



Mickaël Cornu

Xposé – IR3

17 Janvier 2012

Plan

- Description
 - Hébergement des données
 - Diffusion des messages
- Comment assurer l'anonymat?
 - Courrier
 - Formulaire en ligne
 - Tor
- Conclusion

Description

- Site créé en 2006
- Julian Assange
- Diffuse des documents officiels et confidentiels

Hébergement

- Suède => soutien du Parti Pirate Suédois et Bahnhof
- Suisse
- Miroir international => accès ftp ou ssh
<http://geekfault.org/2010/12/05/devenez-miroir-de-wikileaks-sans-risque/>

Diffusion de messages

- Sur leur site web
- Média
- Twitter
- BitTorrent

Comment assurer l'anonymat?

Par courrier

- CDs, DVDs, clé USB, des preuves écrites, photos
- **Adresse :**
BOX 4080
Université de Melbourne
Victoria 3052
L'Australie
- **Scanne les documents puis sont détruits.**

Formulaire en ligne

Please choose a file for upload:
To upload multiple files please compress them as a file archive.
Please split files larger than 200MB into smaller files. Thanks.
To explicitly set an embargo date for the upload uncheck the checkbox and enter the desired release date. Please enter the date in the format YYYY/MM/DD.
The upload will not be released until:

No embargo, defaults to on:

2010 / 7 / 27

Since it seems that you have no JavaScript enabled you can see the progress of your upload if you click on the link. This will open the progress indicator in a new window.

[CLICK HERE](#) to get the upload progress indicator.

To submit the document press the Upload button. After your upload is finished you can provide additional information about the content.

Mettre le document en pdf

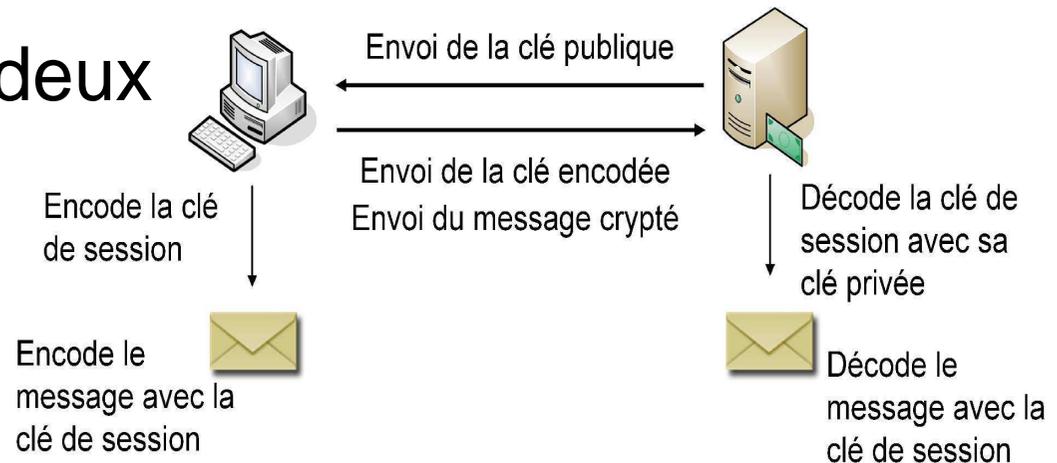
Formulaire en ligne

- SSL assure :
 - Authentification
 - Confidentialité
 - Intégrité

SSL

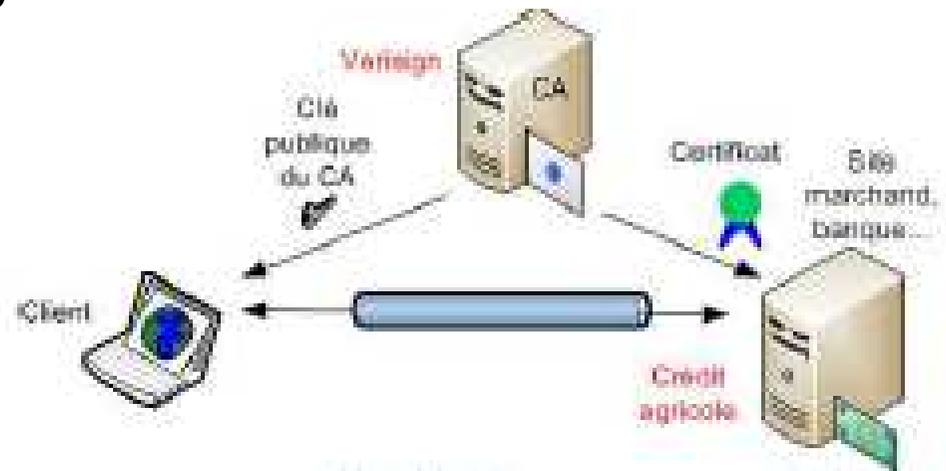
- Cryptage asymétrique
 - Clé publique/ clé privée => authentifier le serveur
- Cryptage symétrique
 - Une seule clé => assurer transmission des données

