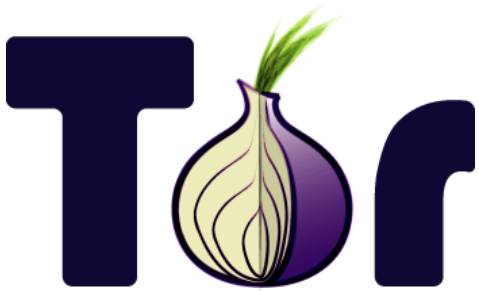
Tor : routage et chiffrement en oignon

Guillaume Piolle
guillaume.piolle@supelec.fr
http://guillaume.piolle.fr/

2014

Présentation de Tor



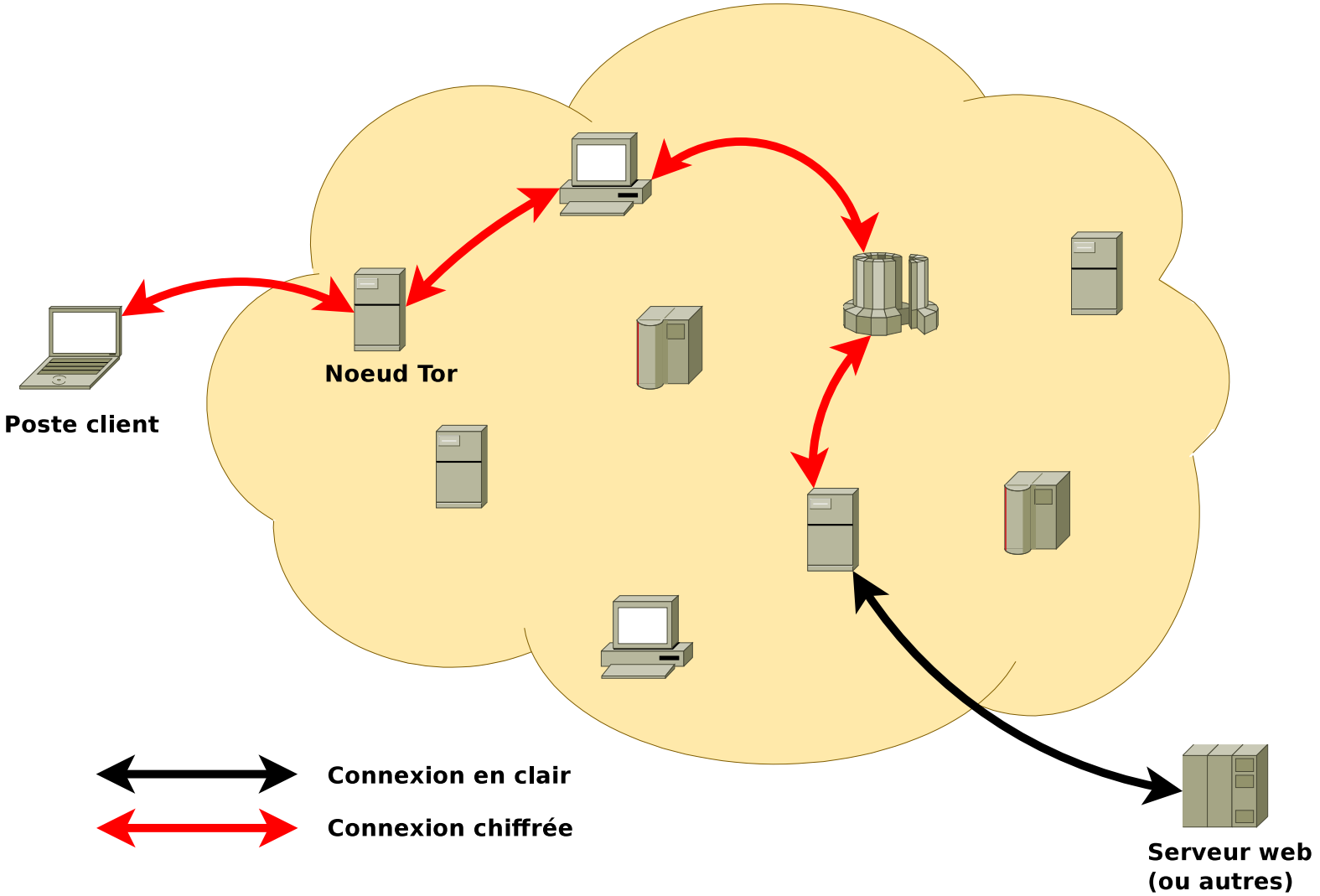
Tor = *The Onion Router*

Principe : faire transiter les messages par un certain nombre de nœuds (machines) choisis au hasard, avant de les remettre à leur destinataire, en utilisant des chiffrements successifs entre les nœuds (chiffrement en couches, d'où l'image de l'oignon).

