

Il faut s'occuper de « Nos oignons »

WhilelM <whilelm@doomfr.com>

23 juin 2013, PSES2013

Presentation :

- Copyright 2013 © Lunar
lunar@anargeek.net,
whilelm@doomfr.com
- License : CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0/>

Image copyrights need to be verified.

Salut !

Je m'appelle WhilelM et je m'intéresse à l'administration système et aux services internet depuis quelques années

Tor

Dans cette présentation, je vais surtout vous parler de Tor. Tor est un système permettant d'anonymiser les connexions sur Internet et de contourner la censure.

Pour cela, le principe utilisé est celui du « routage en oignon ». On y reviendra. Mais c'est pour ça que les gens qui bossent autour de Tor sont un peu fétichiste des oignons (*allium cepa* pour les botanistes).

Sondage :

- Qui utilise Tor ?
- Qui connaît le fonctionnement de Tor ?



Qu'est-ce que Tor ?

Tor c'est plein de choses.

- Tor est un **logiciel libre**,
- grâce auquel existe le **réseau d'anonymisation Tor**
- soutenu par l'organisation **The Tor Project**.

Et... euh... c'est « Tor », pas « TOR » : ce n'est pas un acronymie.

Techniquement, Tor nous permet de se connecter à des machines sur Internet via des relais. Et cela de façon à ce qu'elles ne puissent pas identifier notre connexion (et donc de nous localiser).

Concrètement, ça sert pour :

- échapper au fichage publicitaire,
- publier des informations sous un pseudonyme,
- accéder à des informations en laissant moins de traces,
- déjouer des dispositifs de filtrage (dans sa fac, en Chine ou en Iran...),
- communiquer en déjouant des dispositifs de surveillances,
- tester son pare-feu,
- ... et sûrement encore d'autres choses.

Tor dispose également d'un système de « services cachés » qui permet de fournir un service en cachant l'emplacement du serveur.

Combien de personnes utilisent Tor ?

On estime entre 500 000 et 900 000 le nombre de personnes utilisant Tor chaque jour.



cf. <https://metrics.torproject.org/users.html>

Tor est un réseau d'anonymisation, donc par définition, c'est difficile de faire un compte précis.

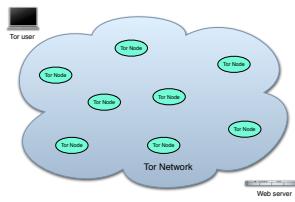
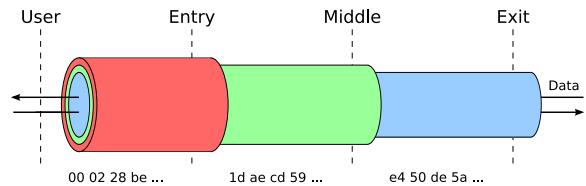
Tor ne fait rien pour cacher que nous utilisons Tor. Donc quand en utilisant Tor, nous nous mettons au milieu de la foule des gens qui utilisent Tor. Plus cette foule est grande, meilleur est l'anonymat.

C'est peut-être ce qui explique que tant de personnes convergent vers Tor : pour l'utiliser, pour l'améliorer, pour y faire de la recherche.

Comment fonctionne Tor ?

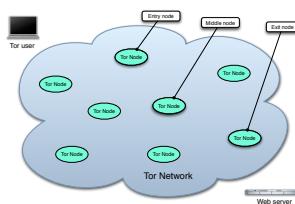
Tor fonctionne grâce à plus de 3000 machines que font tourner des bénévoles. Voici en gros comment se passe une connexion anonyme d'un navigateur configuré pour utiliser Tor vers un serveur web.

La liste de tous les relais (qu'on appelle aussi noeuds) qui composent le réseau Tor est publique. Le client Tor commence donc par la télécharger afin de se faire une image du réseau.



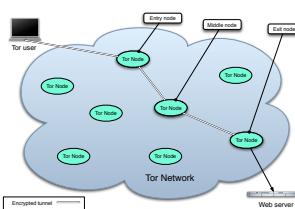
Comment fonctionne Tor ?

Ensuite, le client va choisir trois noeuds au hasard.



Comment fonctionne Tor ?

Après, se déroule tout un processus pour établir un tunnel chiffré jusqu'au noeud de sortie.



Comment fonctionne Tor ?

