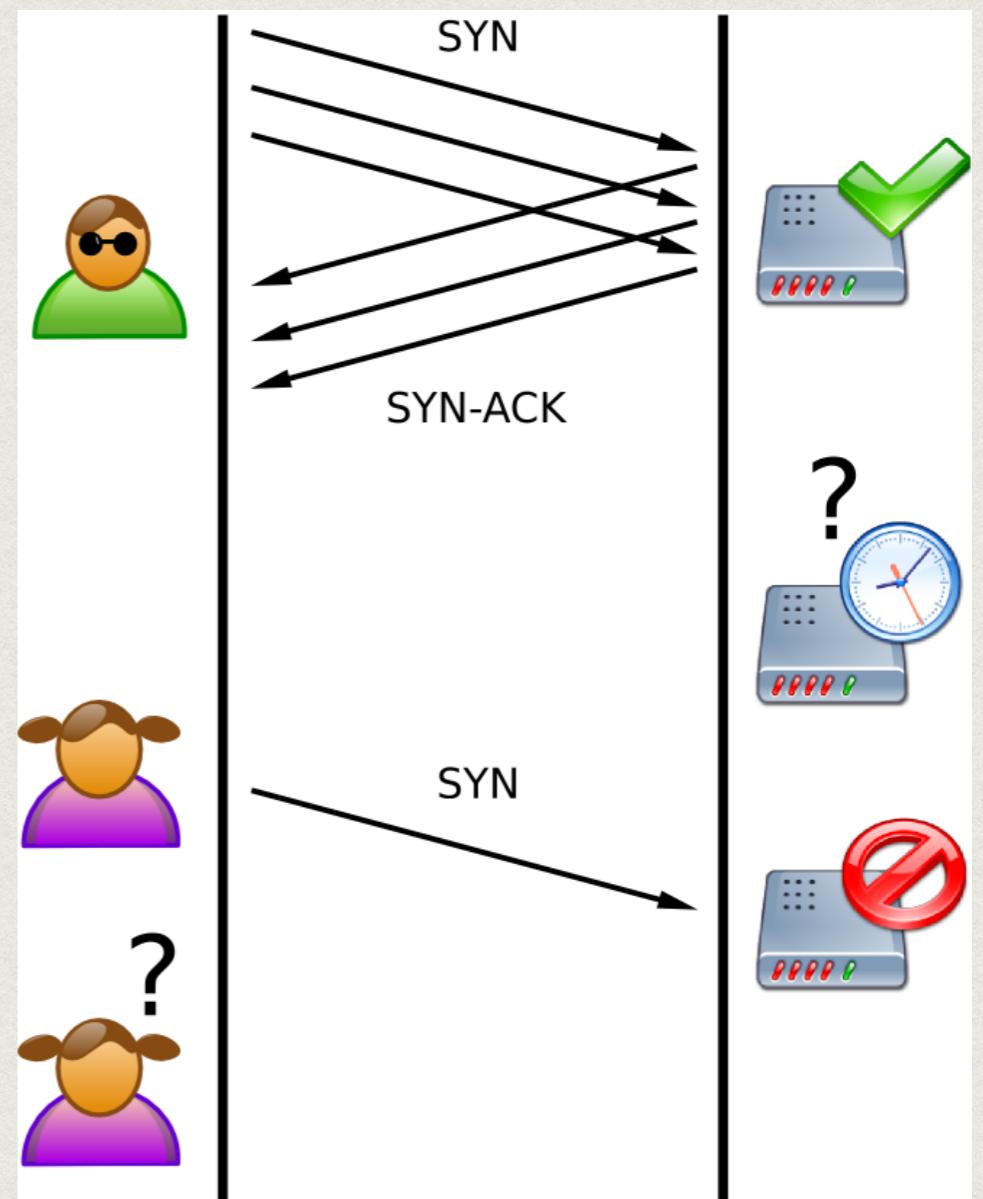
ANTI-INONDATIONS SYN

- Augmenter la taille de la file
- Réduire la durée d'attente du ACK
- Abandonner le plus vieux SYN de la file
- Filtrer les IP des requêtes
- SYN-Cache : file indexée par IP/Port



SYN COOKIES

- Objectif : un protocole sans mémoire (cf. HTTP cookies)
- Lorsque la file pleine, le serveur passe en mode SYN-Cookies
- Sur réception d'un SYN
 - Renvoi d'un SYN/ACK qui contient un cookie
 - Effacement du SYN de la file
- Sur réception d'un ACK
 - contient un cookie valide ? Oui -> ok
- Cookie = $\text{time} \% 32 \mid \text{état-file} \mid \text{signature(t,source/dest IP/port)}$

