

# Sécurité informatique ENSEEIH - 2AppIR

Pierre-Yves Bonnetain-Nesterenko  
[py.bonnetain@ba-consultants.fr](mailto:py.bonnetain@ba-consultants.fr)

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

2019-2020

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code. . .
- Audits et accompagnement conformité RGPD.
- Tests d'intrusion, tests d'applications.
- Réponse à incidents, analyses *post-mortem*.
- Analyses de risques, gestion des risques sur l'information.
- Ingénierie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR  
([www.ossir.org/resist](http://www.ossir.org/resist))

## Quelques références

**OSSIR** Orientation technique. [ossir.org](http://ossir.org).

**CLUSIF** Orientation organisationnel/direction.  
[clusif.asso.fr](http://clusif.asso.fr).

**Club 27001** Orientation normative. [www.club-27001.fr](http://www.club-27001.fr).

**NoLimitSécu, Le Comptoir Sécu** [nolimitsecu.fr](http://nolimitsecu.fr),  
[comptoirsecu.fr](http://comptoirsecu.fr)

**StormCast, Malicious Life** [isc.sans.edu](http://isc.sans.edu), [malicious.life](http://malicious.life)

**JSSI** Journée de la Sécurité des Systèmes d'Informations  
(mars, Paris).

**SSTIC** Conférences sécurité informatique (juin, Rennes).  
[www.sstic.org](http://www.sstic.org).

**Botconf** Conférences sur botnets (décembre).  
[www.botconf.eu](http://www.botconf.eu).

## Partie I

En guise d'échauffement

# Plan

- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

## GMail, tout le monde connaît

- Service de courrier électronique financé par la disparition de votre vie privée.
- Cadre mondial
- Une spécificité : agnostique sur les points.  
toto@gmail.com et  
t.oto...@gmail.com correspondent à la même boîte de réception.
- C'est pas du standard, mais on est Google...



### Soulignons que

Faire des fantaisies avec un standard peut se révéler dangereux, directement ou non.

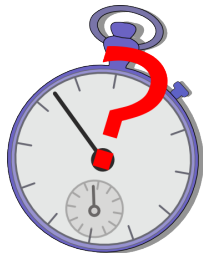
## Netflix, on connaît aussi

- Service de vidéo à la demande
- Mondial, payant
- Compte associé à adresse électronique et carte bancaire
- Respecte l'usage normal pour l'adresse électronique, le point est significatif

**NETFLIX**

## Jusqu'ici, tout va bien

- Deux services distincts, sans rapports entre eux
- Chacun, indépendamment, fonctionne correctement
- Mais si on les combine bien...





## Faire payer son abonnement par un tiers

- Identification compte Netflix associé adresse GMail

## Faire payer son abonnement par un tiers

- Identification compte Netflix associé adresse GMail
- Création nouveau compte avec variation adresse, ajout un point (de façon logique)

## Faire payer son abonnement par un tiers

- Identification compte Netflix associé adresse GMail
- Création nouveau compte avec variation adresse, ajout un point (de façon logique)
- Association carte bancaire jetable

## Faire payer son abonnement par un tiers

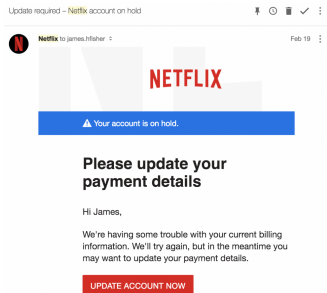
- Identification compte Netflix associé adresse GMail
- Création nouveau compte avec variation adresse, ajout un point (de façon logique)
- Association carte bancaire jetable
- Plus qu'à attendre

## Faire payer son abonnement par un tiers

- Identification compte Netflix associé adresse GMail
- Création nouveau compte avec variation adresse, ajout un point (de façon logique)
- Association carte bancaire jetable
- Plus qu'à attendre
- Possible déclencher opération validation CB

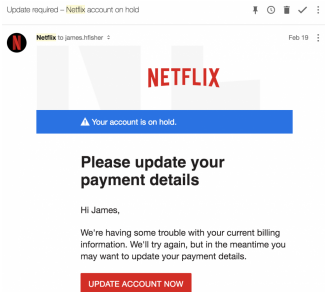
## Faire payer son abonnement par un tiers

- Identification compte Netflix associé adresse GMail
- Création nouveau compte avec variation adresse, ajout un point (de façon logique)
- Association carte bancaire jetable
- Plus qu'à attendre
- Possible déclencher opération validation CB



## Faire payer son abonnement par un tiers

- Identification compte Netflix associé adresse GMail
- Création nouveau compte avec variation adresse, ajout un point (de façon logique)
- Association carte bancaire jetable
- Plus qu'à attendre
- Possible déclencher opération validation CB



### Notons que

Le succès n'est pas garanti, suivant la vigilance de la victime potentielle.