Ces tunnels se font « en oignon » avec des couches de chiffrement empilées. Il y a une première clé de chiffrement vers le noeud d'entrée, une second clé vers le noeud du milieu et une dernière pour le noeud de sortie.

Il faut noter que Tor ne s'occupe pas de chiffrer après le noeud de sortie. Comme n'importe qui peut mettre en place un noeud de sortie, c'est une bonne idée de chiffrer sa communication en plus (par exemple en se connectant aux sites web que l'on visite en HTTPS).

Utiliser Tor : le Tor Browser Bundle

Tor est un réseau. Tout comme Internet, il y a donc plein de manières de l'utiliser. Alors pour faire court, deux méthodes simples pour s'en servir.

Le Tor Browser Bundle est produit par le projet Tor. Il contient ce qu'il faut pour se connecter au réseau, ainsi qu'un navigateur basé sur Firefox.



Utiliser Tor : Tails

Si on veut d'autres usages que simplement le web, ou qu'on a besoin d'une garantie plus grande de ne pas laisser de traces, on peut utiliser le système live Tails.

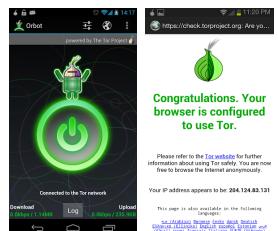
Tails est un système d'exploitation complet basé sur Linux et Debian. Peu importe donc que l'ordinateur fonctionne habituellement avec Windows ou Linux.

Comme c'est un système complet, il est plus difficile de faire des erreurs compromettantes. Comme de coller un lien vers son navigateur habituel plutôt que vers le Tor Browser.



Utiliser Tor : Orbot & Orweb

Sur les téléphones Android, le Guardian Project met à disposition Orbot (un port de Tor) et Orweb (un navigateur web dédié).



Les attaques par confirmation

Tor est un réseau à faible latence.

La latence, c'est le temps nécessaire pour que les données traversent le réseau.

« Faible latence », ça veut dire si on y fait entrer un paquet de données, on le retrouve, un tout petit peu plus tard, de l'autre côté.

Le contraire, c'est les réseaux à « forte latence » telle que La Poste : une lettre devrait arriver entre 11h et 13h quelques jours après avoir été postée...

Dans les réseaux d'anonymisation à faible latence, si un adversaire est capable d'écouter au deux bouts en même temps, il peut percer l'anonymat. Peu importe le chiffrement, il suffit de regarder la forme et la fréquence des communications.

Un exemple : Val publie régulièrement des photos sur son blog pour dénoncer les dégâts environnementaux commis par son entreprise. Dans la boîte, uniquement la dizaine de cadres de la filiale française pouvaient être au courant. L'entreprise a des sous — avec les économies qu'elles font en se débarrassant de produits toxiques dans l'environnement, c'est normal. Elle peut donc payer quelques personnes pour aller recueillir les signaux Wi-Fi émis par les domiciles des différents cadres. Un soir, Val prépare son dernier billet depuis son portable... et le publie. Sur son réseau Wi-Fi, l'adversaire a pu observer une bonne quantité de données circuler de son ordinateur à son routeur. Pendant ce temps là, les autres cadres sont au lit, et pas un paquet ne circule sur leurs réseaux... Et là un nouvel article apparaît sur le blog... Pour ce qui advient de Val, je vous laisse imaginer la suite.

Dans cet exemple, d'ailleurs, l'usage de Tor ou d'un autre outil d'anonymisation ne change rien.

C'est pour ça que Tor ne prétend pas résister à un adversaire global : un adversaire qui serait capable d'écouter tous les points du réseau en même temps pourrait toujours retrouver l'origine des connexions.

D'ailleurs, un mot sur les « VPN » : c'est donc très fragile, vu qu'il suffit à un adversaire d'écouter ou de corrompre un seul et unique endroit pour recouper source et destination.

Le besoin de diversité

Les attaques par confirmation, c'est quand l'adversaire a déjà des suspects. Pour que Tor fonctionne, il est aussi nécessaire que les relais ne soient pas « de mèche ». Sinon, ils sont capables d'affaiblir ou de percer l'anonymat des connexions.



Le besoin de diversité

Les relais doivent :

- être administrés par des personnes différentes
- être situés dans des pays différents
- être situés dans des réseaux différents
- être connectés à des points d'échanges différents

« We ~~need~~ to be everywhere ! »

Pour l'aspect administration, Tor permet de déclarer que des relais sont gérés par les mêmes personnes. Par contre, c'est une simple déclaration volontaire. Les gens ne le font pas forcément.