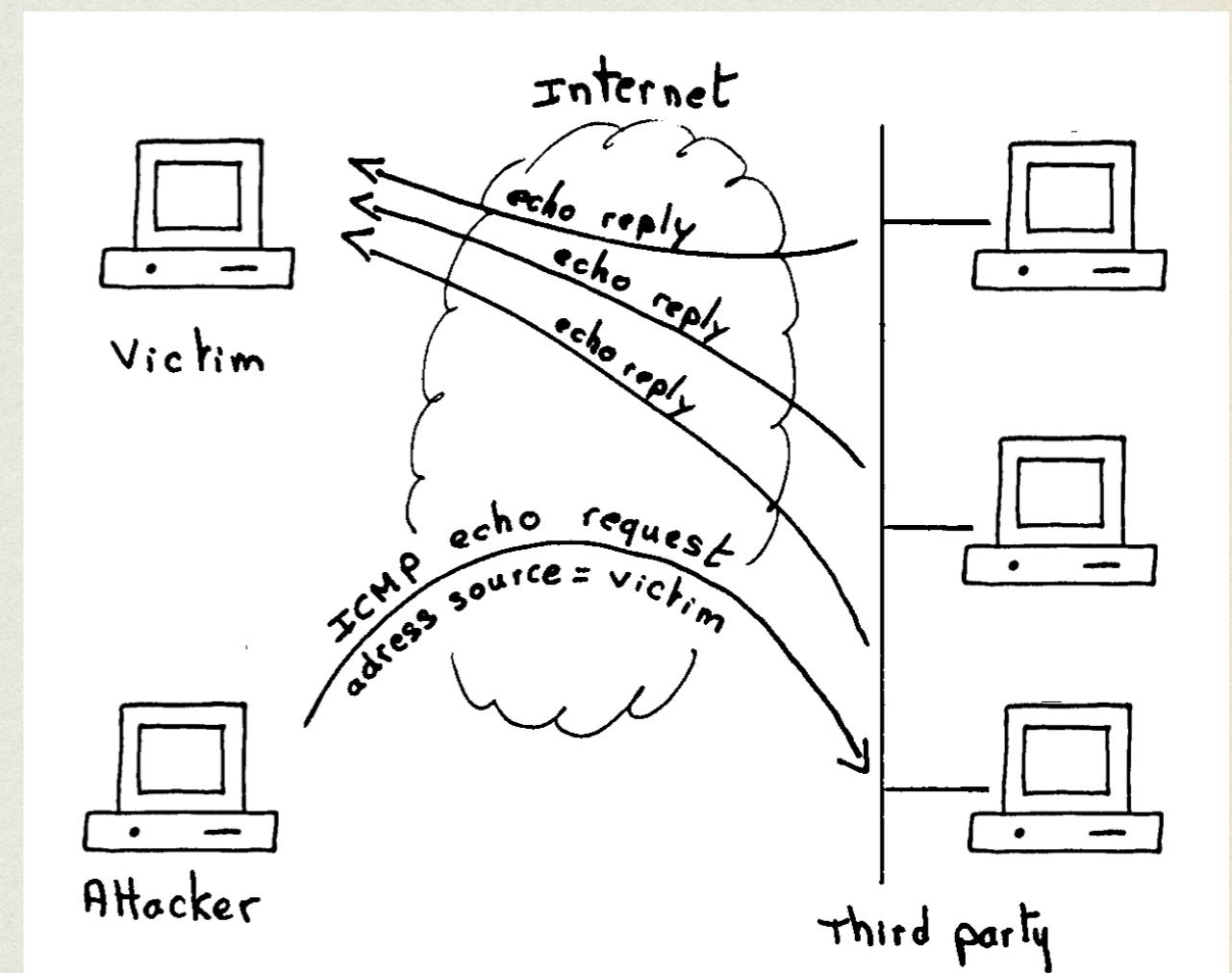


FAMINE DHCP

- DHCP : un protocole de distribution d'adresse IP dans un réseau
- DHCP Starvation
 - Inondation du serveur DHCP avec des requêtes DHCP
 - Provenant d'adresses MAC contrefaites
 - Réserve d'adresses IP du serveur épuisée
 - Clients légitimes ne peuvent plus se connecter au réseau

ATTAQUE SCHTROUMPH

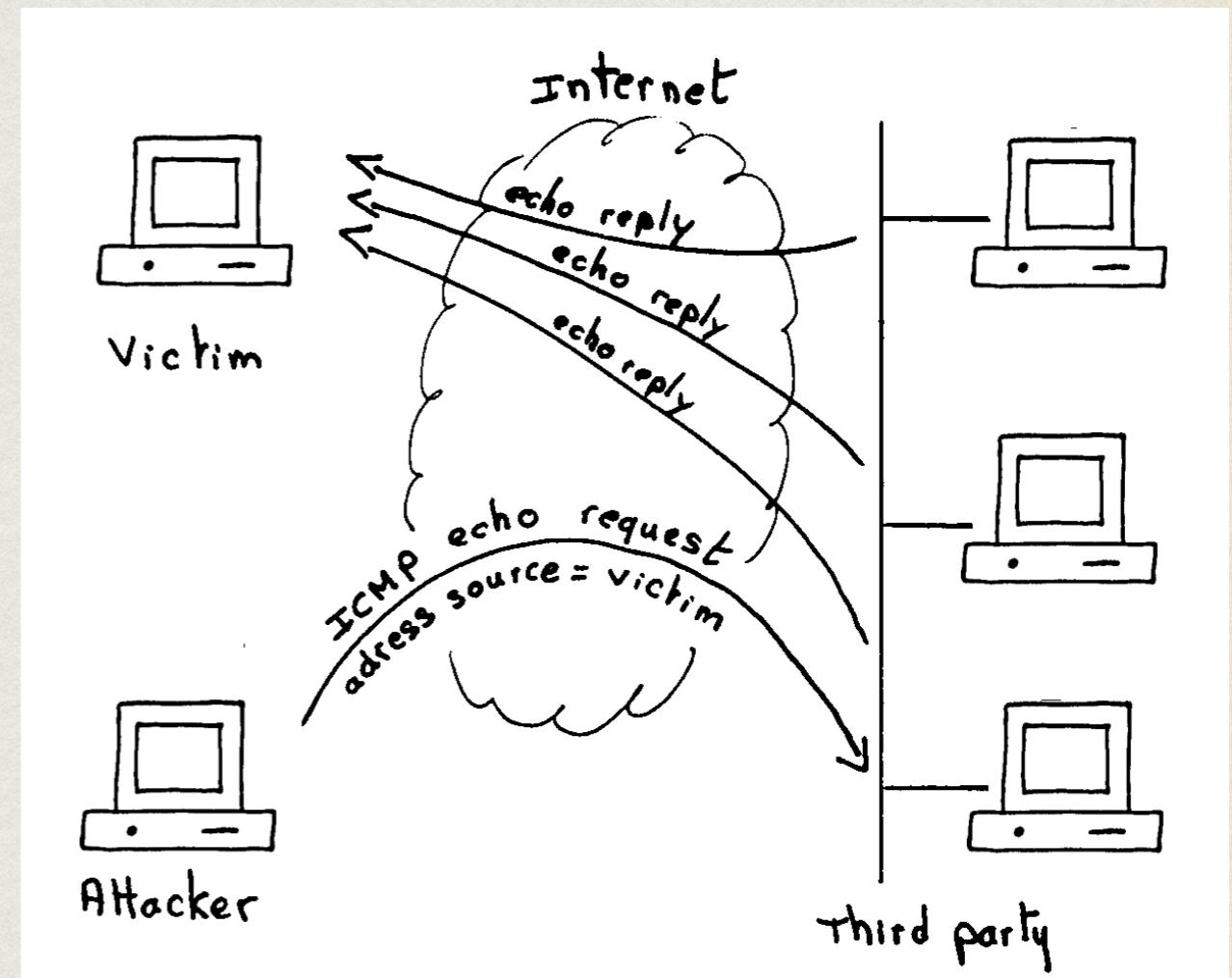
- Smurf attack : étouffer la cible grâce à des amplificateurs de trafic
 - Typiquement : ICMP echo-request (ping)
 - Envoi d'un paquet ping avec la cible comme source
 - La machine « pingée » envoie sa réponse à la source
 - Si le paquet est envoyé à une adresse de broadcast, toutes les machines du réseau répondent à la cible