# Plan

- 1 Interactions négatives
- 2 **Codons mal**
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau



# Plan

- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

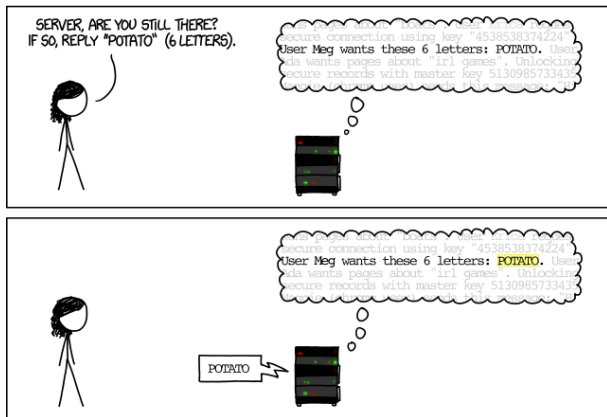
# Heartbleed - printemps 2014

- C'est quoi exactement Heartbleed ?
- Mortel, critique, grave, pas grave ?



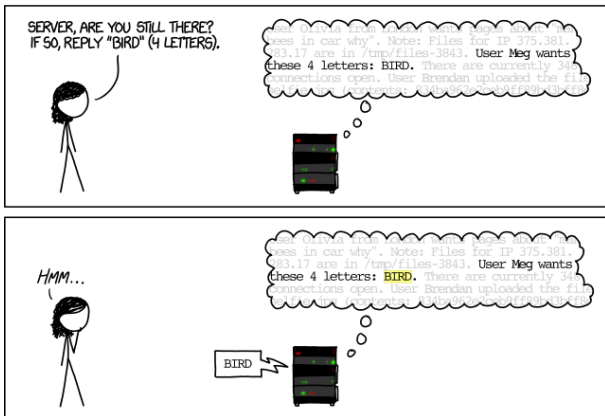
## Heartbleed - printemps 2014

Images (c) XKCD - Randall Munroe – <https://xkcd.com/1354/>



# Heartbleed - printemps 2014

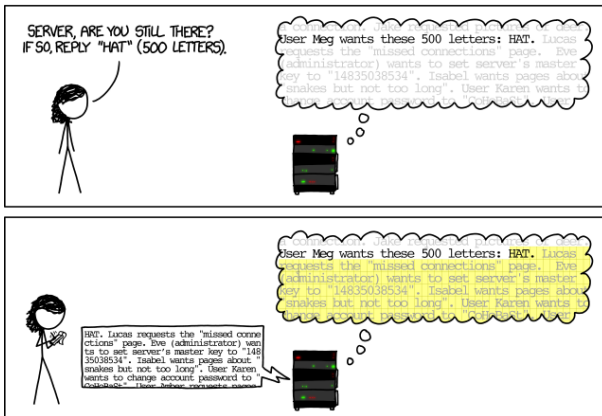
Images (c) XKCD - Randall Munroe – <https://xkcd.com/1354/>



Utilisation « créative » sous-fonction heartbeat de TLS.

# Heartbleed - printemps 2014

Images (c) XKCD - Randall Munroe – <https://xkcd.com/1354/>



Extraction d'informations de la mémoire du serveur.

## Conséquences ?

- Compromission (potentielle) des informations ayant transité dans la mémoire du serveur.
- Aucune trace, aucun élément journalisé pour confirmer ou infirmer compromission.
- Dans le doute... considérer la compromission comme avérée.

### Actions nécessaires (après mise à jour OpenSSL)

Révoquer/changer toute information sensible ayant transité par le serveur : clés de chiffrement, mots de passe... Anticiper conséquences divulgation échanges chiffrés.

### Oui mais...

Beaucoup (trop !) d'équipements (imprimantes, bornes Wifi, caméras, objets connectés...) n'ont pas de capacité de mise à jour.

## Comment est-ce possible ?

- Utilisation d'une information (ici, longueur de la chaîne reçue) fournie par l'extérieur
- Sans vérifier la validité de cette information

Ca marche souvent, mais (bugs, malveillance) c'est une mauvaise idée.

### Conclusion

- **Toujours** valider une information provenant de l'extérieur du système. L'extérieur, c'est tout sauf la RAM du processus en cours d'exécution (disque, base de données, réseau, etc.).
- Mettre une pression d'enfer sur vos fournisseurs et acheteurs pour s'assurer de la maintenabilité des équipements achetés.

## Ca c'est du code...

Février 2014 – extrait du code de SecureTransport (TLS). Utilisé par OS X et iOS pour valider les certificats X509 reçus...

```
1 SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,  
2                               uint8_t *signature, UInt16 signatureLen)  
3 {  
4     OSStatus      err;  
5  
6     ...  
7  
8     if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)  
9         goto fail;  
10    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)  
11        goto fail;  
12    goto fail;  
13    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)  
14        goto fail;  
15  
16    ...  
17  
18 fail:  
19     SSLFreeBuffer(&signedHashes);  
20     SSLFreeBuffer(&hashCtx);  
21     return err;  
22  
23 }
```

### Question

Quelle est le comportement de la fonction ?





