



Réseaux et Services de
Télécommunications



Sécurité des réseaux

NET4101 - Les réseaux:
réalité d'aujourd'hui et défis de demain

Gregory Blanc - Département RST, Télécom SudParis



Sécurité de la pile TCP/IP

Introduction et concepts de base

Qui sont les attaquants?



source: *Hackers*, Iain Softley (1995)

En réalité, ...

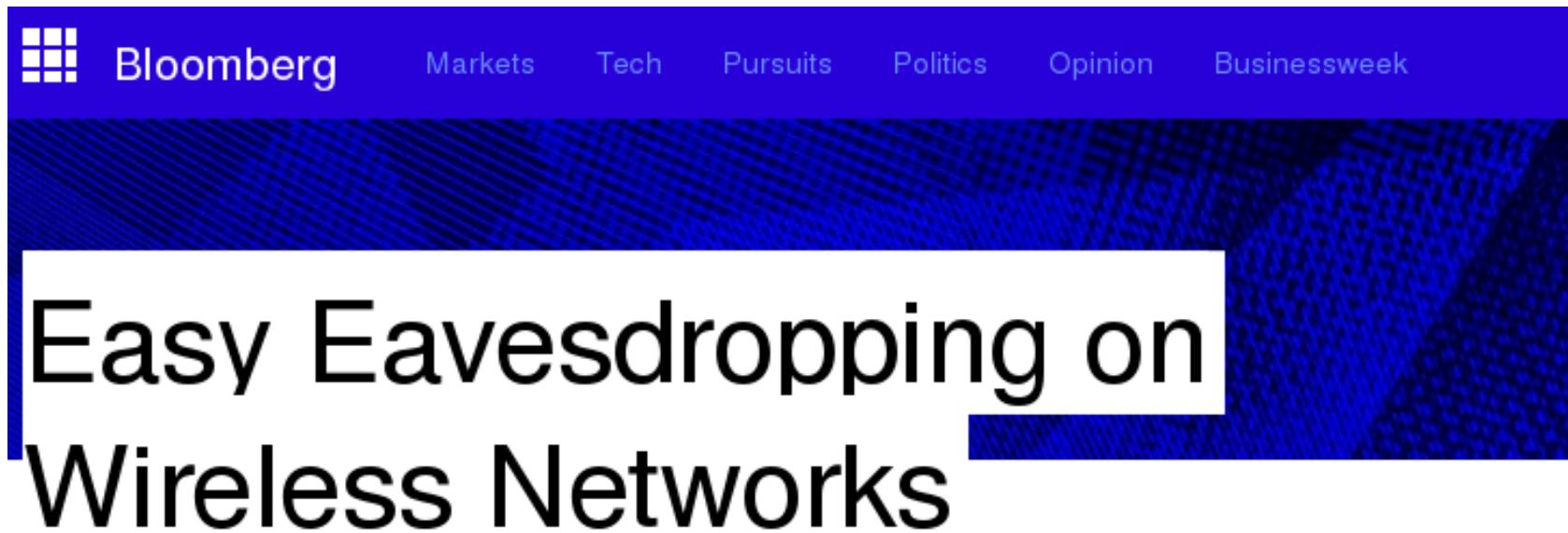
Population

- des criminels
- des terroristes
- des experts en sécurité
- des entreprises
- des employés
- des marginaux
- des citoyens
- des étudiants

Motivation

- pour terroriser
- pour espionner
- pour informer
- pour faire du profit
- pour prendre une revanche
- pour le plaisir ou le prestige
- pour la propagande
- pour satisfaire sa curiosité

Ex: lire les communications sur le WiFi



The image shows a screenshot of a Bloomberg article. At the top, there is a dark blue navigation bar with the Bloomberg logo on the left and categories: Markets, Tech, Pursuits, Politics, Opinion, and Businessweek. Below the bar is a large, dark blue background image with a subtle grid pattern. Overlaid on this image is a white rectangular box containing the main title of the article in large, bold, black font: "Easy Eavesdropping on Wireless Networks".

A new report details serious security flaws in these increasingly popular setups. Here's what you can do to enhance your safety

f t h

Ex: se connecter à une webcam



Big Browser

– PIQUANT – A Londres, des pointes contre les SDF TERRAIN VIRTUEL – Et le vainqueur du Mondial sera ... →

10 juin 2014

INTRUSION 2.0 – Avec Shodan, contrôlez des webcams et imprimez chez les autres.



Ex: rendre indisponible un service de jeux en ligne

The screenshot shows a news article from Ars Technica. The header features the site's logo ('ars TECHNICA') and a navigation bar with links for BIZ & IT, TECH, SCIENCE, POLICY (which is highlighted in orange), CARS, GAMING & CULTURE, FORUMS, and a menu icon. Below the header, a green 'LAW & DISORDER' tag is visible. The main title of the article is '“Anonymous” attacks Sony to protest PS3 hacker lawsuit'. A subtitle below it reads 'Outraged by Sony's lawsuit against PS3 hacker George Hotz, the hacker ...'. The author is listed as 'NATE ANDERSON - 4/4/2011, 7:42 PM'. At the bottom of the article, there is a large image of a person in a suit and tie, with the text 'COURAGE IS CONTAGIOUS' in the top right corner and 'Should you go to jail for making your PS3 run your own programs?' in the bottom left.

Ex: exploiter des ressources accessibles "librement"

[ZDNet.fr > News > OVH noyé par une attaque Ddos sans précédent >](#)

OVH noyé par une attaque Ddos sans précédent

Sécurité : L'hébergeur roubaisien a fait face à une attaque Ddos d'ampleur ayant dépassé la barre du térrabit par seconde. À l'origine de cette offensive, un botnet de caméras IP infectées par des cybercriminels.



Par La rédaction de ZDNet.fr | Mardi 27 Septembre 2016

[Suivre @zdnfr](#)

Les équipes chargées de la protection Ddos d'OVH ont apparemment eu fort à faire la semaine dernière. Sur Twitter, le fondateur et CTO de l'hébergeur roubaisien Octave Klaba expliquait en effet que son groupe faisait face à une attaque Ddos record visant ses infrastructures. Les attaques se sont étendues du 18 au 23 septembre, avec une pointe à 1 térrabit par seconde de trafic malveillant atteint le 20 septembre.