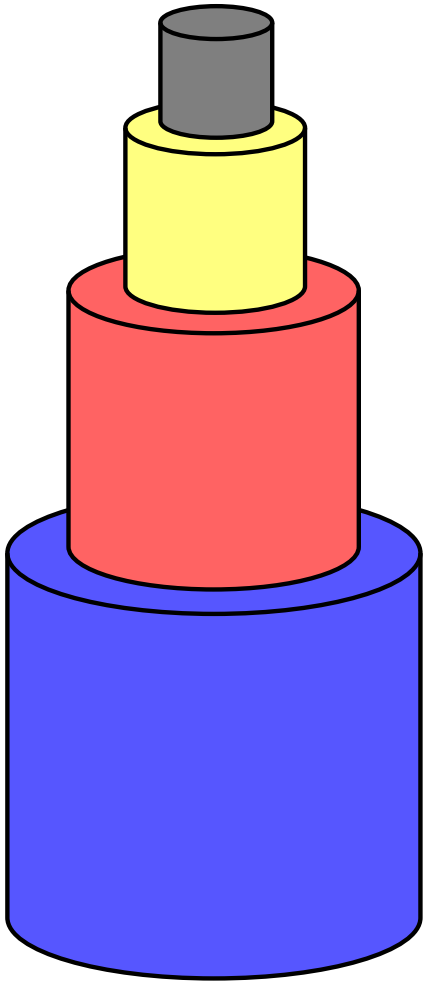
Objectif poursuivi (à préciser dans la suite) : protection de la vie privée d'un usager du web.

Tor est un réseau de machines (nœuds Tor), avec des nœuds « d'entrée » et « de sortie », que tout le monde peut utiliser de cette manière.

Présentation de Tor



Présentation de Tor



Message en clair

Chiffrement avec la clé du noeud n

Chiffrement avec la clé du noeud n-1

Chiffrement avec la clé du noeud n-2

Établissement d'un circuit Tor par le nœud A : principe

- A choisit une séquence de nœuds commençant par un nœud d'entrée (B) et terminant par un nœud de sortie, et récupère les clés publiques des nœuds du circuit ;
- A associe en interne à B un nouveau numéro de circuit $circID_{AB}$;
- A envoie un message `create` à B, contenant $circID_{AB}$ et la première moitié d'un Diffie-Hellman chiffrée avec la clé publique de B ;
- B renvoie un message `created`, avec la deuxième moitié du Diffie-Hellman et le condensat de la clé de session K_{AB} ;
- A envoie un `relay extend` à B en lui désignant C et en transmettant une moitié de Diffie-Hellman chiffrée avec la clé publique de C ;
- B choisit en interne un nouveau numéro de circuit $circID_{BC}$, qu'il associe à $circID_{AB}$;
- B transmet le message à C dans un `create` étiqueté $circID_{BC}$;
- C renvoie un message `created` que B transmet à A sous la forme d'un `relay extended` : A et C partagent K_{AC} ;
- etc.

Manipulation en classe

Matériel requis

- Une classe divisée en 5 groupes A (émetteurs), B (nœuds d'entrée), C (nœuds intermédiaires), D (nœuds de sortie) et E (destinataires) (par exemple organisés en 5 rangées) ;
- Des enveloppes de trois tailles rentrant les unes dans les autres ;
- Des papiers entrant dans les petites enveloppes ;
- Papier et gomme pour chacun ;
- Les fiches pratiques « émetteur », « nœud d'entrée », « nœud intermédiaire », « nœud de sortie », « destinataire » ;
- Un peu de concentration...

Le réseau Tor

Propriétés assurées

- Anonymisation IP du client, vis-à-vis de tout le monde excepté le nœud d'entrée ;
- Contenu des messages et destinataire chiffrés jusqu'au nœud de sortie (point sensible).

Mais !

- Nécessité d'utiliser un proxy spécifique sur la machine client ;
- Nécessité de « torréfier » les applications ;
- Grand temps de latence, inadapté pour les gros volumes de données ;
- Pas d'anonymisation applicative : on peut être identifié par le contenu des messages ;
- Les nœuds d'entrée et de sortie sont publics et peuvent être interdits d'accès.

Crédits