ANTI-ATTAQUE SCHTROUMPH

- Règles élémentaires

- ne pas propager des requêtes broadcastées
- ne pas répondre à des broadcasts
- attention aux applications où la réponse est bien plus grosses que la requête



CONCLUSION

- Les attaques DOS sont techniquement simple et efficaces
- A la base des attaques DDOS
 - DOS à partir d'un réseau de machines (botnet)
 - Louer un botnet est peu dispendieux (e.g. 5000 noeuds/semaine pour 400\$)
- Mais tout cela est puni par la loi !

USURPATION D'IDENTITÉ SPOOFING

Marc-Olivier Killijian

UQAM, CNRS

INF4471

IP SPOOFING

- L'**adresse IP source** est parfois utilisée comme **authentifiant**
 - Routeurs et pare-feux filtrent les paquets en fonction de cette adresse
 - Certains programmes (rlogin, rsh) autorisent certaines IP sources à se connecter **sans authentification**
- Il est facile de forger l'adresse source d'un paquet et d'**abuser la confiance** de cette source (en particulier pour des protocoles basés sur UDP)
- La réponse d'un paquet à la source forgée est envoyée à cette adresse

DNS SPOOFING (UDP)

- Un utilisateur envoie une **requête DNS** à un serveur DNS local
- L'attaquant renvoie une **réponse DNS** plus rapidement que le serveur
 - Il contrôle donc où le client va aller se connecter
 - Ex: REQ(www.desjardins.com)
REP(192.66.66.66=www.mon_faux_site_desjardins.lu)
- DNS est essentiellement basé sur UDP

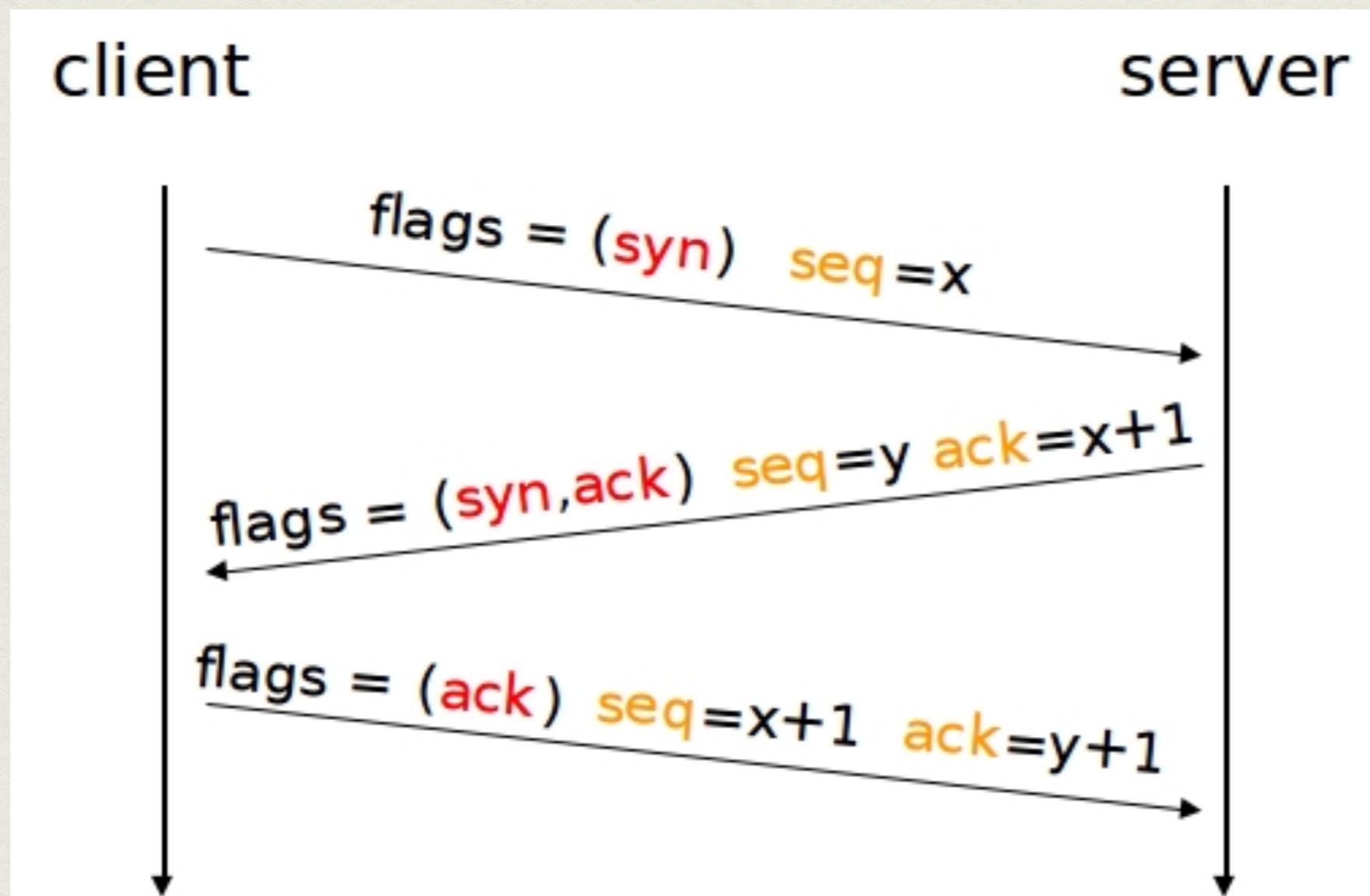
DNS CACHE POISONING (UDP)