Ex: saboter des centrifugeuses nucléaires

BBC BBC ID Menu Search Sections

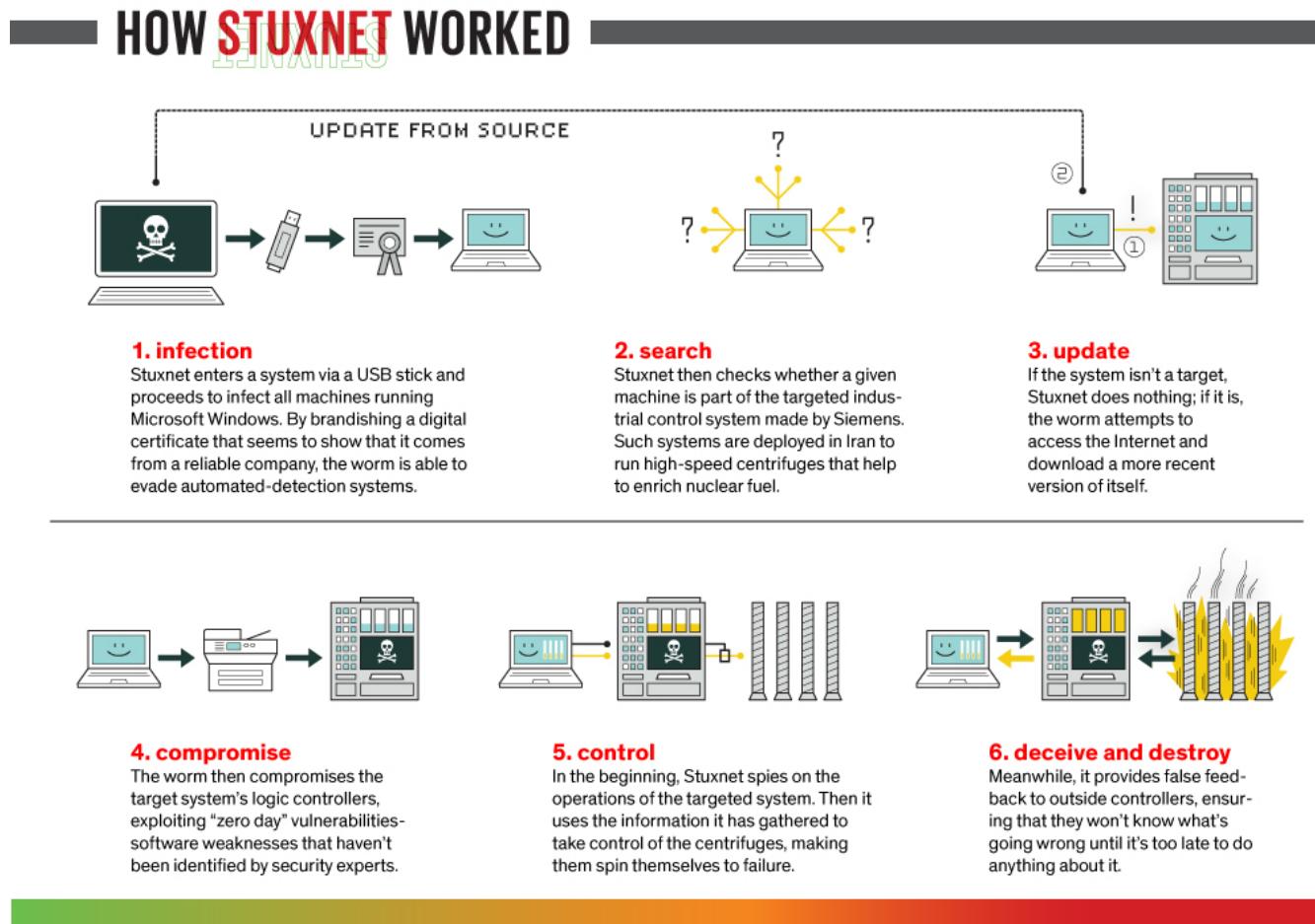
NEWS

Stuxnet 'hit' Iran nuclear plans

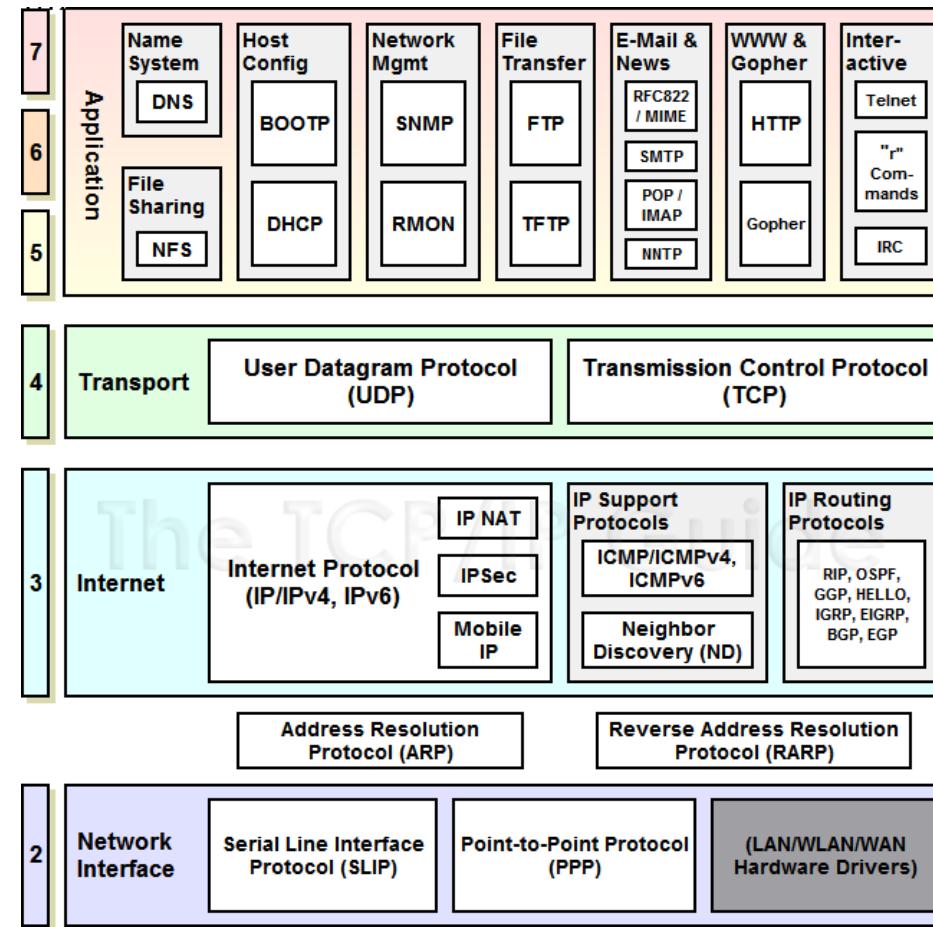
22 November 2010 | Technology



Stuxnet: pas forcément besoin du réseau

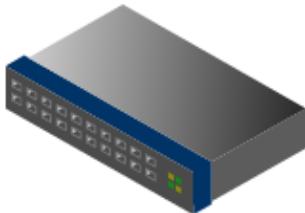


Rappel: pile TCP/IP



source: [The TCP/IP Guide](#)

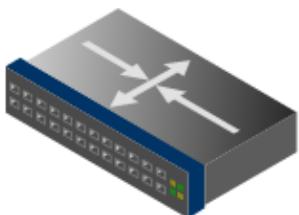
Rappel: équipements réseau



Hub



Commutateur



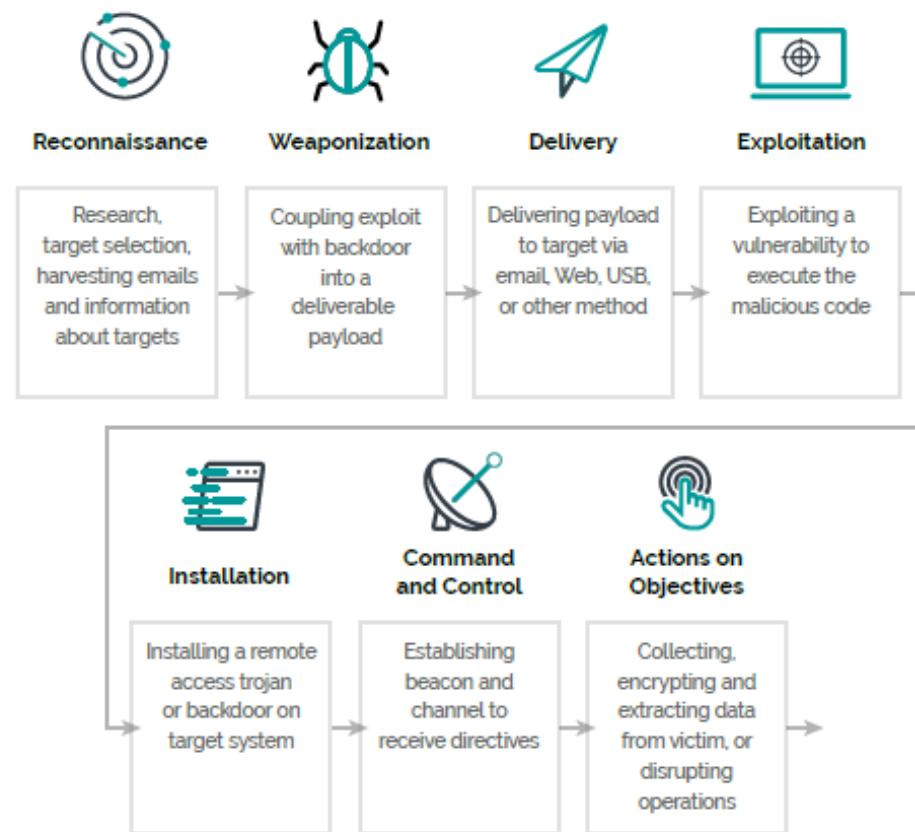
Routeur

- répète un message envoyé sur tous ses ports
- **il suffit d'être connecté au hub pour recevoir les messages**

- transmet un message sur le port du destinataire
- **il reste possible de frauder l'adresse MAC du destinataire**

- transmet un message au réseau du destinataire
- **il reste possible de frauder l'adresse IP du destinataire**

Etapes d'une cyber attaque



source: Cyber Kill Chain (Lockheed Martin, 2010)

Modéliser la menace: STRIDE

Spoofing un attaquant usurpe une identité (par ex., une adresse IP)

Tampering un attaquant altère le contenu de paquets transmis

Repudiation un attaquant nie avoir reçu des paquets

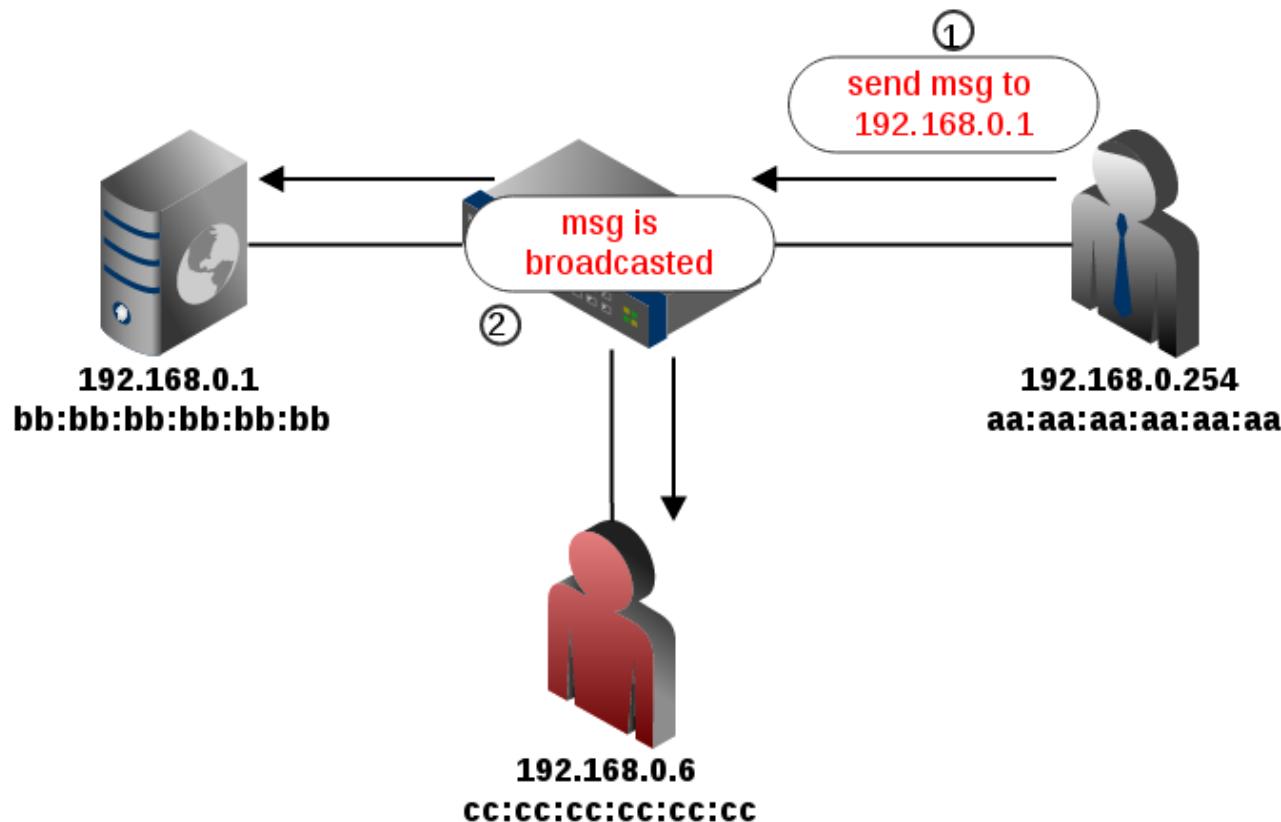
Information Disclosure un attaquant lit le contenu de paquets transmis

Denial of Service un attaquant rend un service ou une ressource indisponible

Privilege Escalation un attaquant obtient des permissions privilégiées sur le réseau