## Oui mais ensuite ?

- Second goto (ligne 12) met un terme aux contrôles du certificat reçu
- err vaut zéro (fonction ligne 10 renvoie 0).
- return err; (ligne 21) renvoie zéro = succès.
- Conséquence ?
  - Certificat n'est pas complètement validé par l'application
  - Faux certificat signé par une AC quelconque
  - Ou un certificat sans signature
  - $\Rightarrow$  attaque par intermédiation (MITM) triviale
- En bref : TLS n'offre plus aucune protection.

### Un peu de perspective...

Tout ça avec une seule ligne de code, 11 caractères en comptant les espaces.

# Plan

- 1 Interactions négatives
- 2 **Codons mal**
  - A haut niveau
  - **Toujours plus bas**
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

# Spectre et Meltdown, janvier 2018

- C'est quoi ?
- Mortel, critique, grave, pas grave ?

GILBERT DELAHAYE - MARCEL MARLIER

## martine

Martine gère un parc de serveurs



castellani



## Exfiltration de données

- Vulnérabilité existe probablement depuis 1995
- Programme *userland*
- Exploitation optimisation micro-processeurs  
(réordonnancement spéculatif instructions) → attaque temporelle (timing attack) sur cache micro-processeur
- Accès indirect (canal caché) à mémoire protégée
  - Spectre : espace noyau rattaché au processus
  - Meltdown : mémoire d'autres processus

## Le plus drôle

- Tout système pouvant exécuter du code non-contrôlé est vulnérable
- Navigateurs : exploitation possible via Javascript → attention où vous surfez ! Bloquer les pubs voire JS ?
- Téléphones portables : navigateur, applications malveillantes... idem
- Systèmes mutualisés : processus client peut lire la mémoire de tous les autres processus

### Machines virtuelles

Meltdown permet à un processus dans une MV de lire la mémoire d'autres MV sur le même hyperviseur...

## Solutions

- ❶ Jeter/remplacer processeurs actuels (post-1995) Intel, AMD et ARM... mais quels remplaçants ???
- ❷ Correctifs noyau, dégradation possible performances
- ❸ Correctifs micro-code processeurs à déployer

### Déjà que...

Correctifs « logiciels » pas toujours installés (objets connectés, téléphones portables...), espérer micro-code rapidement mis à jour très optimiste  $\Rightarrow$  problème va rester très longtemps.

### Mais c'est pas fini

Déplacement investigations sécurité vers micro-code (périphériques, processeurs)  $\rightarrow$  début découvertes vulnérabilités matérielles.

## Quelques références

- <https://meltdownattack.com/meltdown.pdf>
- <https://spectreattack.com/spectre.pdf>
- <https://www.raspberrypi.org/blog/why-raspberry-pi-isnt-vulnerable-to-spectre-or-meltdown/>
- [https://www.schneier.com/blog/archives/2018/01/spectre\\_and\\_mel\\_1.html](https://www.schneier.com/blog/archives/2018/01/spectre_and_mel_1.html)

# Plan

- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

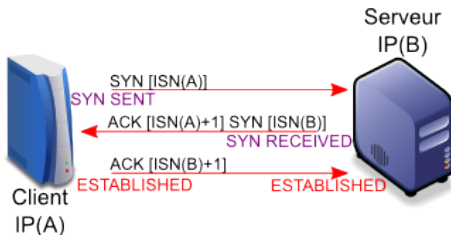


# Plan

- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

## Etablissement de connexion TCP

Trois paquets doivent circuler avant que la connexion ne soit établie.



- Le serveur et le client réservent des ressources pour identifier et gérer la connexion
- Ces ressources sont puisées dans l'espace réservé au noyau
- donc en quantité limitée.

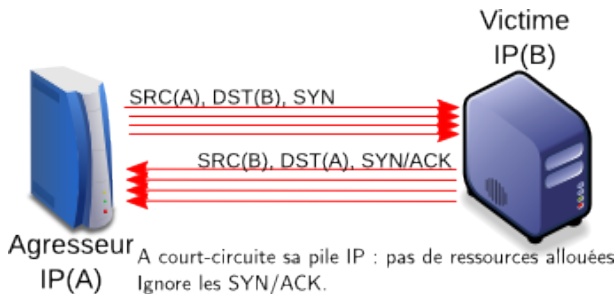
## Inondation SYN ?

À partir du schéma d'établissement de connexion TCP...

- Qu'est-ce qu'une inondation SYN (SYN flood) ?
- Comment et pourquoi cela fonctionne-t-il ?



## Inondation SYN



Oui mais...

Il y a un (très gros) inconvénient à ce mode de fonctionnement.  
Lequel ?

# Plan

- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

## Mascarade IP ?

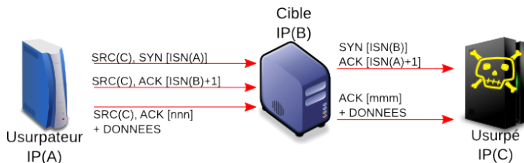
À partir du schéma d'établissement de connexion TCP...  
En supposant que l'agresseur n'est pas sur le chemin des données

- Qu'est-ce qu'une « vraie » mascarade IP (IP spoofing) ?
- Comment est-ce que cela fonctionne pour l'agresseur ?
- Quelles vulnérabilités sont-elles exploitées ?