- L'attaquant envoie une **requête DNS** à un serveur **DNS local**
- Les serveur DNS local interroge son **serveur DNS maître**
- L'attaquant **usurpe l'identité du serveur maître** et donne une **réponse forgée**
 - Nécessite de **deviner l'identifiant de la requête** du serveur local (brute-forcer 2^{16} possibilités)
 - Corrigé en **augmentant l'entropie** en sautant de port en port (2^{32} possibilités -> infaisable en pratique)
 - Nov. 2020 : attaque utilisant des **canaux cachés pour épuiser les ports** disponibles puis deviner le port utilisé par le serveur DNS [Man et al. 2020]
- Utilisable pour des serveurs HTTP mais **ne permet pas de créer de faux certificats pour HTTPS**

BASES TCP/IP

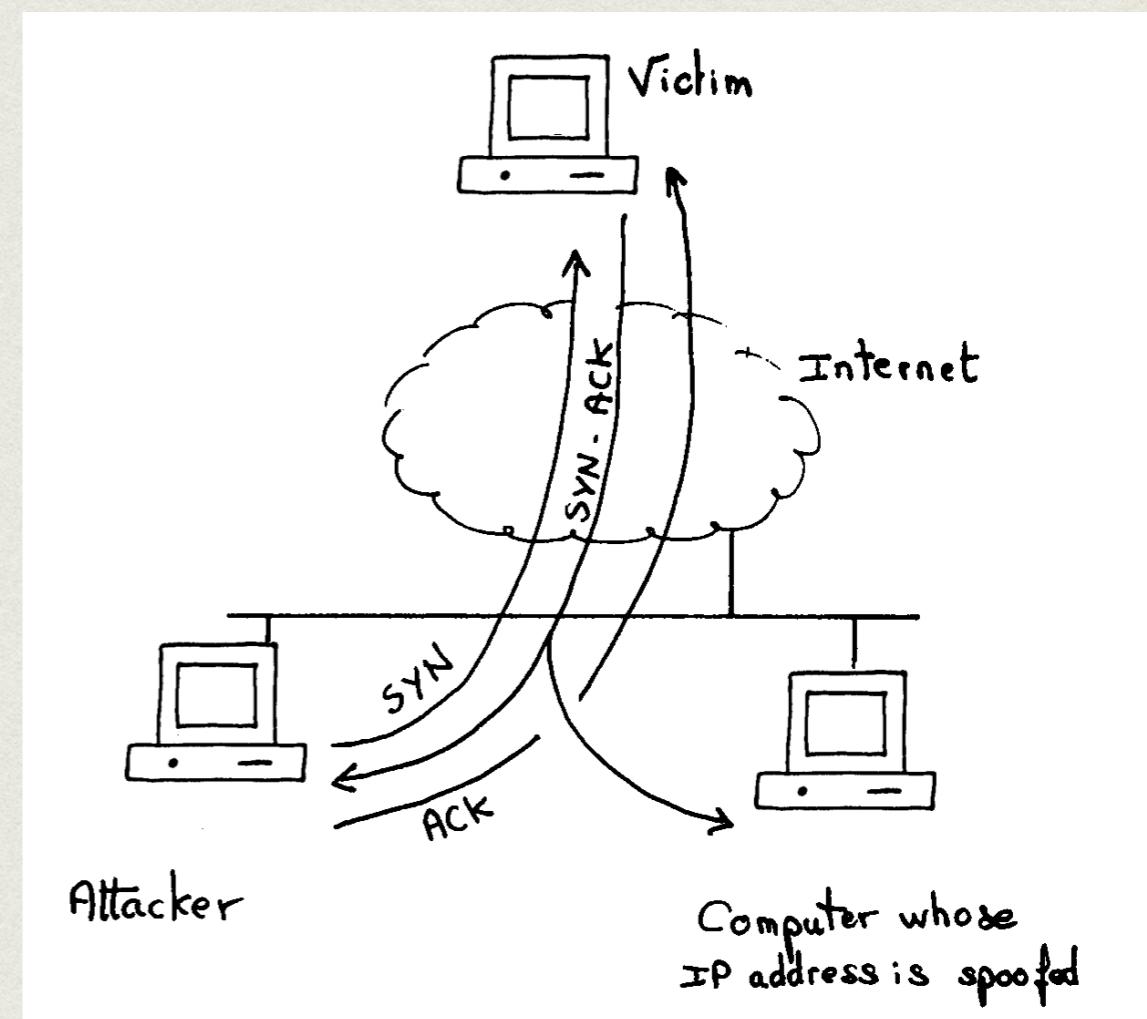
- TCP est un protocole à base de **fenêtres glissantes**
 - il utilise des **numéros de séquence** pour lier requêtes et réponses
- Pour éviter d'utiliser les mêmes numéros de séquence, un numéros de séquence initial (ISN) est choisi **aléatoirement**