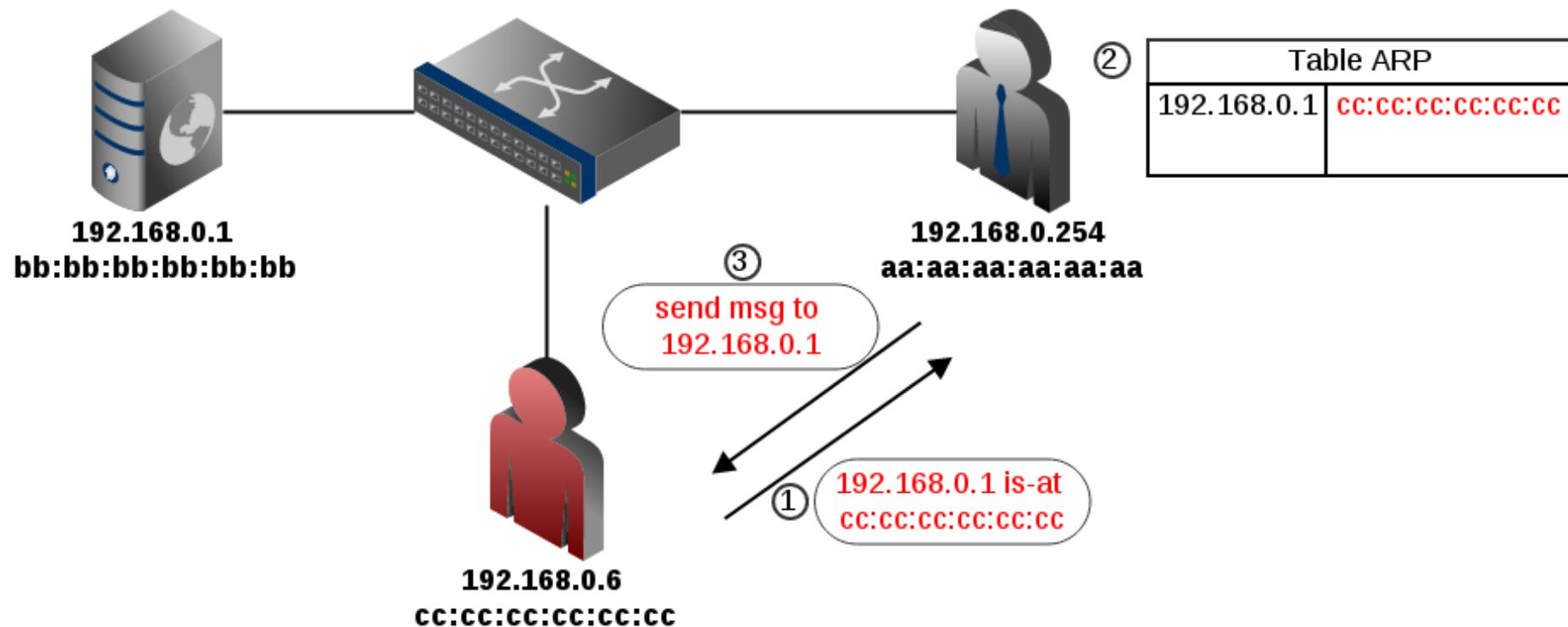
source: [The STRIDE Threat Model](#) (Microsoft, 2005)

Exemple de divulgation d'information: sniffing réseau



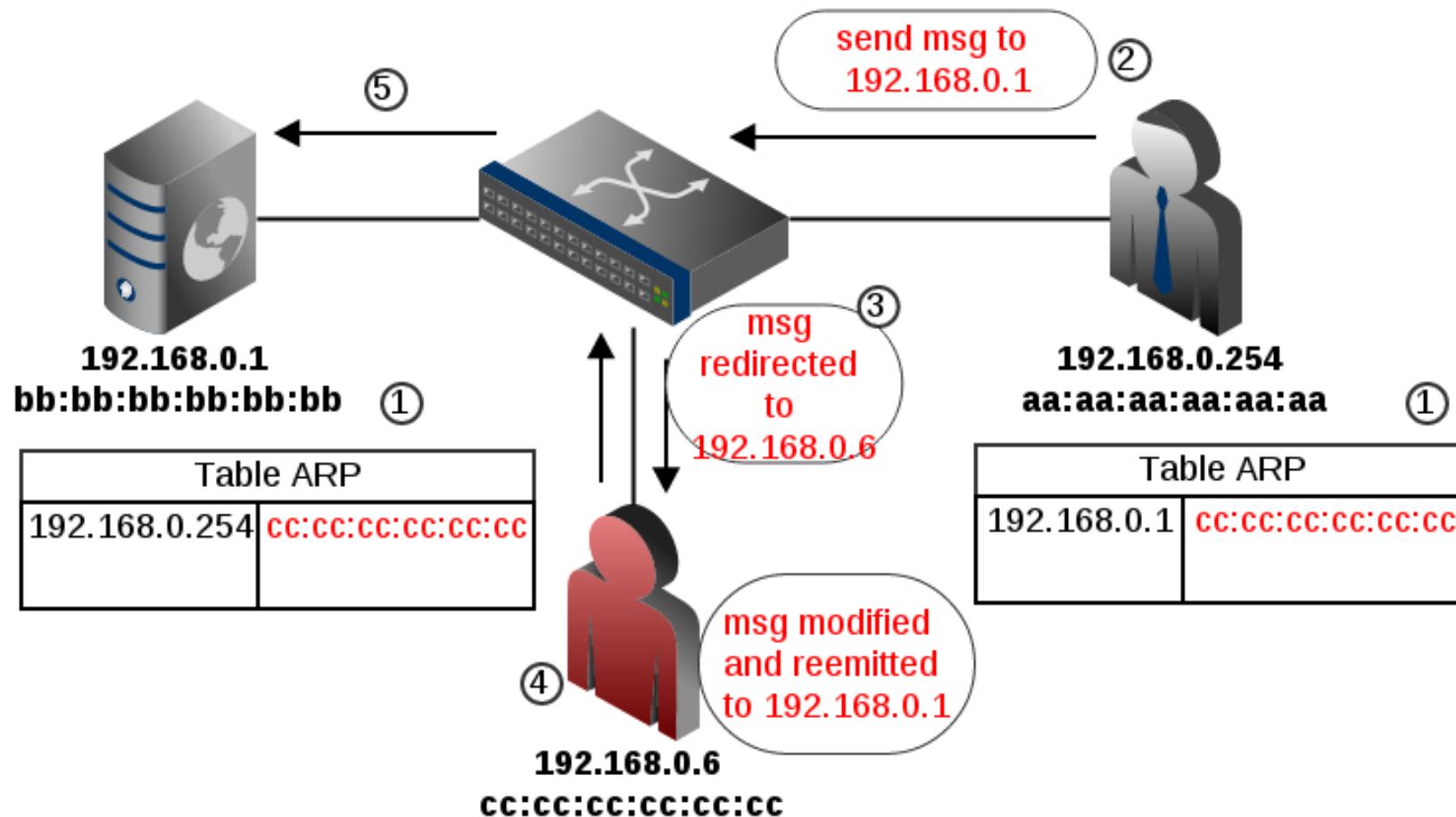
Rien ne permet de chiffrer les informations échangées

Exemple d'usurpation: ARP spoofing



Rien ne permet de vérifier l'authenticité des émetteurs et récepteurs

Exemple d'altération: Man-in-the-Middle (MITM)



Rien ne permet d'empêcher la modification du contenu des paquets

Autres types de menaces

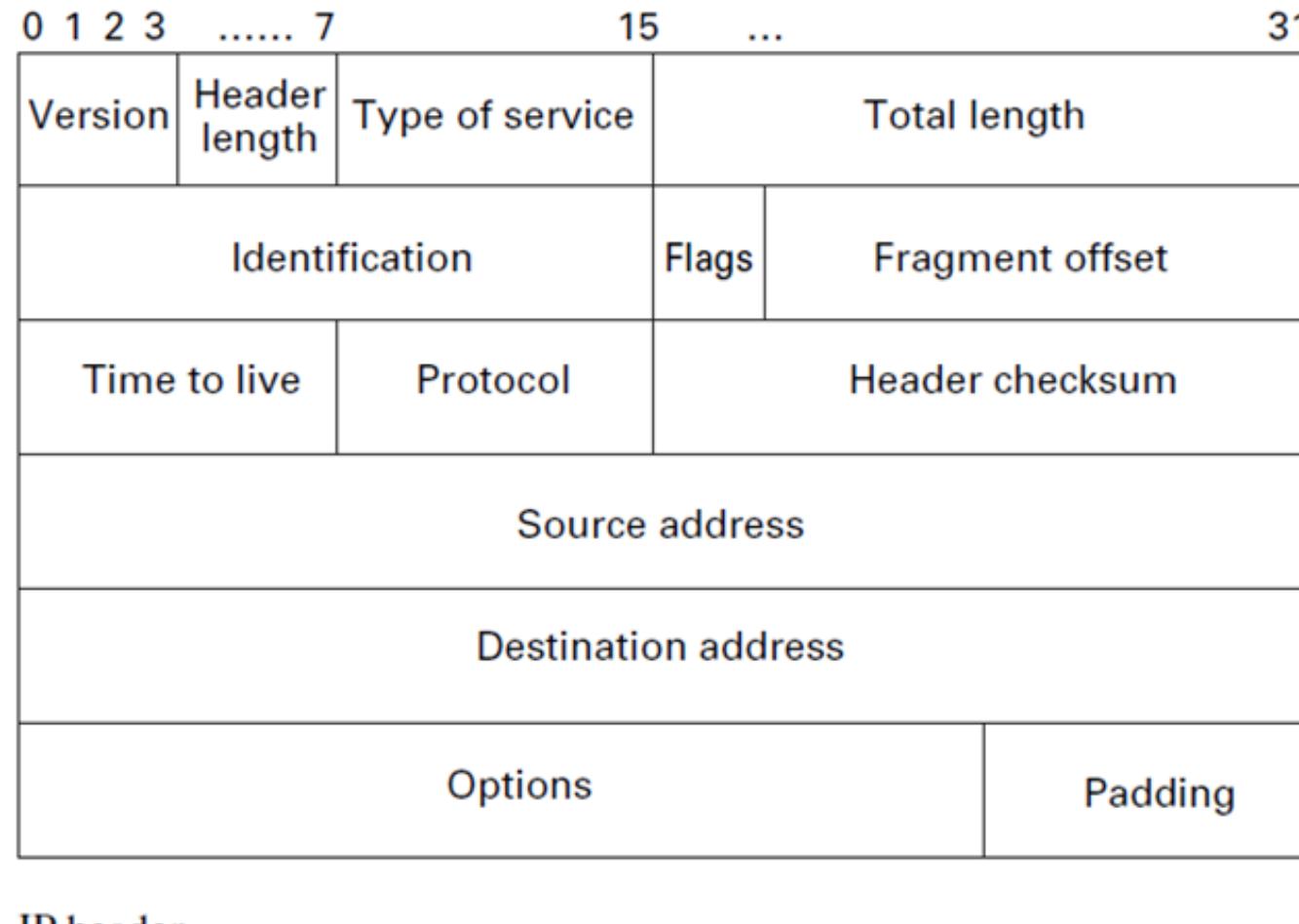
Réputation

- Un émetteur peut nier avoir envoyé un message
- Rien ne permet de retracer ses échanges