## Une vraie mascarade IP

- Attaque **en aveugle** sauf si A sur chemin des paquets
- A ne voit pas les réponses **donc** nécessité de deviner ISN(B) et ses incréments
- ISN joue (indirectement/involontairement) rôle d'un authentifiant
- C ne doit pas répondre, sinon envoie un RST.



### Ca a marché

Quand l'ISN peut être calculé/estimé (incrémentation constante, etc.). Aujourd'hui, aléatoire...

# Empoisonnement DNS

## Heureusement

Une attaque aussi simpliste n'est plus possible depuis longtemps.

- Interrogation DNS client → solveur → serveur



# Empoisonnement DNS

## Heureusement

Une attaque aussi simpliste n'est plus possible depuis longtemps.

- Interrogation DNS client → solveur → serveur
- Identifiant de requête (QID) renvoyé par le serveur

# Empoisonnement DNS

## Heureusement

Une attaque aussi simpliste n'est plus possible depuis longtemps.

- Interrogation DNS client → solveur → serveur
- Identifiant de requête (QID) renvoyé par le serveur
- Donc, QID sert d'authentifiant de la réponse

# Empoisonnement DNS

## Heureusement

Une attaque aussi simpliste n'est plus possible depuis longtemps.

- Interrogation DNS client → solveur → serveur
- Identifiant de requête (QID) renvoyé par le serveur
- Donc, QID sert d'authentifiant de la réponse
- Et si je devine le QID ?

# Empoisonnement DNS

## Heureusement

Une attaque aussi simpliste n'est plus possible depuis longtemps.

- Interrogation DNS client → solveur → serveur
- Identifiant de requête (QID) renvoyé par le serveur
- Donc, QID sert d'authentifiant de la réponse
- Et si je devine le QID ?

## Et si je devine le QID ?

Je peux envoyer une fausse réponse DNS qui sera acceptée comme valide par le solveur, stockée et préservée jusqu'à l'expiration du TTL.

# Empoisonnement DNS

- Il y a très, très longtemps : incrémentation monotone du QID (+1) à chaque requête. Empoisonnement trivial
- Pré-2008 : QID, entropie 16 bits (64K possibilités).
- 2008 : attaque dite « Kaminsky », 16 bits d'entropie se révèlent insuffisants pour empêcher de deviner les QID avec un bon taux de succès.

## Solutions

Augmenter entropie requête (27 bits ; QID : 16, port source : 11).  
Jeu sur les casses de caractères dans la requête. DNSSEC  
(authentification des réponses).

# Plan

- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

## Sur un serveur DNS

- Serveur DNS gérant plusieurs domaines
- Reçoit des requêtes sur des domaines *qu'il ne gère pas* :  
security: client 89.248.172.121#33451 : query  
(cache) 'hizbullah.me/ANY/IN'  
security: client 60.28.246.143#50469 : query  
(cache) 'google.com/A/IN'  
security: client 94.102.52.44#56963 : query  
(cache) './ANY/IN'
- A quoi cela correspond-il ?
- Légitime ? Pas légitime ?
- Qui est l'agresseur ? La victime ?



# Attaque par amplification DNS

Si solveur DNS mal configuré (récursif et ouvert), alors...

- caisse de résonance significative et gratuite
- difficile de remonter en amont (trace inverse paquets entrants).
- requête entrante faible taille (83 octets), sortante forte taille (4031 octets) → amplification facteur 50 environ.
- adresse IP source requête entrante falsifiée, future victime.
- Requêtes sortantes dirigées vers la victime.

## Déni de service distribué

100 000 machines qui jouent à ça...

Trois paquets par seconde et par machine...

Flux terminal  $100000 \times 4031 \times 3 \times 8 \approx 9 \text{ Gbits/s}$

⇒ déni de service sur la connexion de la victime.



## Pendant qu'on y est. . .

- Résultat de la requête vers `hizbullah.me` ?



## Pendant qu'on y est...

- Résultat de la requête vers hizbullah.me ?
- En août 2013, cela donnait

```
$ dig -t any hizbullah.me
;; ANSWER SECTION:
hizbullah.me. 85295 IN SOA ns1.hizbullah.me. admin.hizbullah.me.
      2012292301 28800 86400 3600000 86400
hizbullah.me. 695 IN A 204.46.43.137
hizbullah.me. 695 IN A 204.46.43.211
hizbullah.me. 695 IN A 204.46.43.17
[ 240 lignes semblables... ]
hizbullah.me. 695 IN A 204.46.43.96
hizbullah.me. 695 IN A 204.46.43.59
hizbullah.me. 695 IN NS ns1.hizbullah.me.

;; ADDITIONAL SECTION:
ns1.hizbullah.me. 85295 IN A 200.241.86.132
```



## Pendant qu'on y est...

- Résultat de la requête vers hizbullah.me ?
- En août 2013, cela donnait

```
$ dig -t any hizbullah.me
;; ANSWER SECTION:
hizbullah.me. 85295 IN SOA ns1.hizbullah.me. admin.hizbullah.me.
2012292301 28800 86400 3600000 86400
hizbullah.me. 695 IN A 204.46.43.137
hizbullah.me. 695 IN A 204.46.43.211
hizbullah.me. 695 IN A 204.46.43.17
[ 240 lignes semblables... ]
hizbullah.me. 695 IN A 204.46.43.96
hizbullah.me. 695 IN A 204.46.43.59
hizbullah.me. 695 IN NS ns1.hizbullah.me.

;; ADDITIONAL SECTION:
ns1.hizbullah.me. 85295 IN A 200.241.86.132
```

- Vous en pensez quoi ?



