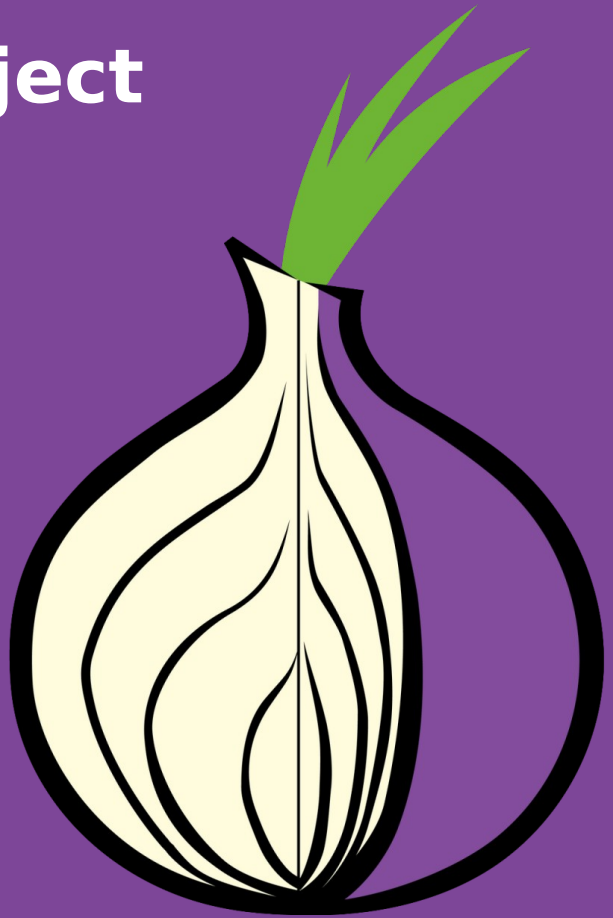
The Onion Router

Sécurité SI – Ynov Informatique

Par
Mickael Rigonnaux
Fabio Pace

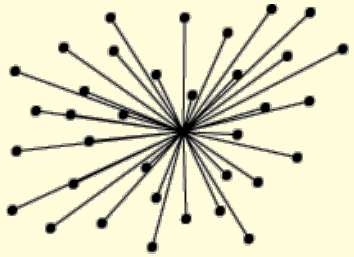
The Tor Project

1 – Présentation
2 – Fonctionnement
3 – Utilisation
4 – Pourquoi ?
5 – Limites & failles
6 – Alternatives
7 – Conclusion

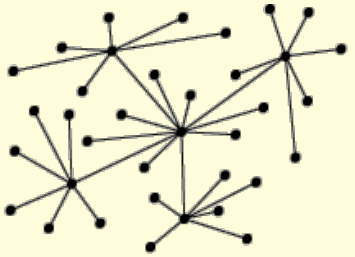


Présentation

- Réseau décentralisé & superposé
- Composé de plusieurs noeuds
  - Client
  - Entrée
  - Intermédiaire
  - Sortie