- Un émetteur abuse du réseau (en envoyant de nombreux paquets) pour rendre indisponible une cible
- Rien ne permet de bloquer ses nombreux messages

Déni de service

Rappel: Internet Protocol (IP)



IP header

Rappel: Fragmentation IP

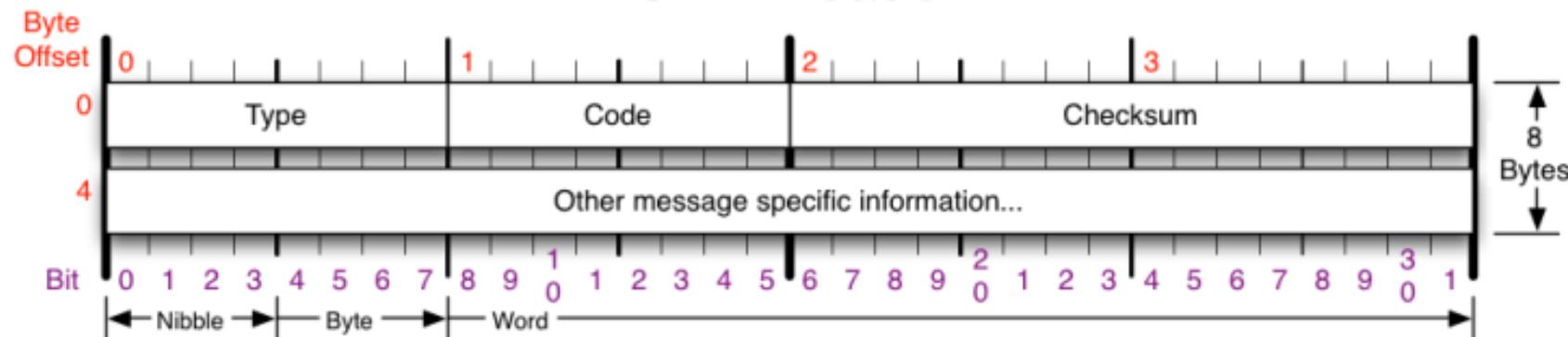
Lorsqu'un paquet IP est transmis entre deux machines:

- il peut traverser de nombreux équipements
- il peut être encapsulé dans divers protocoles L2
- la taille du champ d'information (MTU) peut varier

Un paquet est **fragmenté** lorsque sa taille est **supérieure** au MTU du chemin qu'il traverse:

- ID (2 octets): permet d'identifier un paquet unique entre émetteur et récepteur. Les fragments d'un paquet partagent le même ID
- flag (3 bits): permet de gérer la fragmentation
 - premier bit toujours positionné à 0
 - bit DF (**Don't Fragment**): 0= fragmentation autorisée
 - bit MF (**More Fragment**): 0= dernier fragment
- fragment offset (13 bits): position du premier octet du fragment dans la partie données du paquet d'origine

Rappel: Internet Control Message Protocol (ICMP)



ICMP Message Types		Checksum
Type Code/Name	Type Code/Name	Type Code/Name
0 Echo Reply	3 Destination Unreachable (continued)	11 Time Exceeded
3 Destination Unreachable	12 Host Unreachable for TOS	0 TTL Exceeded
0 Net Unreachable	13 Communication Administratively Prohibited	1 Fragment Reassembly Time Exceeded
1 Host Unreachable	4 Source Quench	12 Parameter Problem
2 Protocol Unreachable	5 Redirect	0 Pointer Problem
3 Port Unreachable	0 Redirect Datagram for the Network	1 Missing a Required Operand
4 Fragmentation required, and DF set	1 Redirect Datagram for the Host	2 Bad Length
5 Source Route Failed	2 Redirect Datagram for the TOS & Network	13 Timestamp
6 Destination Network Unknown	3 Redirect Datagram for the TOS & Host	14 Timestamp Reply
7 Destination Host Unknown	8 Echo	15 Information Request
8 Source Host Isolated	9 Router Advertisement	16 Information Reply
9 Network Administratively Prohibited	10 Router Selection	17 Address Mask Request
10 Host Administratively Prohibited		18 Address Mask Reply
11 Network Unreachable for TOS		30 Traceroute

Checksum of ICMP header
RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

Ping of death

Remarques préliminaires

- Champ longueur du paquet IP = **16 bits** → taille maximum autorisée: **65535 octets**
- En pratique, MTU = 1500 octets → paquet IP **fragmenté**
- Champ **fragment offset** = 13 bits → décalage maximum d'un fragment IP = **65528**
- En-tête ICMP = 8 octets → taille maximale champ de données: **65507 octets**
- La machine destinataire ré-assemble les paquets fragmentés

Question

- Que se passe t'il lorsqu'un paquet ICMP fragmenté présente un dernier fragment dont le champ de données fait plus de 8 octets?
- Lorsque la machine destinataire ré-assemble le paquet, la mémoire tampon, qui conserve l'ensemble des fragments, est débordée faisant planter la machine

ICMP redirect

Remarques préliminaires

- Un message **ICMP redirect** est normalement envoyée par les routeurs lorsque **la route** vers une destination a changé
- Un hôte recevant une telle instruction **modifie sa table de routage** pour le destinataire vers le réseau ou la passerelle indiquée
- Un hôte recevant ce genre de message **fait confiance** à la source qui le lui a envoyé

Question

- Comment un attaquant pourrait-il tirer avantage de ce type de message ICMP?
- En forgeant un paquet **ICMP redirect** dont l'adresse source est un hôte ou un routeur (passerelle) avec lequel la victime souhaite communiquer ...
- ... et en spécifiant une machine contrôlée par l'attaquant comme adresse de redirection
- Un attaquant peut alors espionner, rejouer, capturer, modifier ou bloquer les paquets de la victime

ICMP source quench

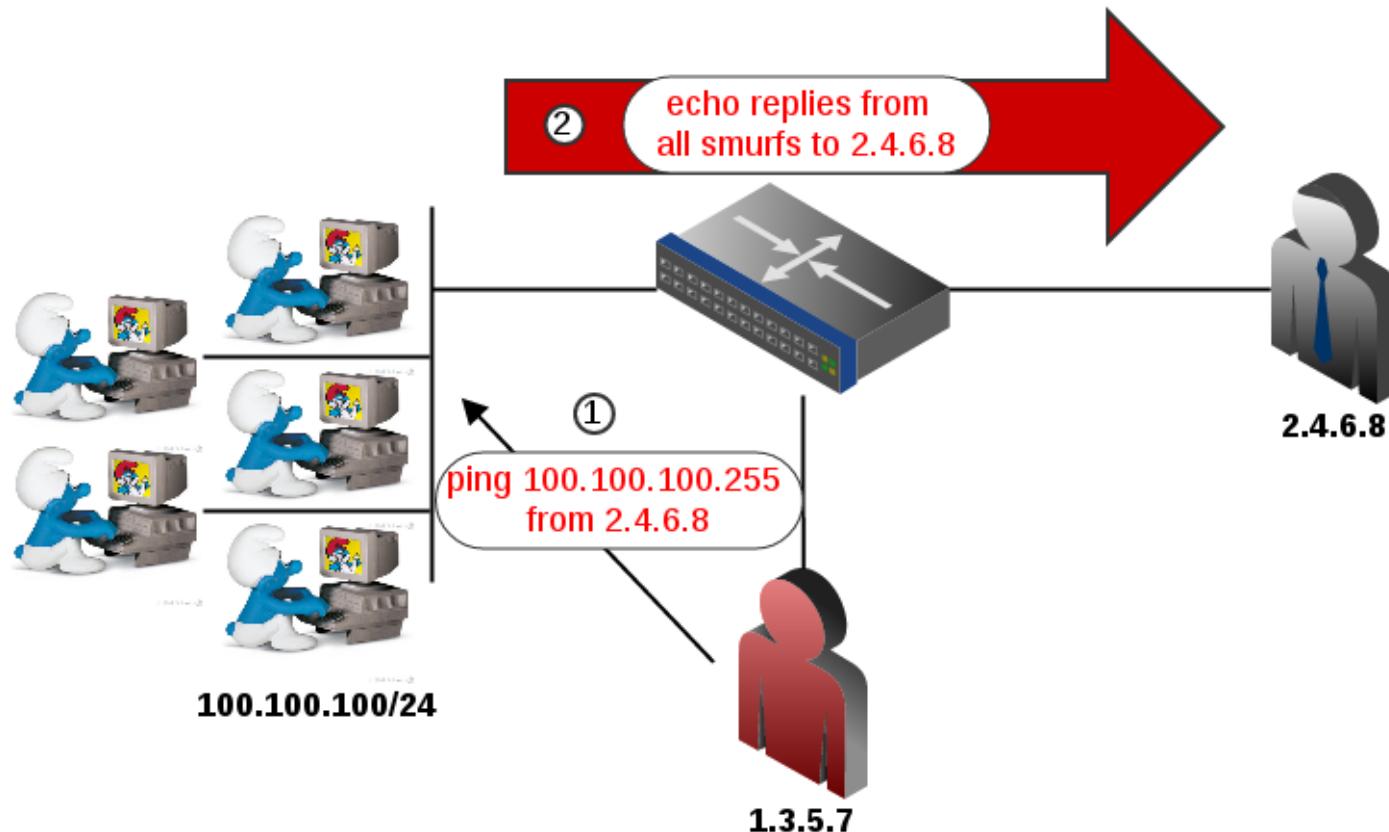
Remarques préliminaires

- Un message ICMP source quench est normalement envoyée par un routeur lorsqu'il est **incapable** de traiter un volume de paquets entrants
- Cela signifie souvent que l'émetteur doit **réduire son débit**

Question

- Comment un attaquant pourrait-il tirer avantage de ce type de message ICMP?
- En forgeant un paquet ICMP source quench dont l'adresse source est un routeur avec lequel la victime communique
- Cela aura pour effet de réduire le débit de la victime
- C'est une forme subtile de **déni de service**

Smurf attack



Une variante sur UDP existe et consiste en l'envoi de messages spoofés vers des ports echo, chargen, daytime, qotd

Synthèse

Les protocoles principaux de la pile TCP/IP (IP, TCP, UDP, ICMP, etc.) ne prennent pas en compte la sécurité

En particulier, IP n'implémente aucun mécanisme de sécurité.