BASES TCP/IP



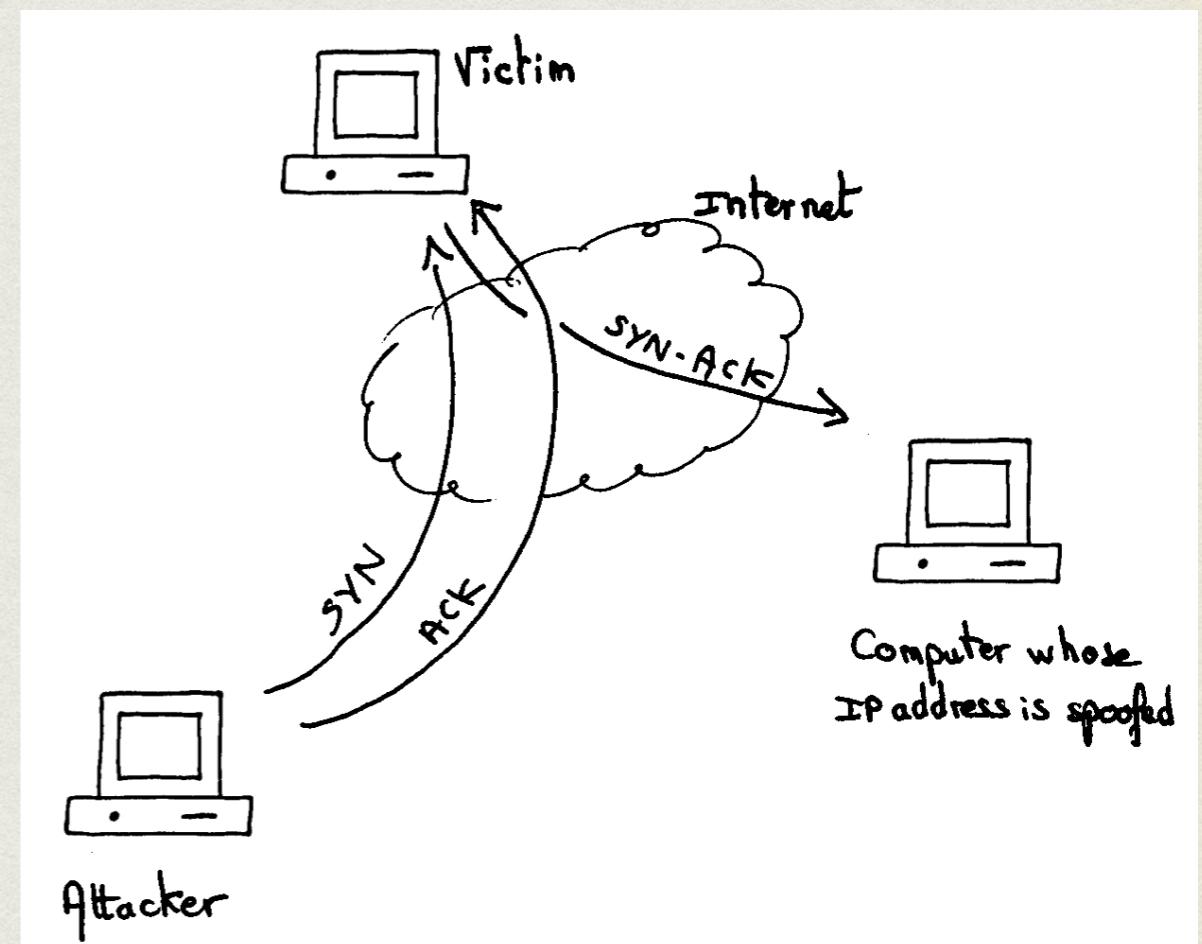
TCP/IP SPOOFING DANS UN LAN

- L'attaquant initie un **handshake en spoofant la source**
- La victime **répond à la source**
 - **Réponse visible par l'attaquant (LAN)**
- L'attaquant empêche la source de répondre (e.g. par inondation SYN)
- Répond à sa place en ayant pu observer les numéros de séquence



TCP/IP SPOOFING HORS D'UN LAN

- L'attaquant doit deviner l'ISN car il ne peut **pas observer le SYN-ACK**
- RFC793 : l'ISN doit être incrémenté toutes les 4 us
- Possible dans certaines implémentations TCP
 - Ouvre une connexion authentique et **obtient l'ISN courant et les incréments**
 - Lance la connection forgée avec **l'ISN+incrément** (ou plusieurs attaques avec différents incréments)



TCP/IP SPOOFING HORS D'UN LAN

14:18:25.90	kevin.1000	>	bob.514:	S	1382726990		
14:18:26.09	bob.514	>	kevin.1000:	S	2021824000	ack	1382726991
14:18:26.17	kevin.1000	>	bob.514:	R	1382726991		
14:18:26.50	kevin.999	>	bob.514:	S	1382726991		
14:18:26.69	bob.514	>	kevin.999:	S	2021952000	ack	1382726992
14:18:26.77	kevin.999	>	bob.514:	R	1382726992		
14:18:27.01	kevin.998	>	bob.514:	S	1382726992		
14:18:27.17	bob.514	>	kevin.998:	S	2022080000	ack	1382726993
14:18:27.25	kevin.998	>	bob.514:	R	1382726993		
14:18:27.54	kevin.997	>	bob.514:	S	1382726993		
14:18:27.71	bob.514	>	kevin.997:	S	2022208000	ack	1382726994
14:18:27.79	kevin.997	>	bob.514:	R	1382726994		
14:18:28.05	kevin.996	>	bob.514:	S	1382726994		
14:18:28.22	bob.514	>	kevin.996:	S	2022336000	ack	1382726995
14:18:28.30	kevin.996	>	bob.514:	R	1382726995		