Pour la partie pays, Tor ne cherche pas spécialement à être malin.

Pour la partie réseau, Tor choisit au maximum un relai par /16 IPv6 dans un circuit donné. C'est bien mais pas top.

Pour les points d'échanges, personne n'a pour l'instant beaucoup étudié la question. Mais théoriquement, si la connexion vers tous les relais choisis passe par le même équipement réseau, il devient trivial de percer l'anonymat en mettant l'équipement sur écoute.

Bon, mais alors où en est-on ?

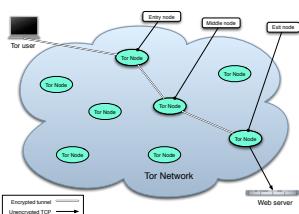
Etat des lieux : nombre d'admin.

Qui gère les 3500 relais qui composent le réseau ?

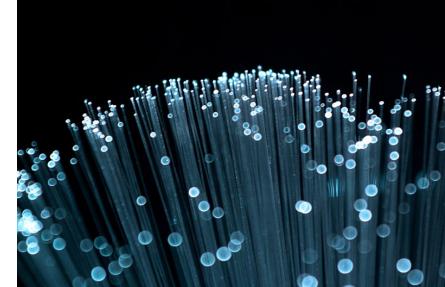
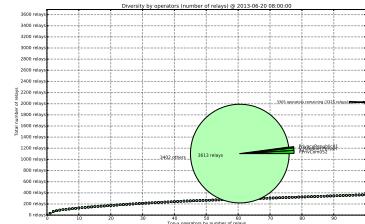
Le graph représente la distribution du réseau en terme de nombre de relais par opérateurs (ou famille de relais).

Les 3 premiers opérateurs ne gèrent que 75 relais sur 3500+.

Mais alors, tout va bien ?



Optimisons la bande passante



Optimisons la bande passante

Plutôt que de prendre les relais au hasard, depuis 2004, Tor choisit les relais en fonction de leur bande passante.

Sources : <https://commons.wikimedia.org/wiki/File:Modems.jpg>, <https://secure.flickr.com/photos/twistiti/1747920810/sizes/o/>

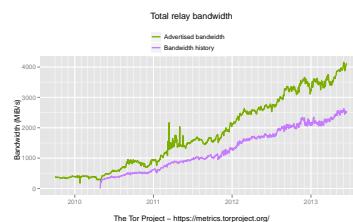


Au niveau réseau, c'est pareil. Mieux vaut donc que les clients Tor privilégiennent les noeuds avec beaucoup de bande passante lors de la création des circuits.

Évolution de la bande passante

La bande passante du réseau augmente vraiment depuis quelques années.

Autour de 20 Gbit/s de bande passante utilisée (sur 32 Gbit/s disponible).



Sources : <https://secure.flickr.com/photos/hudsson/5269743852/sizes/l/>, <https://secure.flickr.com/photos/45952129@N00/5073044080/sizes/l/>

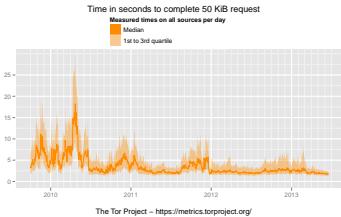
Ce serait dommage de faire autrement : si plein de voitures essaient de passer par une petite route de campagne, ça fait un bouchon. Vu qu'il existe des autoroutes, mieux vaut encourager les gens à les utiliser.

Évolution de la latence

Et Tor tente d'utiliser au mieux les différentes ressources pour rester à peu près *rapide*.

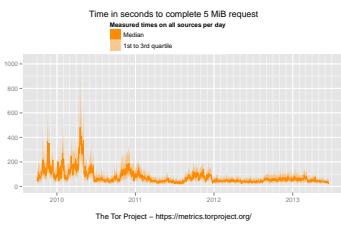
L'algorithme de sélection s'est d'ailleurs affiné en 2010 pour tenir compte de leur position dans le circuit (entrée, milieu ou sortie).

Autour de 2 secondes pour télécharger 50 kio (\pm 200 kbit/s).