Plusieurs faiblesses mises en évidence

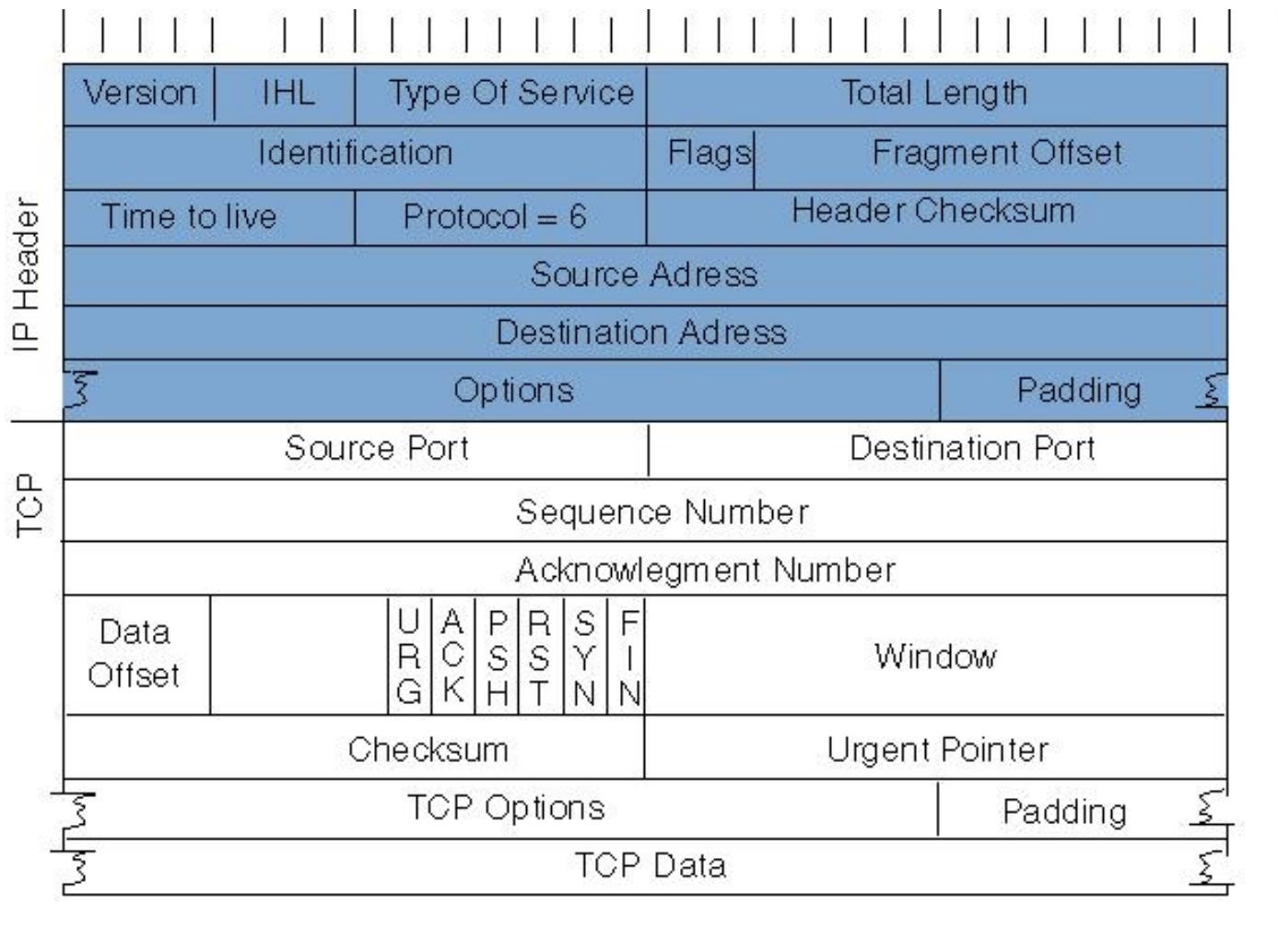
- Absence d'authentification des émetteurs et récepteurs de paquets
- Absence de chiffrement des données échangées
- Absence de vérification de l'intégrité des messages ([fragmentation](#)) et de leur ordre

TCP a toutefois permis d'apporter certaines garanties

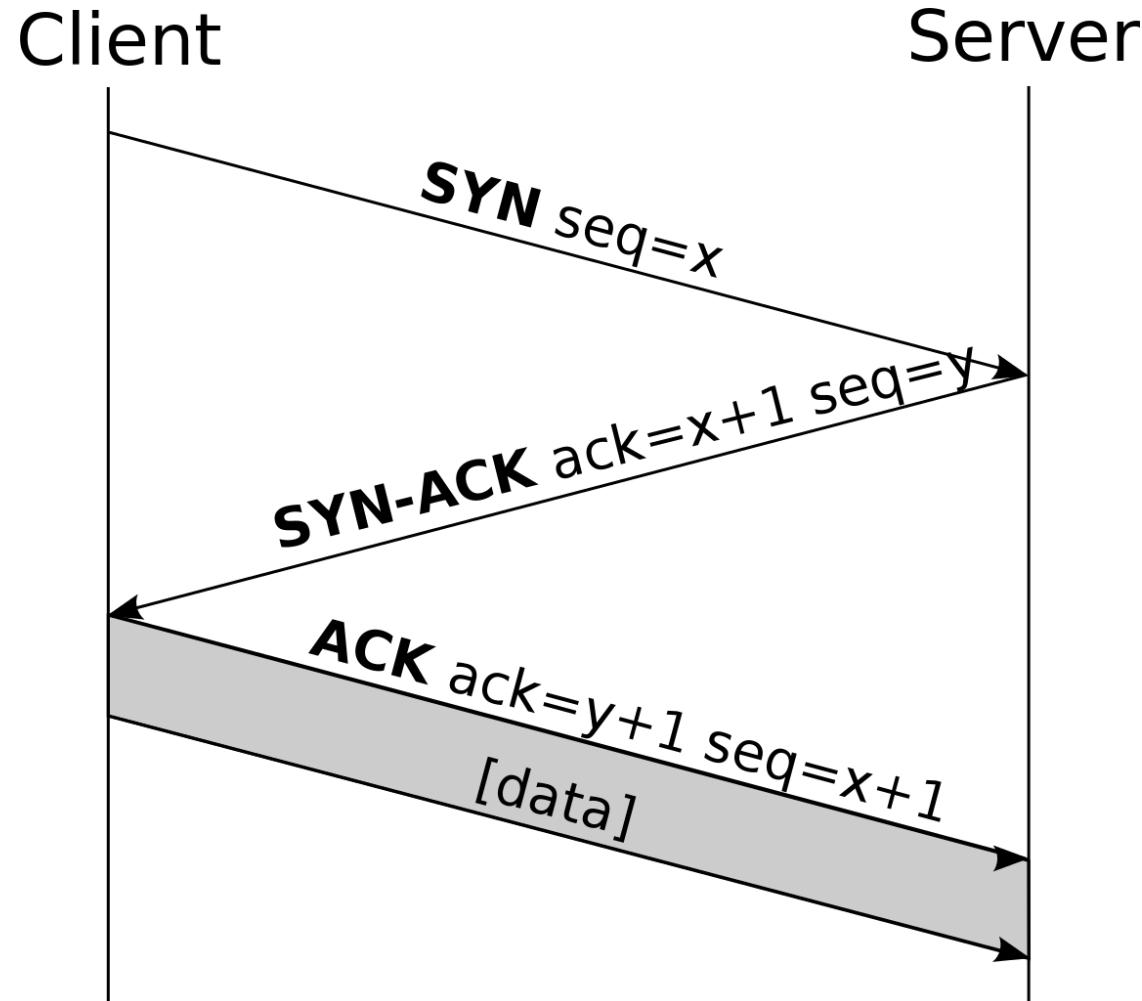
un mode connection permet de fiabiliser la communication

- session
- ordonnancement
- confirmation de réception

Transport Control Protocol (TCP)



La poignée de main (handshake) TCP



Détournement (hijacking) de session TCP

Objectif

Un attaquant va prendre le contrôle d'une session ouverte par un hôte

Principe

Il faut créer un paquet avec le numéro de séquence (**aléatoire**) attendu par le serveur

Approches

1. Deviner le numéro de séquence attendu = 2^{32} possibilités
2. Observer les échanges entre le client et le serveur:
 - dans le cas d'un hub dans le même sous-réseau → trivial!
 - dans le cas d'un réseau commuté → MITM (ARP poisoning, ICMP redirect)

L'attaquant s'approprie la session en injectant un paquet avec le numéro de séquence: **numéro de séquence [serveur] + 1**

Déni de services (denial of service (DoS))

Principe

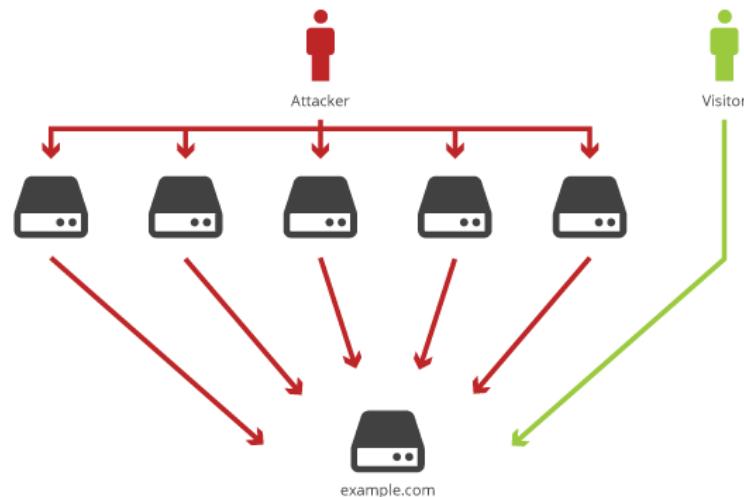
Un attaquant abuse d'un service ou de l'accès à ce service pour en empêcher l'usage ou l'accès à d'autres utilisateurs