ARP POISONING

- ARP : Address Resolution Protocol
 - Un protocole pour trouver l'adresse MAC (couche 2-Ethernet) à partir d'une adresse IP (couche 3)
- Simple et non sécurisé :
 - Client : « qui connaît l'adresse MAC de 10.1.2.3 ? »
 - N'importe qui : « 10.1.2.3 à l'adresse MAC 010203040506 »
- Facile de forger des réponses (même non sollicitées) pour rediriger le trafic

ARP POISONING

- L'attaquant doit être dans le LAN attaqué, ou y avoir accès
- Il envoie une réponse ARP à la passerelle en associant l'IP spoofée à son adresse MAC
- La passerelle diffuse ce changement de table dans son réseau
- Les clients qui veulent accéder à l'IP spoofée envoie leur trafic à l'attaquant qui peut l'inspecter et le transmettre (ou le jeter)
- Contremesures dans commutateurs récents : configuration commutateurs (pVLAN) ; inspection dynamique de paquets ARP ; détection de faux serveur DHCP (DHCP Snooping)

VOLS DE SESSION HIJACKING

Marc-Olivier Killijian

UQAM, CNRS

INF4471

SESSION HIJACKING

- Différent des attaques d'usurpation, où l'attaquant commence la session avec l'identité de la victime (sans mot de passe)
- Au lieu de voler un mot de passe
 - L'attaquant attend que l'utilisateur s'identifie
 - Et lui vole sa session
- Applicable à **différents niveaux** : modem, TCP, HTTP, etc.

VOL DE SESSION TCP

- Si un attaquant peut observer une connexion TCP entre A et B
 - Il peut insérer un paquet TCP avec un numéro de séquence correct
 - Et continuer cette session alors que la victime A est dans une avalanche de paquet avec la destination B
 - A, qui n'a pas envoyé ce paquet, envoie un ACK avec un autre numéro de séquence à B
 - B, qui a bien vu et traité le paquet, insiste sur le numéro de séquence et envoie également un ACK

VOL DE SESSION HTTP

- HTTP n'est pas orienté session
 - Couples requêtes/réponses sont indépendants
 - Les sites utilisent des artifices pour reconnaître les requêtes d'une session : cookies ou URL personnalisées
 - Un attaquant qui a accès à ces données peut s'insérer dans une session

CONCLUSION

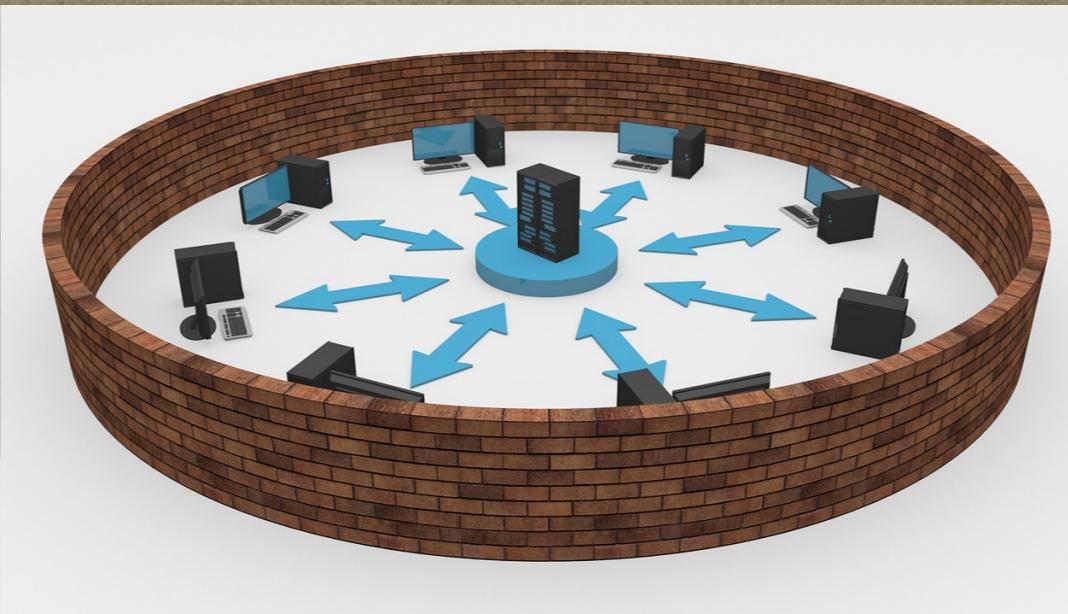
- La plupart des attaques présentées sont **connues depuis longtemps**
 - Mais malheureusement **toujours valides**
- **ARP Poisoning** est une attaque efficace
- Des **contremesures existent** mais sont rarement mises en place

FIREWALLS

Marc-Olivier Killijian

UQAM, CNRS

INF4471



- Un pare-feu sert à **prévenir la propagation** d'un feu
- Un pare-feu réseau doit prévenir la propagation d'une attaque **tout en laissant passer le trafic légitime**
- Un pare-feu/firewall peut être **logiciel ou matériel**

TYPES DE FIREWALL

- **Logiciel**
 - Stations de travail standard avec logiciel pare-feu : Checkpoint, IPcop, IPtables (nftables)
- **Matériel**
 - Boîte noire spécialisée (qui contient du logiciel) : Cisco PIX, Juniper, WatchGuard, SonicWall

LOGICIEL VS MATÉRIEL

- Un pare-feu logiciel hérite des **vulnérabilités de l'OS** sur lequel il s'exécute
- Les architectures des logiciels pare-feu sont bien connues, il est **plus facile d'exploiter** leurs vulnérabilités (par buffer overflow par exemple)
- Les pare-feux logiciels ont souvent de **meilleures performances** et bénéficient des avancées du matériel PC générique