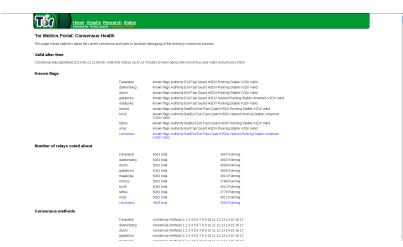
Évolution de la latence

Autour de 40 secondes pour télécharger 5 Mio (± 1 Mbit/s).



Grosso-modo, ça fonctionne mieux que ce qu'on peut régulièrement avoir comme qualité de connexion lorsqu'on utilise un téléphone mobile.

Le « consensus »



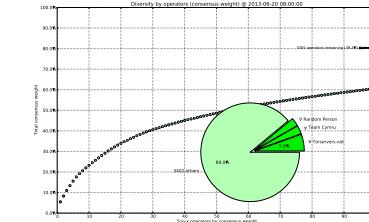
Afin de connaître les relais en service, Tor télécharge un document baptisé « consensus » qui contient la liste de relais et leurs caractéristiques.

On appelle ce document le consensus parce que Tor fonctionne avec des « annuaires faisant autorité ». Ce sont actuellement 9 serveurs différents. Pour éviter tout un tas d'attaques, il existe un système de votes sur les informations contenues dans l'annuaire entre ses machines. La *vue du réseau* sur laquelle elles sont d'accords est publiée toutes les heures dans un document qu'on appelle donc « le consensus ».

La popularité d'un relai s'estime donc avec son « poids dans le consensus » : c'est grosso-modo la probabilité qu'il soit utilisé dans un circuit... et donc son importance pour le réseau Tor.

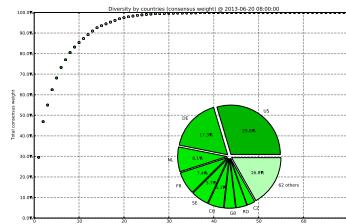
État des lieux : poids dans le consensus par admin.

40 opérateurs de relais gèrent 50% du réseau Tor.



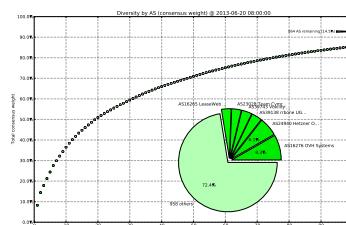
État des lieux : poids dans le consensus par pays

Près de la moitié du réseau entre les USA et l'Allemagne.



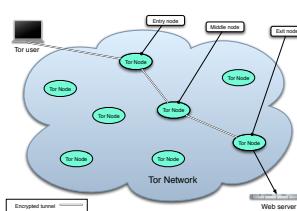
État des lieux : poids dans le consensus par AS

1/4 du réseau Tor se trouve chez 5 fournisseurs réseau



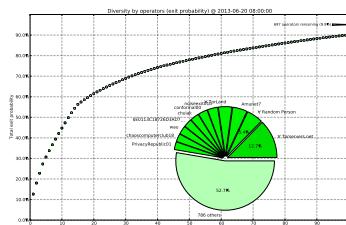
Les nœuds de sortie

849 nœuds de sortie sur 3411 relais.



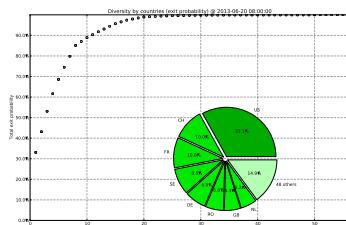
État des lieux : probabilité de sortie par admin.

Une connexion sur deux sortent chez les 8 mêmes admin.



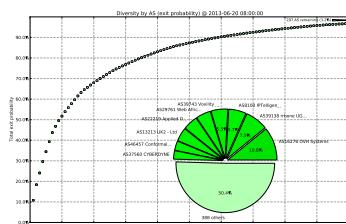
État des lieux : probabilité de sortie par pays

8 connexions sur 10 sortent par les même 6 pays.



État des lieux : probabilité de sortie par réseaux (AS)

6 connexions sur 10 sortent par les 10 mêmes fournisseurs réseaux



Améliorer la situation

- Plus nous sommes à utiliser Tor, meilleur est l'anonymat
- Tor doit rester utilisable
- Il faut donc d'avantage de « gros » noeuds

Tor doit rester utilisable, il ne faut pas donner trop de poid aux petits neuds qui augmenteraient la latence de Tor

Faire tourner de « gros » noeuds



On peut rassembler ses forces pour pouvoir mutualiser les ressources et les énergies afin de mettre en oeuvre des gros neuds.