# A qui appartient le réseau 204.46.43 ?

- .me : Montenegro.

## WHOIS/IPWHOIS Lookup Results for 204.46.43.0

### Results for Target: 204.46.43.0

Created Date : 1994-05-19  
Updated Date : 2002-03-01  
WHOIS Server: whois.arin.net

### Discovered Nameservers

[ NOT DETECTED ]

\*Please note these results are obtained from third party databases (

## Contact Information

### Registrant

NC 54 at Alexander Drive  
NC  
US  
U.S. Environmental Protection Agency

## A qui appartient le réseau 204.46.43 ?

- .me : Montenegro.
- WhoIS sur 204.46.43 :  
US Environmental  
Protection Agency.

IP Information Results for 204.46.43.0

Country	Country Code	Region	City	Latitude	Longitude
us	us	nc	durham	36.016998	-78.949997
United States	US	North Carolina	not found	35.227100	-80.843102
UNITED STATES	US	NORTH CAROLINA	DURHAM	35.994030	-78.898621

## A qui appartient le réseau 204.46.43 ?

- .me : Montenegro.
- WhoIS sur 204.46.43 :  
US Environmental  
Protection Agency.
- Implantation  
nord-américaine (Caroline  
du Nord).

IP Information Results for 204.46.43.0

Country	Country Code	Region	City	Latitude	Longitude
us	us	nc	durham	36.016998	-78.949997
United States	US	North Carolina	not found	35.227100	-80.843102
UNITED STATES	US	NORTH CAROLINA	DURHAM	35.994030	-78.898621

## A qui appartient le réseau 204.46.43 ?

- .me : Montenegro.
- WhoIS sur 204.46.43 :  
US Environmental  
Protection Agency.
- Implantation  
nord-américaine (Caroline  
du Nord).

IP Information Results for 204.46.43.0

Country	Country Code	Region	City	Latitude	Longitude
us	us	nc	durham	36.016998	-78.949997
United States	US	North Carolina	not found	35.227100	-80.843102
UNITED STATES	US	NORTH CAROLINA	DURHAM	35.994030	-78.898621

### Attention

DNSSec ne changera rien à ce problème

## A qui appartient le réseau 204.46.43 ?

- .me : Montenegro.
- WhoIS sur 204.46.43 :  
US Environmental  
Protection Agency.
- Implantation  
nord-américaine (Caroline  
du Nord).

IP Information Results for 204.46.43.0

Country	Country Code	Region	City	Latitude	Longitude
us	us	nc	durham	36.016998	-78.949997
United States	US	North Carolina	not found	35.227100	-80.843102
UNITED STATES	US	NORTH CAROLINA	DURHAM	35.994030	-78.898621

### Attention

DNSSec ne changera rien à ce problème

Juste pour rire ... un peu

Résolution domaine hizbullah.me considérée comme accès site organisation terroriste ?



# Plan

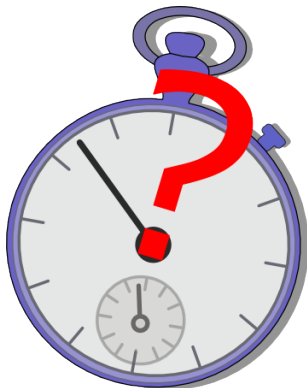
- 1 Interactions négatives
- 2 Codons mal
  - A haut niveau
  - Toujours plus bas
- 3 Jouons avec des identifiants
  - TCP, ISN et autres
  - Mascarade
- 4 Jouons avec le DNS
- 5 Sniffons le réseau

## Il est beau mon réseau local...

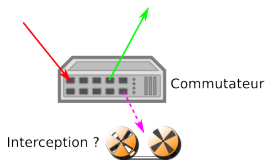
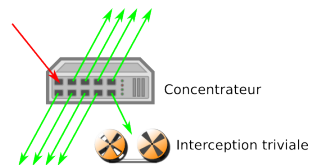
Un cas d'école...

- Réseau simple (bâtiment, étage, plateau...)
- Construit en étoile autour de commutateurs réseau

Comment intercepter les paquets qui circulent sur le réseau ?



## Concentrateurs et commutateurs



- Principales différences entre les commutateurs (switch) et les concentrateurs (hubs)
  - Concentrateur (presqu'absent aujourd'hui) diffuse sur tous ses ports
  - Commutateur envoie sur le port où le destinataire est joignable
- Concentrateur : interception triviale, par nature.
- Commutateur : interception facile si on sait comment fonctionne un commutateur.