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- Chaque élément du système (utilisateur, logiciel) n'a que les **droit minimaux nécessaires pour remplir sa tâche**
- Exemples :
 - Utilisateurs « réguliers » ne sont **pas admins**
 - Administrateurs doivent utiliser leur **compte utilisateur régulier**
 - Un serveur Web a un **compte non-privilégié** (e.g. Unix : nobody; windows : IUSR)

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- **Plusieurs mesures de sécurité valent mieux qu'une seule**
- Exemples :
 - Anti-virus sur les serveurs mail **et** sur les PC
 - Sécurisation des machines (configuration, mises à jour), **même si elles sont derrière un pare-feu**
 - **Pas de serveur FTP**, même si les connexions FTP ne passent pas le pare-feu

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- La sécurité est plus facile à assurer si tout le trafic passe en **un seul point** (passerelle/gateway)
- **Pas de points d'accès clandestins** (modems, smartphones, etc.)
- Interconnexion avec d'autres compagnies/réseau doivent **passer par le pare-feu**

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- Le réseau et le pare-feu ne sont pas plus sécurisés que le **lien le plus faible**
- Inutile de dépenser de l'argent pour protéger une partie du réseau **si d'autres partie ne le sont pas**
- Exemples: un antivirus dispendieux pour le trafic HTTP est inutile s'il n'y en a pas un pour **SMTP**

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- Il est plus sécuritaire d'**interdire tout ce qui n'est pas explicitement autorisé**
- Que d'autoriser ce qui n'est pas explicitement interdit
- On ne connaît pas **à l'avance les menaces** auxquelles on sera exposées
- En cas d'erreur, **mieux vaut interdire** qq-chose d'utile que de permettre une attaque

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- Un système de protection n'est efficace que si **tous ses utilisateurs le soutiennent**
- L'objectif d'un pare-feu est d'**autoriser ce qui est utile et d'éviter les dangers**
- Un système trop **restrictif** pousse les utilisateurs à le **contourner**
- **Comprendre les besoins** des utilisateurs et leur **expliquer les restrictions**

PRINCIPES DE BASE DE LA SÉCURISATION D'UN RÉSEAU

- Moindre privilège
- Défense en profondeur
- Point de contrôle obligatoire
- Maillon le plus faible
- Interdiction par défaut
- Implication des utilisateurs
- Simplicité
- La plupart des problèmes de sécurité ont pour **origine une erreur humaine**
- Avec un **système simple**
 - Le risque d'erreur est faible
 - Plus facile de vérifier le fonctionnement correct
 - Particulièrement dans des réseaux évoluants
 - Particulièrement avec plusieurs administrateurs

FONCTIONS D'UN PARE-FEU

- Filtrage
- Traduction d'adresse réseau
- Analyse de contenu
- Authentification
- Accès réseau distant

FONCTIONS D'UN PARE-FEU

- Filtrage
 - Objectif: limiter le trafic aux services utiles
- Traduction d'adresse réseau
 - Basé sur des critères multiples
 - IP source ou destination
 - Protocoles et ports
 - Flags et options
- Analyse de contenu
- Authentification
 - Ex: filtrage d'adresse source empêche l'IP spoofing
- Accès réseau distant

FONCTIONS D'UN PARE-FEU

- Filtrage
- Traduction d'adresse réseau
- Analyse de contenu
- Authentification
- Accès réseau distant

	Src	Port	Dst	Port	Prot	Action
1	any	any	128.3.3.1	25	tcp	allow
2	128.3.3.1	25	any	any	tcp	allow
3	128.3.3.1	any	any	25	tcp	allow
4	any	25	128.3.3.1	any	tcp	allow
5	any	any	any	any	any	deny

FONCTIONS D'UN PARE-FEU

- Filtrage
- Traduction d'adresse réseau
- Analyse de contenu
- Authentification
- Accès réseau distant

	Src	Port	Dst	Port	Prot	Action
1	any	any	128.3.3.1	25	tcp	allow
2	128.3.3.1	25	any	any	tcp	allow
3	128.3.3.1	any	any	25	tcp	allow
4	any	25	128.3.3.1	any	tcp	allow
5	any	any	any	any	any	deny

trop permisif: tous les ports du serveur sont accessibles à partir du port 25

FONCTIONS D'UN PARE-FEU

- Filtrage
- Traduction d'adresse réseau
- Analyse de contenu
- Authentification
- Accès réseau distant

	Src	Port	Dst	Port	Prot	Flag	Action
1	any	any	128.3.3.1	25	tcp	ack=*	allow
2	128.3.3.1	25	any	any	tcp	ack=1	allow
3	128.3.3.1	any	any	25	tcp	ack=*	allow
4	any	25	128.3.3.1	any	tcp	ack=1	allow
5	any	any	any	any	any	ack=*	deny

spécifier le flag ack
permet d'éviter l'envoi
de paquet SYN

FONCTIONS D'UN PARE-FEU

- Filtrage
- Traduction d'adresse réseau
- Analyse de contenu
- Authentification
- Accès réseau distant
- Adresses IP publiques sont rares
 - à l'intérieur d'un réseau on utilise une plage d'adresse
 - 10.0.0.0-10.255.255.255
 - 172.16.0.0-172.31.255.255
 - 192.168.0.0-192.168.255.255
 - et on fait du NAT

FONCTIONS D'UN PARE-FEU

- Filtrage
- Network Address Translation (NAT)
 - Adresses privées à l'intérieur du réseau
 - Une ou plusieurs adresses publiques pour sortir
 - Le pare-feu remplace la source des paquets qui sortent par l'adresse publique
 - Et la destination d'un paquet qui rentre par l'adresse privée
 - En utilisant une table de traduction adresses publiques/privées
 - Peut-être dynamique ou statique, cf. cours de réseau
- Analyse de contenu
- Authentification
- Accès réseau distant