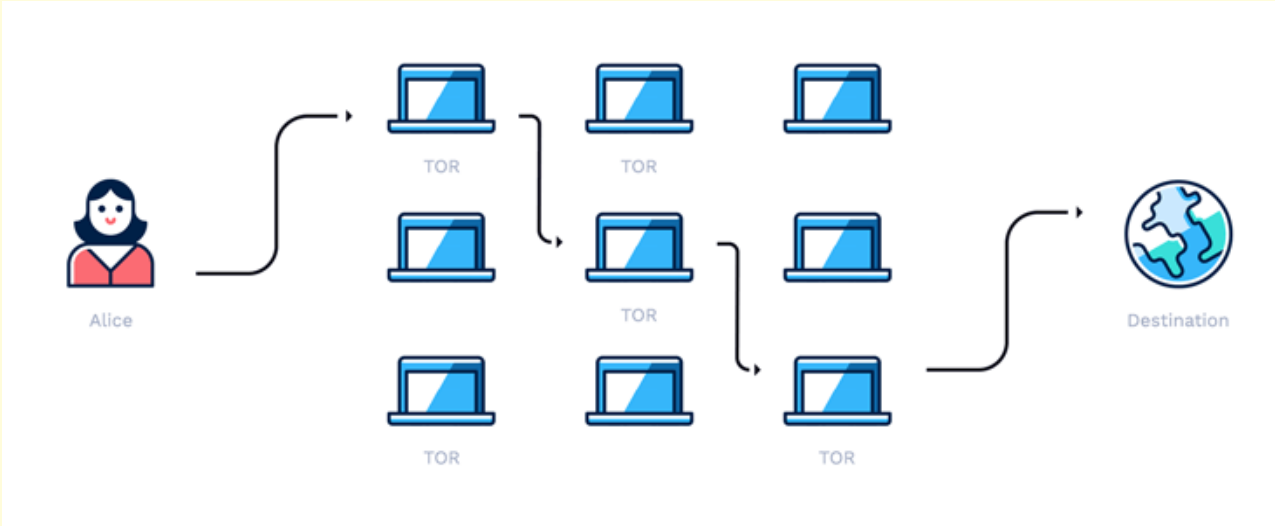
centralised



decentralised

- Support TCP
- Liste des noeuds publiques

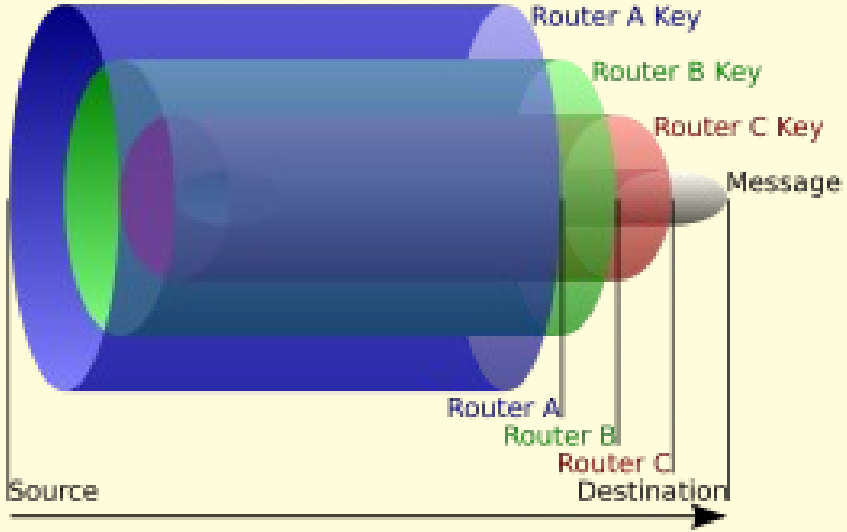
Fonctionnement



- Système de confiance
- Les flux sont chiffrés
- Utilisation comme un Proxy

Fonctionnement

Les flux sont chiffrés plusieurs fois (autant de fois que de noeuds) :



- Serveur avec l'ensemble des noeuds et les clés (publique)
- RSA 1024 par noeuds
- SSLv3/TLS1.x entre les noeuds
- Curve25519 (EC & DH 128 bits)
- Ed25519 (EdDSA, EC & DSA)