Approches

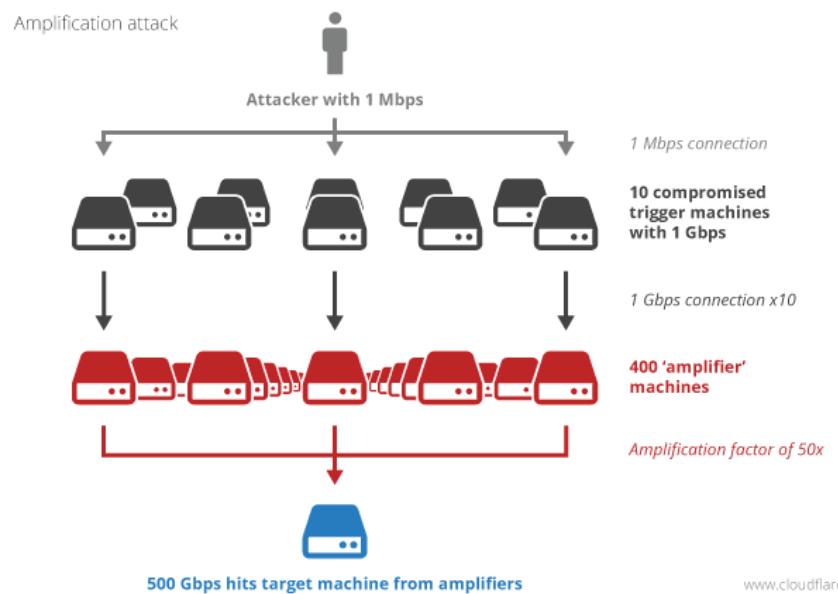
1. Réseau:
 - Congestion du lien d'accès au service
 - Reroutage du service
2. Système:
 - Epuisement des ressources du service
 - Plantage du service

DoS avancés

DoS distribué (DDoS)



DoS réfléchi (DrDOS)



source: CloudFlare

SYN flooding

Principe

Un attaquant initie de nombreuses connexions TCP avec la victime sans jamais les ouvrir

Attaque

Chaque connexion semi-ouverte est maintenue un certain temps par le serveur, ce qui a pour effet de consommer des ressources (processeur, mémoire) inutilement

Un attaquant peut alors tenter d'épuiser les ressources du serveur en initiant un très grand nombre de connexions TCP, sans jamais les honorer

Il y a **déni de service** lorsque le serveur ne peut plus servir un client:

- soit parce qu'il a planté, sous la pression de la charge de l'attaque
- soit parce qu'il a atteint le nombre maximum de connexions autorisées

Quelques outils

Scan: nmap, hping, Nessus, OpenVAS

Sniff: tcpdump, Wireshark

MITM: ettercap

Exploit: metasploit, Empire

Connect: netcat, Scapy



Sécurité des protocoles de routage

RIP, OSPF, BGP

Rappel: Routage intérieur

RIP

Algorithme: basé sur Bellman-Ford (type distance-vecteur)

Table de routage maintient les routeurs et la métrique associée (**distance = nombre de sauts**)

Routeur diffuse sa table de routage à ses voisins toutes les 30 secondes

A réception d'une table de routage, le routeur calcule les métriques locales des routes apprises, sélectionne les meilleures routes et en déduit sa table de routage, qu'il renvoie si elle a changé

Les échanges continuent jusqu'à ce que l'algorithme **converge**

OSPF

Algorithme: Shortest Path First de Dijkstra (type état des liens)

Table de l'état des liens **unique et partagée** par tous les routeurs

Routeur **acquiert** la base de données du routeur principal, met à jour sa base de données (vision globale du réseau), calcule ses meilleures routes et en déduit sa table de routage

Chaque routeur diffuse la liste de ses voisins immédiats et le coût de la liaison à tout le réseau

A chaque **changement** de l'état d'un lien, les routeurs émettent des messages (LSA)

Falsification des tables RIP

Principe

Un attaquant reroute le trafic entre deux routeurs

Attaque

L'attaquant désire intercepter les paquets à destination d'un réseau cible X

L'algorithme de calcul du protocole RIP reposant sur la notion de meilleure métrique

- L'attaquant doit alors convaincre le routeur qu'il permet d'atteindre le réseau X avec une meilleure route

L'attaquant envoie donc au routeur une table de routage où la métrique associée au réseau X est meilleure que la route qu'il connaît

Le routeur met alors sa table de routage à jour et reroute donc le trafic destiné au réseau X via l'attaquant

Rappel OSPF: Link State Advertisement (LSA)

Découverte des voisins

Chaque routeur découvre dynamiquement ses voisins sur les liens qui lui sont attachés

Lorsque la relation ([adjacency](#)) est établie, ils échangent leur bases de LSAs

Propagation des LSAs

Les LSAs sont propagés à travers tout le réseau à tous les routeurs

Chaque routeur a une vue globale du réseau

Chaque LSA est identifié par un triplet (Numéro de séquence, Checksum, Age)

Mécanisme de [fight back](#): lorsqu'un routeur reçoit une copie plus récente de sa propre table LSA, il en réemet immédiatement une nouvelle

Forces et faiblesses d'OSPF

Sécurité

Intégrité des messages: chaque lien possède un secret partagé

Intégrité des liens: un lien doit être publié par les deux extrémités

Non-répudiation des LSAs: les LSAs sont envoyés à tout le réseau

Mécanisme de **fight back**

Vulnérabilités

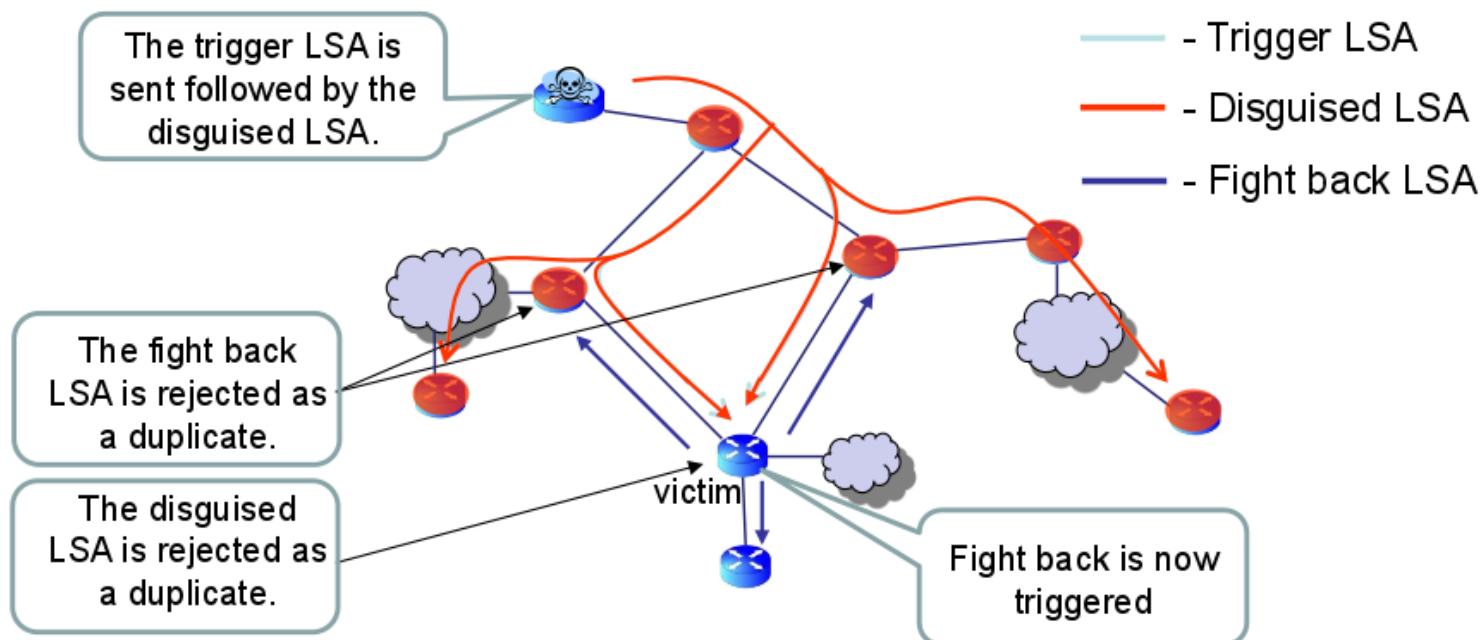
La fonction MAC d'intégrité d'OSPF n'est pas sûre

Une déclaration d'**adjacency** ne requiert pas de validation du pair

Deux LSAs sont considérées identiques si elles ont le même triplet, mais pas forcément le même contenu

Maquillage de LSA

- Un faux message LSA est propagé pour dérouter le trafic d'un routeur cible
- Pour éviter qu'il ignore comme duplicité, un LSA déclencheur est envoyé juste avant
- Le faux LSA doit anticiper la génération d'un nouveau LSA par le routeur victime



source: *Persistent OSPF Attacks*, G. Nakiby et al. (NDSS, 2012)

Rappel: Border Gateway Protocol (BGP)

Routage externe

- Les protocoles de routage externe permettent d'assurer le routage des paquets sur Internet entre ASs
- A ce niveau, le réseau est maillé mais peu structuré, et chaque AS a sa propre philosophie sur le coût des liens et son propre algorithme de routage interne

Border Gateway Protocol permet

- d'échanger des routes entre ASs indépendants
- d'implémenter les politiques de routage de chaque AS
- d'être indépendant des IGPs utilisés en interne
- de minimiser le trafic induit sur les liens
- de garantir une bonne stabilité au routage