FONCTIONS D'UN PARE-FEU

- Filtrage
- Network Address Translation (NAT)
- Analyse de contenu
- Authentification
- Accès réseau distant
- Le pare-feu peut analyser les paquets pour vérifier leur format et contenu
 - Eliminer les paquets mal formés (ping of death)
 - Eliminer les paquets qui ne correspondent pas à l'état du protocole (réponse non sollicitée)
 - Eliminer les paquets au contenu indésirable (virus)
 - Analyse de certains protocoles applicatifs
 - E.g. éliminer certaines commandes SMTP

FONCTIONS D'UN PARE-FEU

- Filtrage
- Network Address Translation (NAT)
 - Le pare-feu peut vérifier l'authentification avant de laisser une connexion s'établir
 - En sortie : seuls les utilisateurs privilégiés
 - En entrée : pour un utilisateur légitime qui se connecte de l'extérieur
 - Remote Network Access
 - Connexion chiffrée (tunnel) via internet ou un modem
 - L'utilisateur se retrouve dans le LAN
- Analyse de contenu
- Authentification
- Accès réseau distant

CONCLUSION

- Un pare-feu est un équipement de sécurité essentiel
- Il doit être adapté à son environnement
 - Il existe des pare-feu personnels pour le domicile
- Il ne protège pas (bien) contre
 - Attaques internes
 - Attaques initiées par de l'équipement mobile (laptops, USB)
 - Les utilisateurs natifs ou malveillants

DÉTECTION D'INTRUSION

Marc-Olivier Killijian

UQAM, CNRS

INF4471

GÉNÉRALITÉS

- Protéger c'est bien mais détecter et se défendre c'est mieux
- **Ne pas attendre les symptômes d'une attaque avant de réagir**
- Les Systèmes de Détection d'Intrusion (IDS) analysent :
 - **Traffic réseau** (Network IDS, NIDS)
 - **Évènements serveurs** (Host IDS, HIDS)
- Cette analyse peut être en **temps-réel** ou **hors-ligne**

CLASSIFICATION

	Temps-réel	Hors-ligne
Network IDS	Capture et analyse du trafic réseau	Analyse des traces et des configuration
Host IDS	Inspection des interruptions, des appels systèmes et de registres	Analyse des traces systèmes

NETWORK IDS

- Composé d'un sniffer et d'un inspecteur de trafic
- Des règles sont appliquées aux paquets capturés
 - dans des protocoles de toutes les couches
- Lorsqu'une règle est activée, une action est exécutée
 - Journalisation
 - Envoi d'une alarme : texto, courriel, interface web, etc.
 - Couper une connexion, reconfigurer le pare-feu

INTRUSION PREVENTION SYSTEM IPS

- Un IPS est un IDS qui réagit à une attaque
 - IP : filtrer la source de l'attaque dans le pare-feu (pour un temps donné)
 - TCP : envoyer un paquet TCP spoofé pour clore la connexion
 - Application : « corriger » une requête web pour enlever les caractères spéciaux
- Attention aux attaques en déni de service qui pourraient utiliser l'IPS

CARACTÉRISATION DU TRAFIC

- Un IDS qui fait des analyses **statistiques sur le trafic réseau**
- Si une valeur **sort de ses limites habituelles**, on assume qu'il y a une attaque (e.g. nombre de paquets reçus sur un port donné)
 - Peut détecter de **nouvelles attaques** (o-day)
 - Peut ne pas détecter une attaque (**faux négatifs**)
 - Peut détecter des attaques quand il n'y en a pas (**faux positifs**)
- Fort taux de faux positifs -> type d'IDS **impopulaire**

IDS PAR SIGNATURES

- L'IDS a une **base de signatures d'attaques connues**
 - Ex: une requête web de taille >2000 caractères = buffet overflow
 - Signatures collectées sur des **pots de miel**, des machines spécialement conçues pour attirer et observer les attaques
- Ne peut pas reconnaître de nouvelles attaques, besoin d'être mis-à-jour constamment
- Faux négatifs
 - Attaques manuelles ciblées dévient du comportement décrit par la signature
 - Signatures trop restrictives, empêche de détecter les variantes
- Faux positifs a priori inexistant mais détections pas forcément pertinentes (e.g. attaque Windows sur réseau Linux)

SNORT

- SNORT est un sniffer pour Linux et Windows
- Analyse le trafic, par exemple devant le pare-feu
- Envoi de courriel et/ou reconfiguration du pare-feu
- Enorme base de signatures maintenue par les utilisateurs et développeurs
- Exemples de signatures :
 - log tcp any 80 -> any any :
 - journalise les paquets TCP venant de n'importe quelle adresse port 80 et allant vers n'importe quelle destination, n'importe quel port
 - alert tcp any any -> 192.168.1.0/24 143 (content: « |90C8 COFF FFFF|/bin/sh »;msg « IMAP buffer overflow! »;) :
 - Alerte sur reception d'un paquet de n'importe quel noeud, n'importe quel port vers le port 143 du noeud 192.168.1.0/24 lorsque le paquet contient la chaine « |90C8 CoFF FFFF|/bin/sh ».



CONCLUSION

- IDS à base de signatures fonctionnent bien mais
 - la plupart des attaques dont on dispose d'une signature peuvent être bloquées par le pare-feu ou par une mise-à-jour système
 - portée limitée aux cas où une mise-à-jour doit attendre, d'où l'importance de la **mise-à-jour de la base de signatures**
 - Comment **réagir correctement** face à une attaque est difficile
 - Réactions automatiques peuvent être **sources de DOS** !
 - Mise en oeuvre de la **sécurité en profondeur**