- Combinaison des deux



SSL

- Authentification par certificat
 - Autorité de certification délivre un certificat
- Contenu d'un certificat:
 - Informations dont la clé publique du propriétaire et l'algorithme de hachage
 - Signature



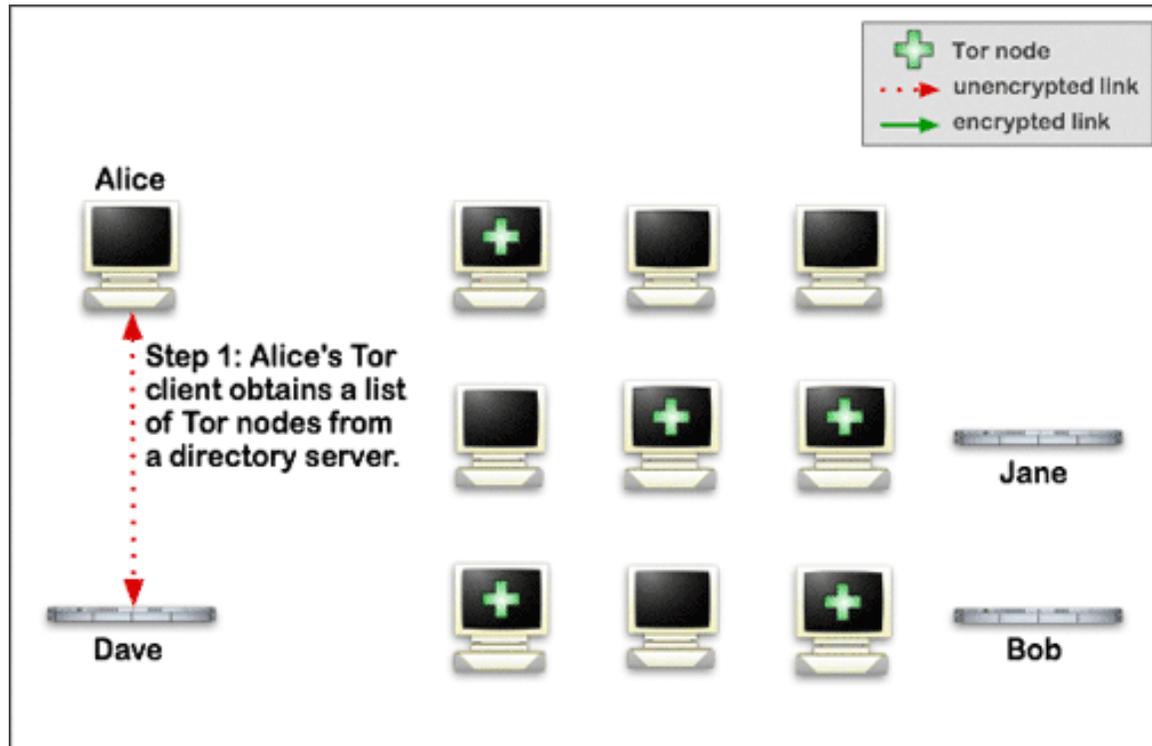
Tor

- Acronyme: The Onion Router
- logiciel libre
- Naviguer anonymement sur Internet
- Les Onions Routers (OR) représentent le coeur fonctionnel du réseau.
- Les noeuds clients (OP).
- Les Directory Servers (serveurs d'annuaire), référencent les ORs connus.