## Interception locale

Trois grandes possibilités :

**Configuration commutateur** Accès au commutateur, mot de passe standard ou trivial, activation port mirroring.

**Fonctionnement commutateur** Attaque du commutateur par dépassement de ses capacités. Problème : maintenir la saturation.

- Visible pour les exploitants (saturation)
- Imparfait (certains paquets ne seront pas vus quand même)

**Protocole sous-jacent** Attaque d'un protocole lié à Ethernet (niveau 2)

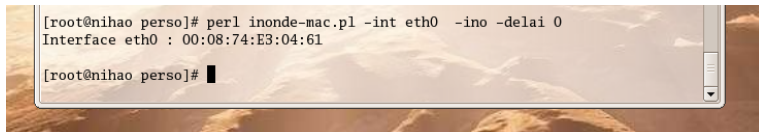
### Une conséquence

Même sur le réseau local, pas d'échanges en clair.

## Un commutateur qui va paniquer

Saturation de la table *Adresse MAC* ↔ *Port* par envoi de paquets ARP « gratuits ».

- Commutateur : composant de télécommunications, **pas** de sécurité.
- Incident ⇒ mission d'abord ⇒ transmettre les paquets ⇒ sur tous les ports.
- 20 lignes de Perl suffisent.

A terminal window with a light brown background and a dark border. The text inside shows a root user at a machine named 'nihao' in a directory 'perso' running a Perl script 'inonde-mac.pl' with arguments '-int eth0 -ino -delai 0'. The output shows the interface 'eth0' with MAC address '00:08:74:E3:04:61'. The prompt returns to the root user.

```
[root@nihao perso]# perl inonde-mac.pl -int eth0 -ino -delai 0
Interface eth0 : 00:08:74:E3:04:61

[root@nihao perso]#
```

# Un commutateur qui va paniquer

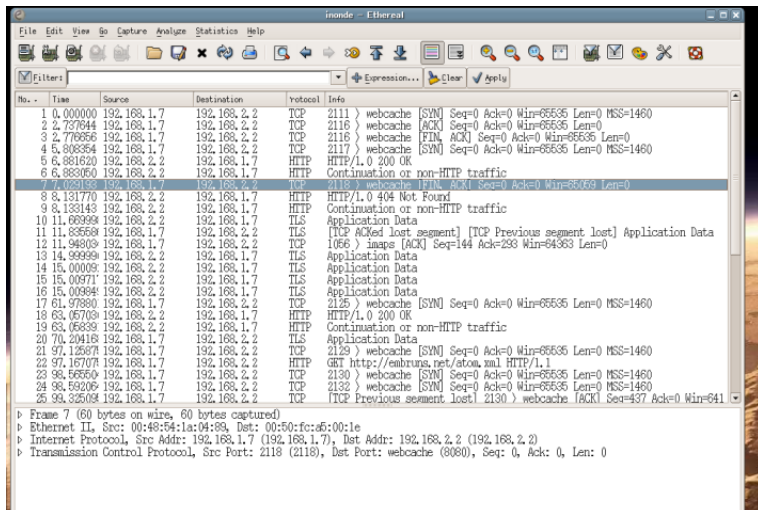
Saturation de la table *Adresse MAC*  $\leftrightarrow$  *Port* par envoi de paquets ARP « gratuits ».

- Commutateur : composant de télécommunications, **pas** de sécurité.
- Incident  $\Rightarrow$  mission d'abord  $\Rightarrow$  transmettre les paquets  $\Rightarrow$  sur tous les ports.
- 20 lignes de Perl suffisent.

```
[root@nihao ~]# tethereal -i eth0 -n not arp and not \( \( tcp or udp \) and host 192.168.1.2 \)
Capturing on eth0
0.000000 192.168.2.2 -> 192.168.1.7 TLS Application Data
0.158112 192.168.1.7 -> 192.168.2.2 TLS [TCP ACKed lost segment] [TCP Previous segment lost] Application Data
3.129922 192.168.2.2 -> 192.168.1.7 TLS Application Data
3.139679 192.168.2.2 -> 192.168.1.7 TLS Application Data
3.139776 192.168.2.2 -> 192.168.1.7 TLS Application Data
3.139891 192.168.2.2 -> 192.168.1.7 TLS Application Data
```

# Un commutateur qui panique

Manque parfois des morceaux (ici, entre paquets 16 et 17) :