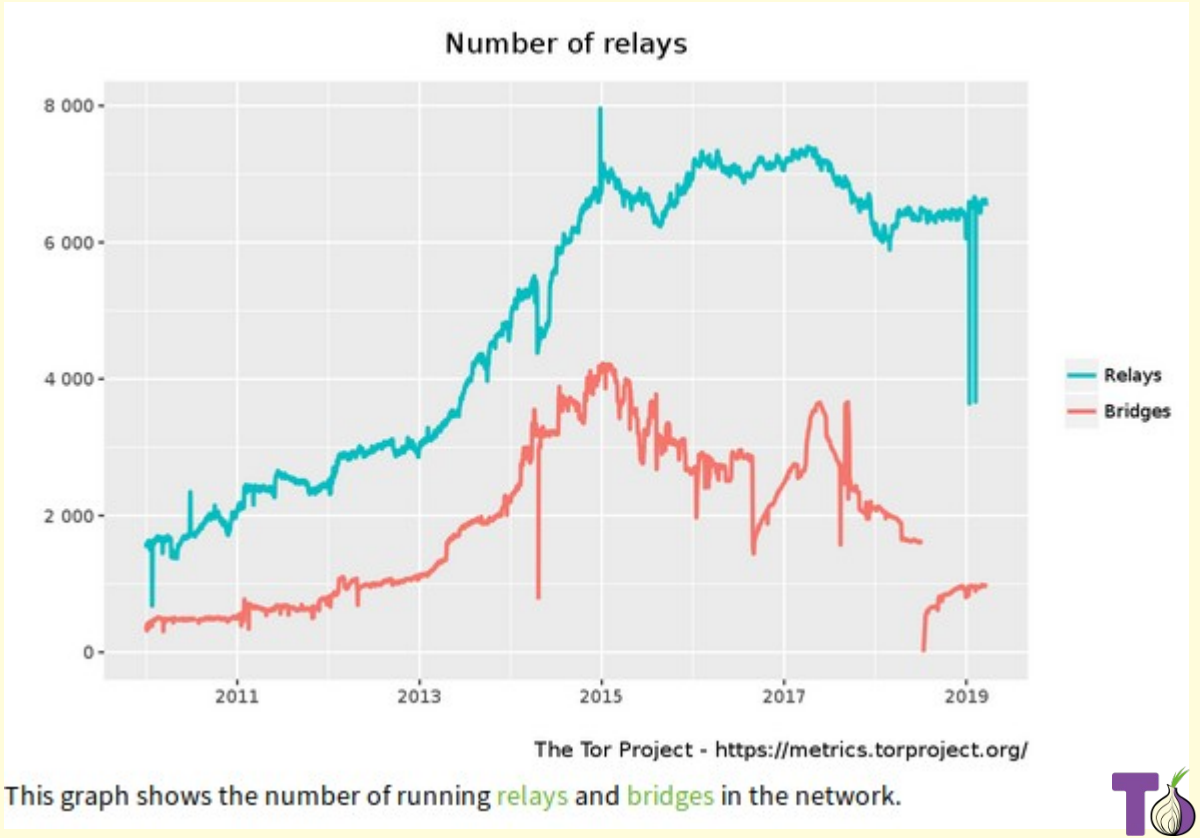
Source : https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

Les noeuds

~7000 Relay operators
~1000 Bridge operators
50+ Projects, services
and products
~2 Million users

~8 Employees
~12 Contractors
6 Board members

~40 Volunteers
~160 unique contributors: little-t-tor
~12 Contractors
~20 Professors
~100 Grad students
Lots of R&D



L’utilisation

- Ne pas utiliser avec Windows
- Désactiver le JS (NoScript)
- Eviter les connexions (Gmail, etc.)
- VPN en plus
- Ordinateur dédié et depuis réseau public (++)

Pour qui ? Pourquoi ?

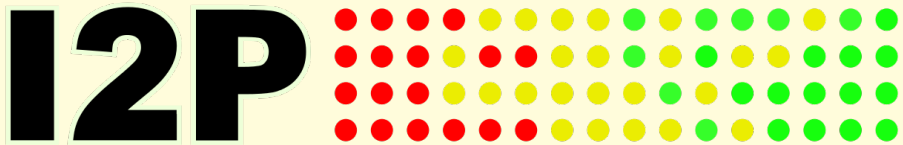
- Opposants à un régime
- Journalistes (dictature, démocratie)
- Lutte contre l’espionnage
- Criminels
- Liberté d’expression
- Contourner la sensure
- Ethique
- …

Limites & Failles

- Plusieurs états et/ou groupes ont des relais
- Le relais de sortie peut lire le traffic si pas de SSL/TLS
- Faille potentiel (Hacking Team, 2014)
- La liste des noeuds est publiques
- Assez lent

]HackingTeam[

Les alternatives



Merci !

https://www.torproject.org
https://lists.torproject.org
https://net-security.fr
https://metrics.torproject.org