Source : <https://secure.flickr.com/photos/vike/7917176960/sizes/l/>

Quelques initiatives

- Chaos Computer Club
- Noisebridge
- DFRI
- Torservers.net
- ...

torservers.net

- Crée par Moritz Bartl en mai 2010 : <https://lists.torproject.org/pipermail/tor-talk/2010-May/014519.html>
- Association à but non-lucratif allemande : *Zwiebefreunde e.V.*

Dans son mail, il précise qu'il y a un problème dans le réseau Tor avec un seul neud qui regroupe 1/4 du trafic de sortie de Tor. Ce neud a disparu depuis.

torservers.net : HOWTO

1. Créer une association
2. Obtenir un numéro de fax
3. Obtenir un numéro de téléphone
4. Créer des enregistrements administratifs pour les IPs (ARIN, RIPE, etc.)
5. Trouver de bons hébergeurs
6. Être rapide à répondre aux notifications d'abus

<https://lists.torproject.org/pipermail/tor-relays/2012-July/001391.html> (juillet 2012)

La perle rare des hébergeurs :

- qui veut bien héberger Tor,
- pas cher,
- pas déjà utilisé par un autre relai.

Nos oignons

Alors un petit groupe de gens se disent que le moment est venu de s'occuper de :



Nos oignons

- Des années qu'« on » en parle
- Début du projet juillet 2012
- Appel aux bonnes volontés en janvier 2013
- Association loi 1901 parue au J.O. en mai 2013
- Dons acceptés via le Fond de Défense de la Neutralité du Net depuis le 25 mai 2013
- 5 personnes au C.A.
- 5 membres du comité de déontologie : Jean-Marc Manach, Olivier "Bluetouff" Laurelli, Jérémy "jz" Zimmermann, Grégoire Pouget, Stefano "zack" Zaccchioli
- 7 admin. sys.

Nos oignons : combien ça coûte ?

Poste	coûts	par an
Frais parution J.O.	40,00 € création	40,00 €
Noms de domaines (.net + .org + .fr)	24,08 € / an	24,08 €
Adhésion Tetaneutral	20,00 € / an	20,00 €
Hébergement web + mail + outils	10,00 € / mois	120,00 €
Compte bancaire	7,00 € / mois	84,00 €
Domiciliation + numérisation des courriers	17,94 € / mois	217,08 €
Téléphone + Fax	2,41 € / mois	28,94 €
Provision pour frais de justice	100,00 € / mois	1 200,00 €
Premier relai 100 Mbps	200,00 € / mois	2 400,00 €
Second relai 100 Mbps	200,00 € / mois	2 400,00 €
Total	6 432,10 €	

(surcoût : 6,71%)

À vous de jouer !

- Faites tourner des relais !
- Participez à Nos oignons ! <https://nos-oignons.net/Participez/>
- Donnez des sous !
<https://nos-oignons.net/Donnez/>
- Hébergez-nous !
contact@nos-oignons.net

Questions ?

Les fournisseurs d'un relai Tor ne sont pas responsables des informations transmises (à condition de ne pas être à l'origine de la transmission, de ne pas sélectionner le destinataire de la transmission et de ne sélectionner ni modifier les informations transmises) (article 12 de la directive et 32-3-3 du CPCE).

En vertu de l'article 12 alinéa 3 de ladite Directive, "une juridiction ou une autorité administrative, conformément aux systèmes juridiques des Etats membres" peut "exiger du prestataire qu'il mette un terme à une violation ou qu'il +prévienne une violation".

L'article 12 de la Directive a été transposé en droit français au sein de l'article 32-3-3 du CPCE. Ce dernier n'exige pas que les transporteurs préviennent ou mettent un terme à une violation.

->



Merci à koolfy d'avoir pavé la voie à cette présentation :
<http://koolfy.be/2013/01/27/well-need-a-bigger-onion/>

Merci à delber pour avoir écrit les premières lignes de Compass. Merci à Karsten et à Sathya d'avoir poursuivi le développement. Merci à Karsten pour ses suggestions sur les graphes.

Et à toutes les personnes qui ont bien voulu relire les brouillons.

slides, notes et sources :

<https://nos-oignons.net/Présentations/PSES2013/>