Tor

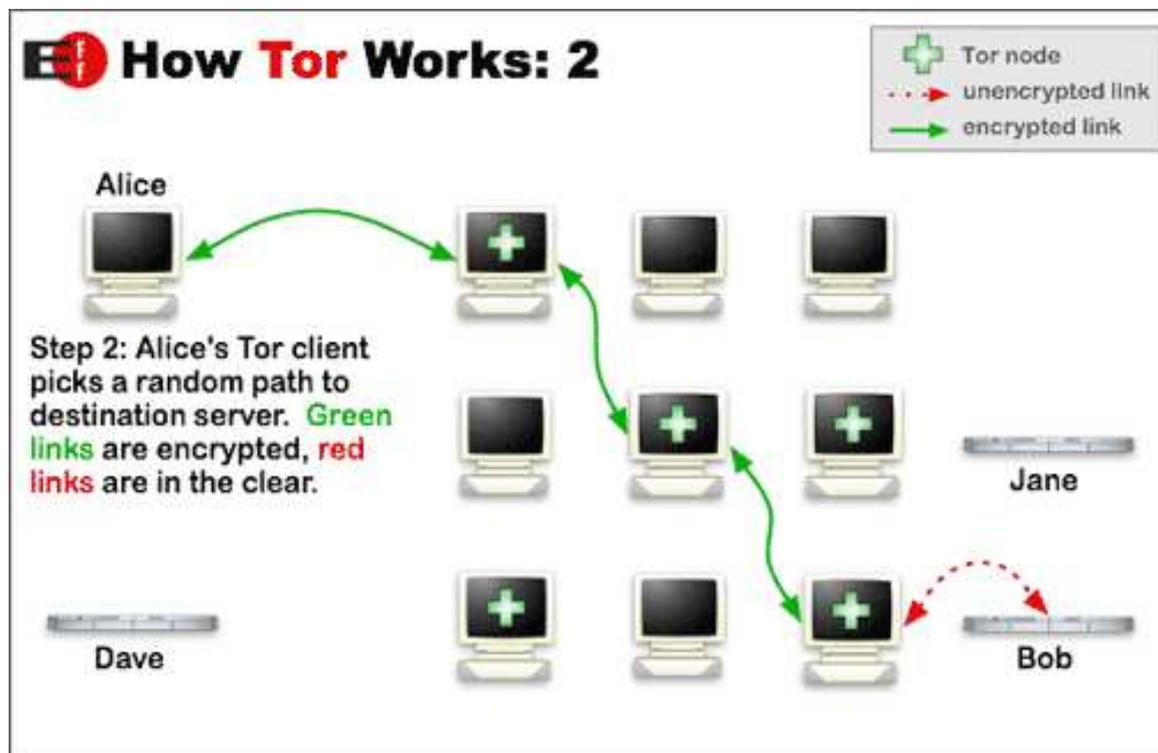
- **Fonctionnement**

Alice veut accéder à un site web (Bob) de manière anonyme.



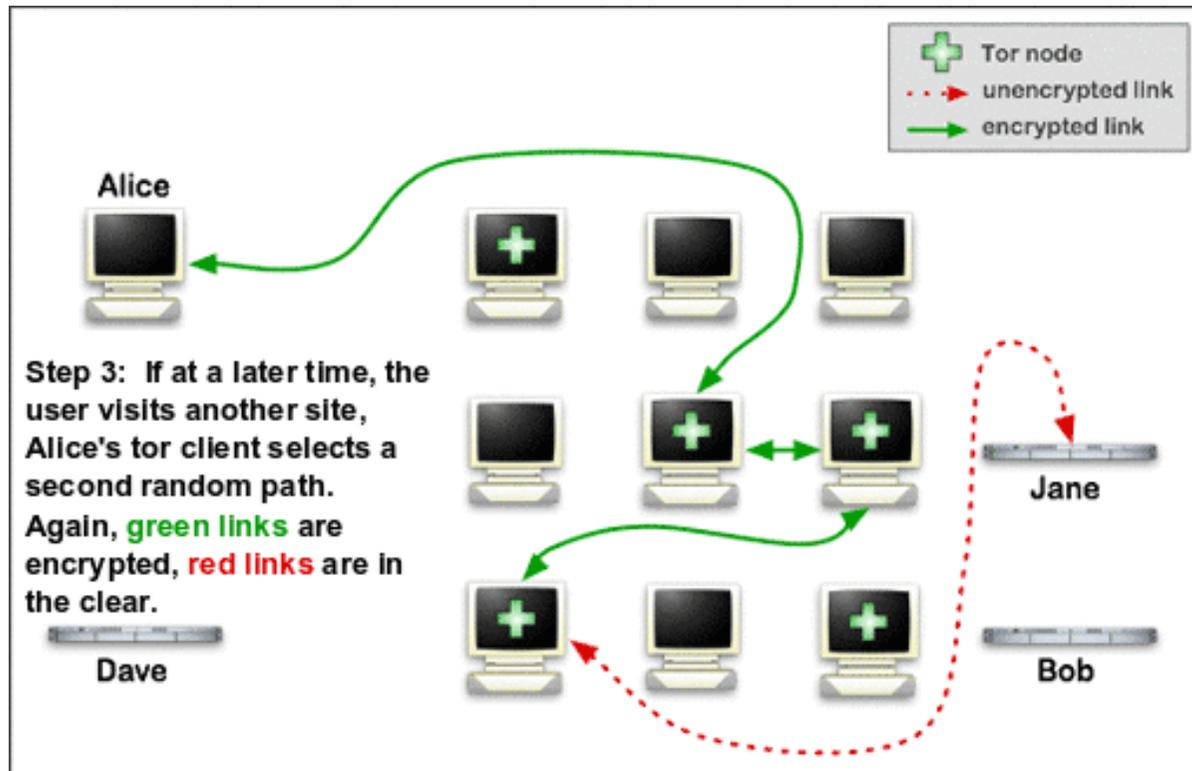
Fonctionnement de Tor

- Création du chemin



Fonctionnement de Tor

- Nouvelle connexion



Tor

- Services cachés
 - Tor permet aux clients et aux relais d'offrir des services cachés

Tor

- Inconvénients
 - Lenteur
 - Pas de protection pour les paquets UDP
 - Cookies et données personnelles
 - HTTP : non crypté entre le dernier relai et le serveur

Conclusion

- Courrier
- Tor logiciel efficace

Bibliographie

- <http://fr.wikipedia.org/wiki/WikiLeaks>
- <http://www.wikihow.com/Submit-a-Leak-to-Wikileaks>
- <http://www.torproject.org>

Merci

Avez-vous des questions?