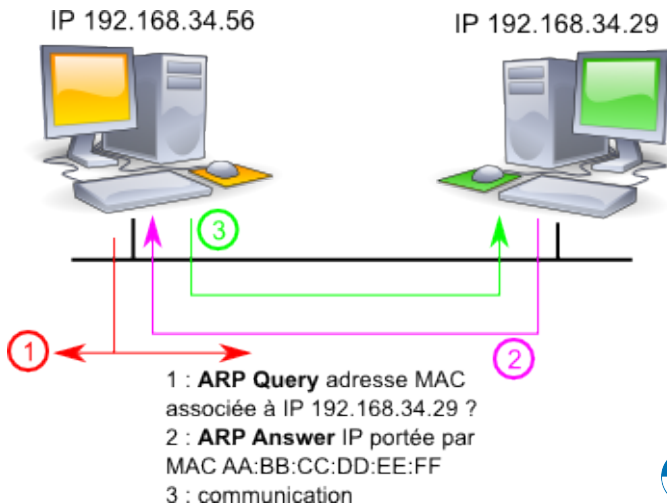


The image shows a Wireshark packet capture window titled "inonde - Ethereal". The packet list on the left shows a sequence of packets from 1 to 25. Packet 16 is a TCP segment (Seq=0, Ack=0, Win=65535, Len=0) from 192.168.1.7 to 192.168.2.2. Packet 17 is a TCP segment (Seq=0, Ack=0, Win=65535, Len=0) from 192.168.1.7 to 192.168.2.2. The packet details pane on the right shows the structure of the selected packet (packet 16), including Ethernet II, Internet Protocol, and Transmission Control Protocol fields. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.7	192.168.2.2	TCP	2111 > webcache [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
2	2.737644	192.168.1.7	192.168.2.2	TCP	2116 > webcache [ACK] Seq=0 Ack=0 Win=65535 Len=0
3	2.776666	192.168.1.7	192.168.2.2	TCP	2116 > webcache [FIN, ACK] Seq=0 Ack=0 Win=65535 Len=0
4	5.808354	192.168.1.7	192.168.2.2	TCP	2117 > webcache [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
5	6.881620	192.168.2.2	192.168.1.7	HTTP	HTTP/1.0 200 OK
6	6.883050	192.168.2.2	192.168.1.7	HTTP	Continuation or non-HTTP traffic
7	7.029193	192.168.1.7	192.168.2.2	TCP	2118 > webcache [FIN, ACK] Seq=0 Ack=0 Win=65535 Len=0
8	8.131770	192.168.2.2	192.168.1.7	HTTP	HTTP/1.0 404 Not Found
9	8.133143	192.168.2.2	192.168.1.7	HTTP	Continuation or non-HTTP traffic
10	11.669999	192.168.2.2	192.168.1.7	TLS	Application Data
11	11.835568	192.168.1.7	192.168.2.2	TLS	[TCP ACKed lost segment] [TCP Previous segment lost] Application Data
12	11.948039	192.168.1.7	192.168.2.2	TCP	1066 > imap5 [ACK] Seq=144 Ack=238 Win=64363 Len=0
13	14.999999	192.168.2.2	192.168.1.7	TLS	Application Data
14	15.000009	192.168.2.2	192.168.1.7	TLS	Application Data
15	15.009711	192.168.2.2	192.168.1.7	TLS	Application Data
16	15.009844	192.168.2.2	192.168.1.7	TLS	Application Data
17	61.978800	192.168.1.7	192.168.2.2	TCP	2125 > webcache [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
18	63.057039	192.168.2.2	192.168.1.7	HTTP	HTTP/1.0 200 OK
19	63.058339	192.168.2.2	192.168.1.7	HTTP	Continuation or non-HTTP traffic
20	70.204168	192.168.1.7	192.168.2.2	TLS	Application Data
21	97.126877	192.168.1.7	192.168.2.2	TCP	2129 > webcache [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
22	97.167074	192.168.1.7	192.168.2.2	HTTP	GET http://enbruns.net/atom.xml HTTP/1.1
23	98.565559	192.168.1.7	192.168.2.2	TCP	2130 > webcache [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
24	98.592069	192.168.1.7	192.168.2.2	TCP	2132 > webcache [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
25	99.325034	192.168.1.7	192.168.2.2	TCP	[TCP Previous segment lost] 2130 > webcache [ACK] Seq=437 Ack=0 Win=641

Frame 7 (60 bytes on wire, 60 bytes captured)  
Ethernet II, Src: 00:48:54:1a:04:89, Dst: 00:50:fc:a5:00:1e  
Internet Protocol, Src Addr: 192.168.1.7 (192.168.1.7), Dst Addr: 192.168.2.2 (192.168.2.2)  
Transmission Control Protocol, Src Port: 2118 (2118), Dst Port: webcache (8080), Seq: 0, Ack: 0, Len: 0

# Fonctionnement ARP





# Mascarade ARP

- Echanges sur un segment Ethernet n'utilisent pas adresse IP mais adresse MAC (physique) du destinataire.
- ARP (Adress Resolution Protocol) pour initialiser l'échange : « quelle adresse MAC porte l'adresse IP a.b.c.d ? »
- Pas d'authentification des paquets ARP
- Mascarade (ou empoisonnement) : signaler qu'une certaine adresse IP est « maintenant » portée par notre adresse MAC.

## Résultat

Détournement/interception d'un échange local (y compris s'il est déjà en cours)

## Pas toujours malveillant

Fonctionnement des boîtiers redondants (type HSRP).