Fonctionnement de BGP

- Granularité du routage: AS
- Sessions BGP établies point à point entre les routeurs de bord des ASs
- Sessions BGP établies via des messages **OPEN** identifiant l'AS auprès de son voisin et proposant une durée de maintien de la session
- En cas de changement, un message **UPDATE** permet d'échanger les informations de routage:
 - routes à éliminer
 - attributs de la route
 - ensemble des réseaux accessibles
- Le message **UPDATE** active le processus BGP:
 - modification des informations de routage dans la base du routeur de bord d'AS
 - émission d'un message **UPDATE** vers les autres voisins

Détournement de routes BGP

Faiblesse

Les messages de mise à jour de route ne sont pas authentifiés

Exemple

Incident Pakistan-Youtube (2008)

- Le gouvernement pakistanais a ordonné à Pakistan Telecom de bloquer Youtube
- Pakistan Telecom a alors publié une route BGP vers un sous-réseau de Youtube
- Le FAI de Pakistan Telecom n'a pas vérifié l'authenticité de la mise à jour et a commencé à la propager
- Comme la mise à jour décrit une route pour un sous-réseau plus spécifique que celui de Youtube, la plupart des ASs l'ont adopté comme route privilégiée
- De nombreux spectateurs de Youtube ont donc été redirigés vers le Pakistan, et ne purent regarder leur programme

MITM de route BGP

Diversion en Biélorussie (2013)



source: [The New Threat: Targeted Internet Traffic Misdirection](#) (Dyn Research, 2013)



Sécurité des protocoles applicatifs

SMTP, DNS, HTTP

Rappel: Simple Mail Transfer Protocol (SMTP)

Ce protocole permet à un émetteur de communiquer avec un destinataire de courrier électronique par le biais de commandes en chaînes de caractères:

- en mode connecté (supporté par TCP)
- au format texte

Une transaction SMTP consiste en l'envoi/réception de trois commandes:

- MAIL: permet de renseigner l'adresse de retour (émetteur)
- RCPT: permet de renseigner le ou les destinataires du message
- DATA: permet d'écrire le contenu du message

Usurpation d'adresse de messagerie (email spoofing)

Le protocole SMTP en lui-même ne prévoit pas de mécanisme d'authentification de l'émetteur

Le routage du message se fait sur la base du domaine de l'adresse du destinataire