## Mascarade ARP

- Echanges sur un segment Ethernet n'utilisent pas adresse IP mais adresse MAC (physique) du destinataire.
- ARP (Adress Resolution Protocol) pour initialiser l'échange :  
« quelle adresse MAC porte l'adresse IP a.b.c.d ? »
- Pas d'authentification des paquets ARP
- Mascarade (ou empoisonnement) : signaler qu'une certaine adresse IP est « maintenant » portée par notre adresse MAC.

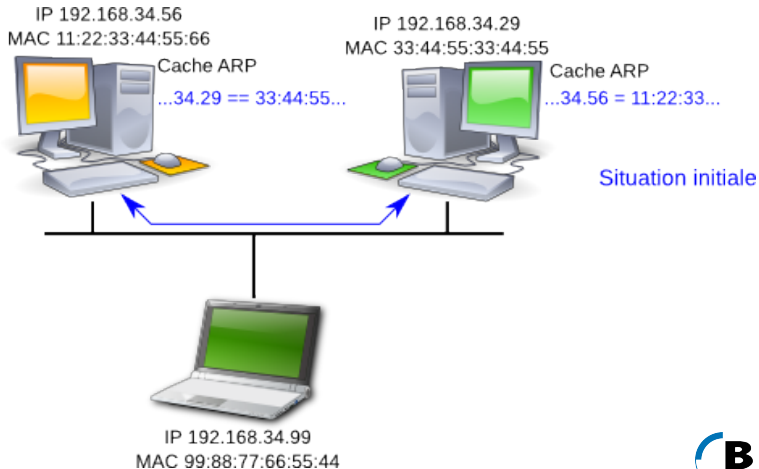
### Résultat

Détournement/interception d'un échange local (y compris s'il est déjà en cours)

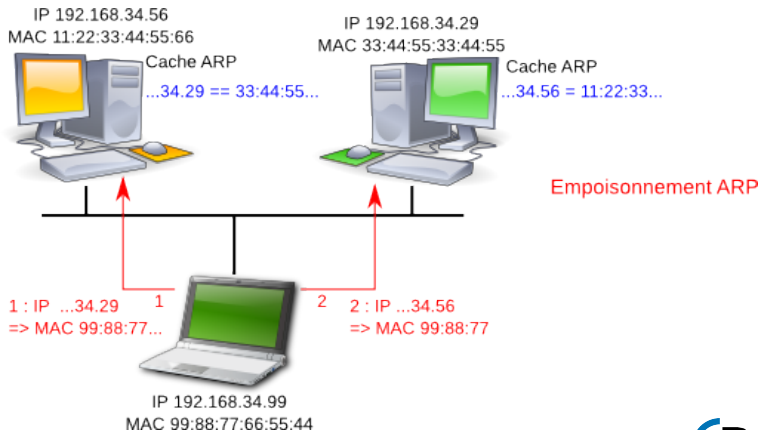
### Conclusion

Chiffrement des flux. Tout le temps. En interne comme en externe.

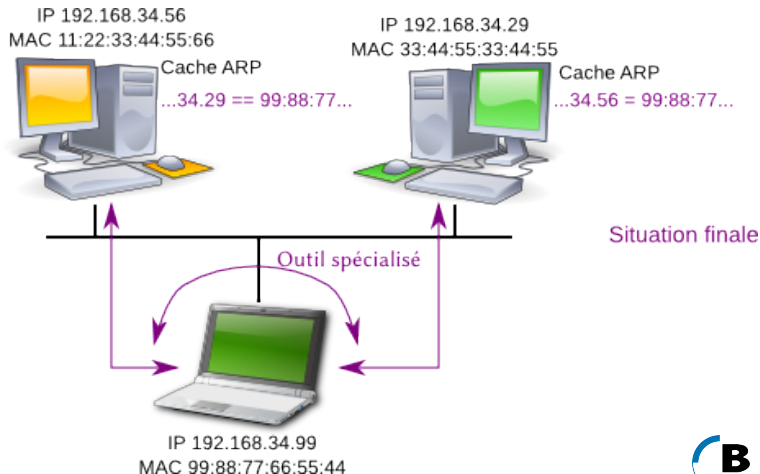
# Empoisonnement ARP



# Empoisonnement ARP



# Empoisonnement ARP



## Dans la même veine...

- Pouvez-vous trouver d'autres protocoles permettant des « fantaisies » similaires ?

## Dans la même veine...

- Pouvez-vous trouver d'autres protocoles permettant des « fantaisies » similaires ?
- ... protocoles internes à un réseau ?

## Dans la même veine...

- Pouvez-vous trouver d'autres protocoles permettant des « fantaisies » similaires ?
- ... protocoles internes à un réseau ?
- DHCP, BootP



## Dans la même veine...

- Pouvez-vous trouver d'autres protocoles permettant des « fantaisies » similaires ?
- ... protocoles internes à un réseau ?
- DHCP, BootP
- ... ou protocole externe, global ?

## Dans la même veine...

- Pouvez-vous trouver d'autres protocoles permettant des « fantaisies » similaires ?
- ... protocoles internes à un réseau ?
- DHCP, BootP
- ... ou protocole externe, global ?
- BGP