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:
S: 250 Ok
C: RCPT TO:
S: 250 Ok
C: DATA
S: 354 End data with .
...
...
```

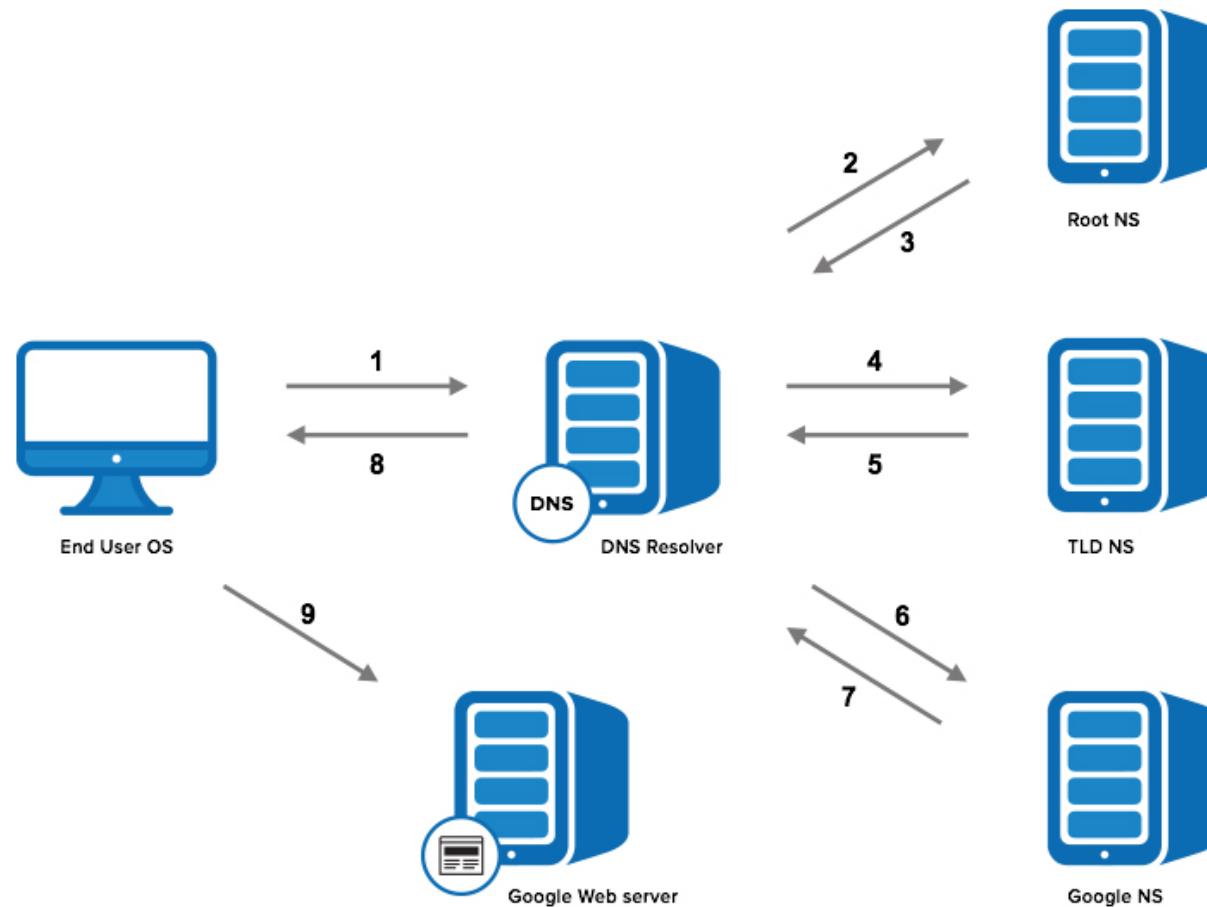
Rappel: Domain Name System (DNS)

- Système décentralisé de nommage pour tout système ou ressource connecté à Internet ou à un réseau privé
- Fournit de nombreuses informations pour un nom de domaine, en particulier, les adresses IP associées
- Les espaces de noms de domaine sont hiérarchisés en sous-domaine
- DNS repose sur un système hiérarchique de serveurs de noms qui mémorisent les correspondances entre noms et IP
 - les serveurs ROOT: pour les domaines de plus haut niveau (TLD)
 - les serveurs autoritaires (authoritative) pour les sous-domaines
 - les serveurs locaux qui maintiennent en cache un certain nombre de noms et consulte les serveurs autoritaires lorsqu'ils ne connaissent pas un nom

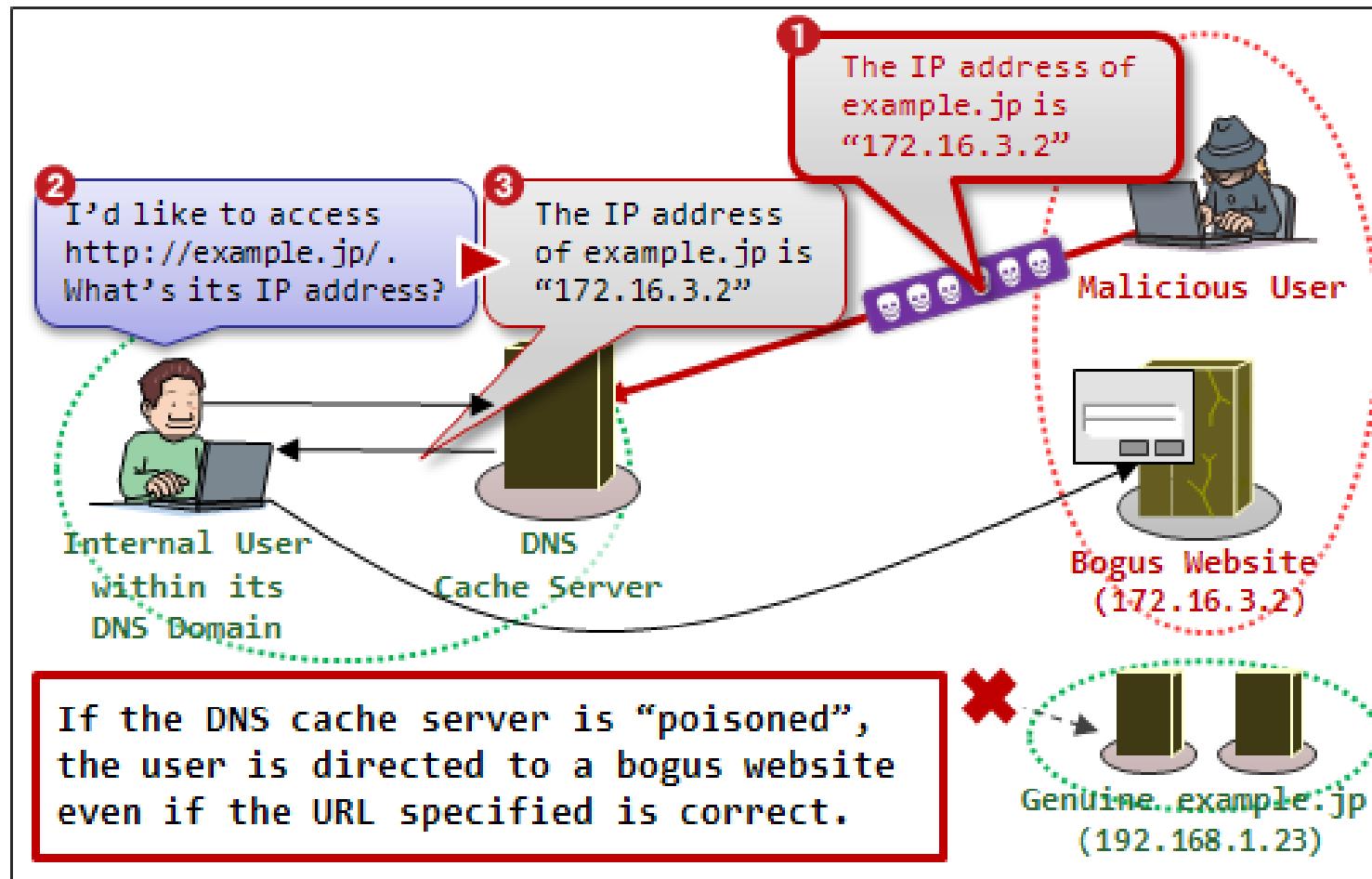
Mise en cache

- les réponses aux consultations DNS sont mises en cache afin de pallier les requêtes répétitives
- les réponses négatives sont aussi mises en cache, puisqu'elles permettent d'épargner du temps si un site n'existe pas
- les réponses ont une date de péremption (TTL) spécifiée par le propriétaire de la ressource

Consultation DNS (lookup)



Pollution du cache DNS



source: [Vulnerabilities: Security Alert for DNS Cache Poisoning \(IPA\)](#)

Amplification DNS

Open resolver

Il s'agit de serveurs DNS qui n'effectuent peu ou pas de contrôle sur les requêtes qui leur sont soumises

Principe

Un attaquant peut alors tirer avantage d'un ou plusieurs open resolvers pour monter une attaque DoS par réflexion

Attaque

En effet, DNS est un protocole basé sur UDP → un attaquant peut alors "spoofe" son adresse IP avec celle de sa victime

En émettant une requête DNS vers un grand nombre d'open resolvers, il obtient une réflexion DoS distribuée

Qui plus est, avec certains messages particuliers, il est capable d'obtenir des taux d'amplification de l'ordre de 50x

Rappel: HyperText Transfer Protocol

Le protocole d'accès au Web de type client-serveur

Repose sur un certain nombre de méthodes:

- GET
- POST
- HEAD
- CONNECT
- PUT
- TRACE

Et sur des en-têtes:

- Host
- Referer
- User-Agent

HTTP session hijacking

Principe

L'attaquant désire s'approprier la session d'un utilisateur authentifié sur un site Web

Faiblesse

Les sites Web utilisent des **cookies** afin de conserver des informations de session

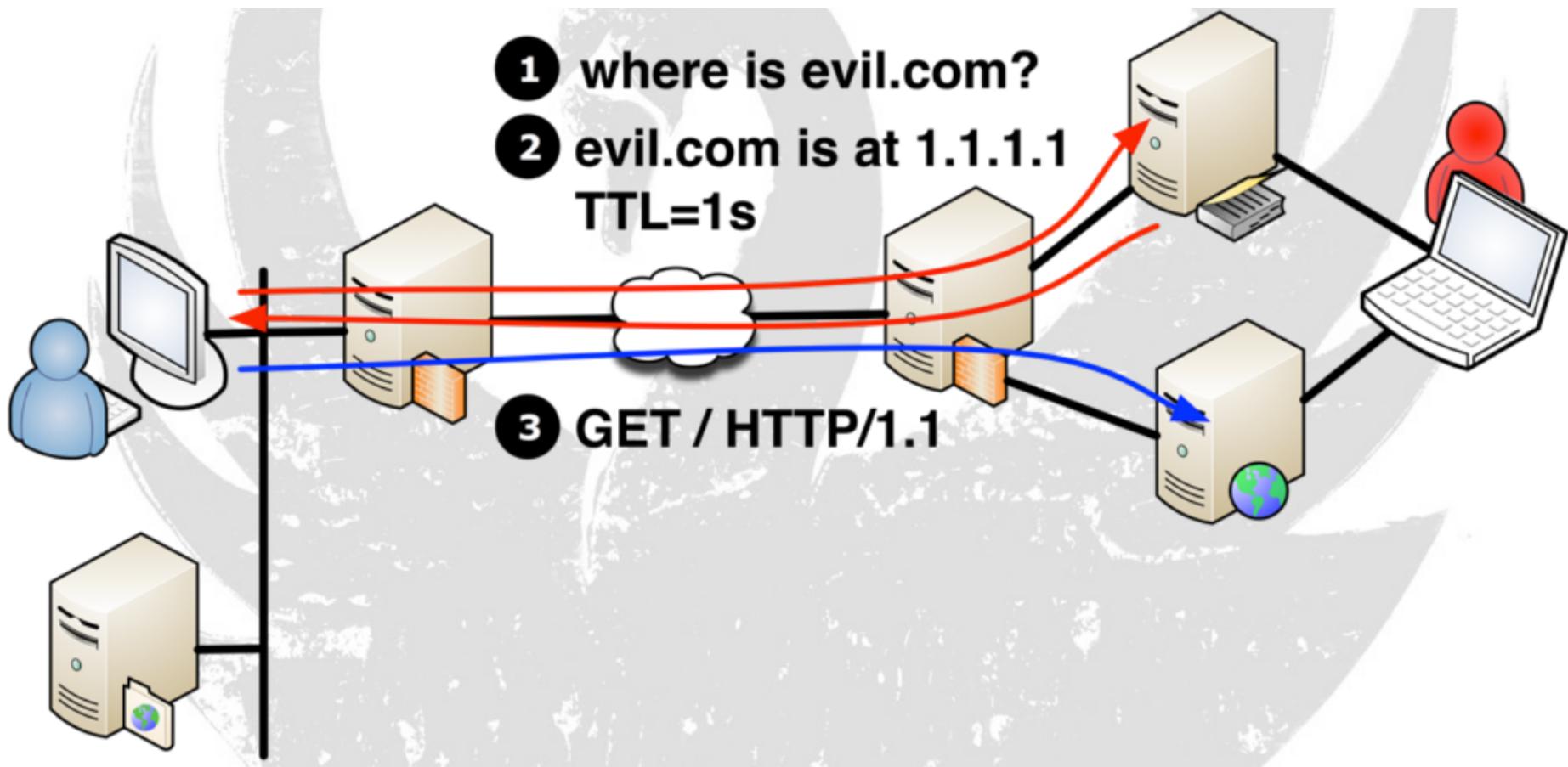
Ces cookies doivent être insérés dans une requête HTTP pour être authentifiée par le serveur comme faisant partie de la session

Attaque

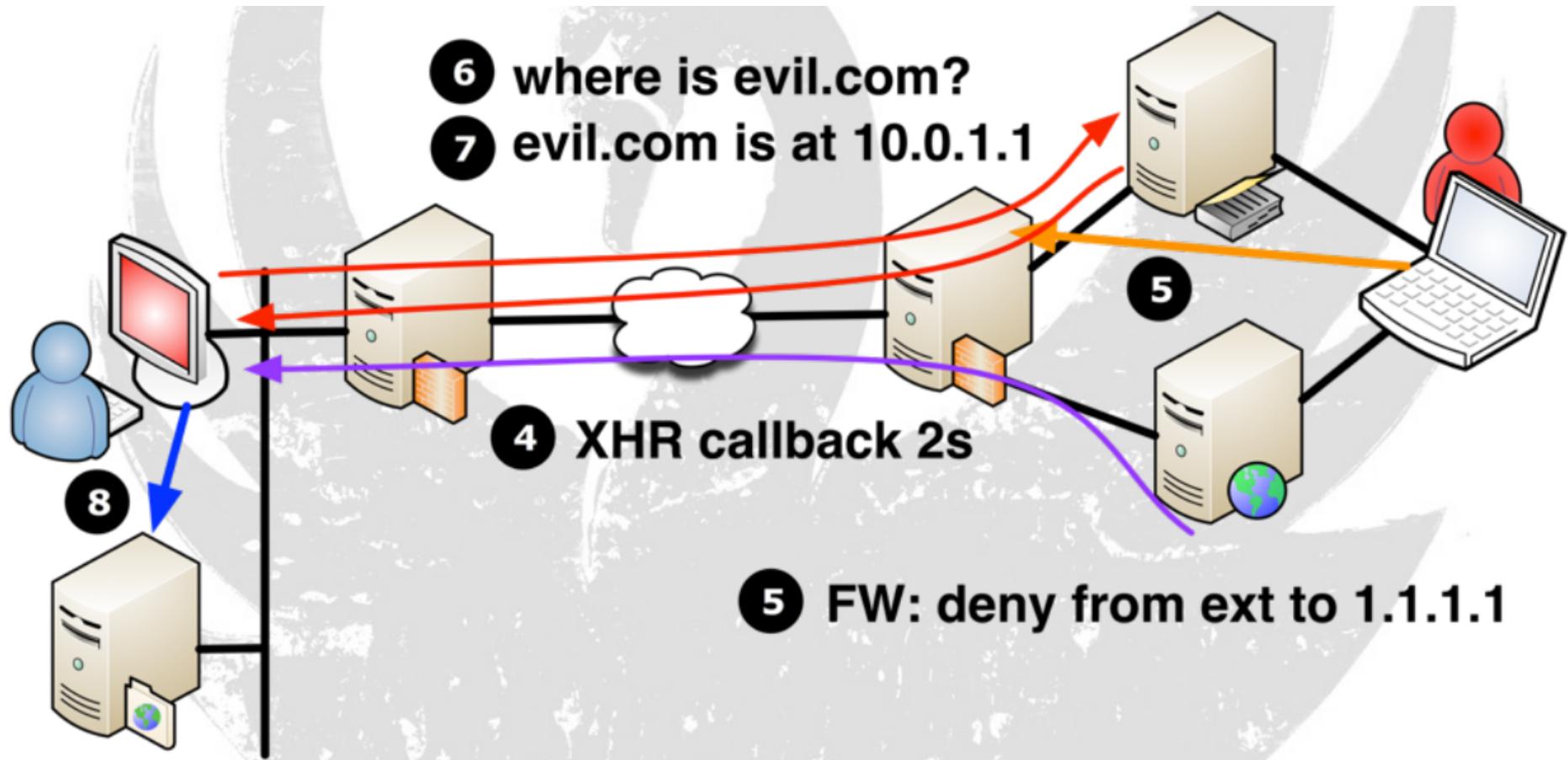
Un attaquant, pour voler une session, doit voler un cookie authentifiant la victime:

- **sniffing**: soit en écoutant le réseau, dans le cas où les transactions HTTP seraient en clair
- **cross-site scripting**: soit en piégeant la victime sur une page vulnérable où un script sera injecté pour voler le cookie

DNS Rebinding



DNS Rebinding





Sécuriser les réseaux

Equipements et protocoles de sécurité

Sécurité: les objectifs

- Confidentialité
- Intégrité
- Disponibilité
- Authentification
- Non-répudiation
- Preuve

Sécurité: les principaux mécanismes

<Merci!>



Des questions?
Ou plus tard, par email.

@ gregory.blanc@telecom-sudparis.eu

twitter [@cloudgravity](https://twitter.com/cloudgravity)

www www.blackcat.im

