Xposés IR3 2009/2010

TOR - The second-generation Onion Router

Rémy MASSON

12 janvier 2010

Plan

Généralités

- Oui, un oignon
- Opensource
- Distributed overlay network
- Composé de noeuds
- Anonymiser les connexions TCP
- Clients construisent des circuits
  - Noeuds ont des connaissances limitées
  - Onion Routers (OR) routent le trafic
- Application haut niveau

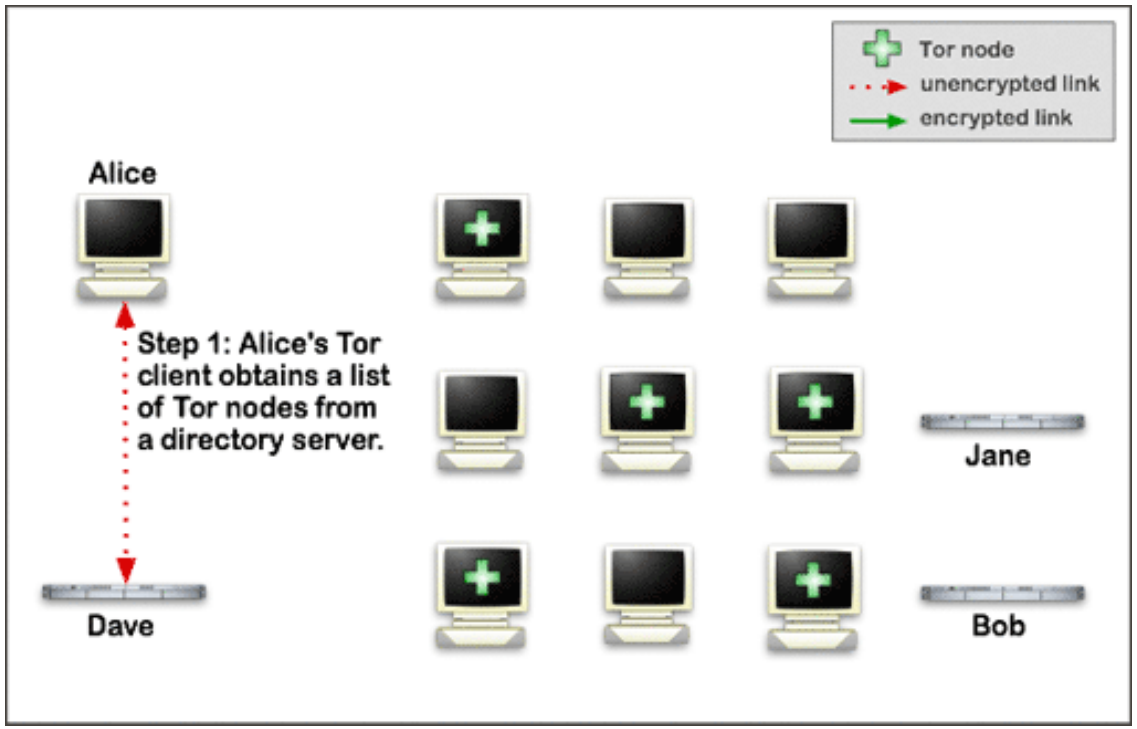
Généralités

- Nécessite une compatibilité SOCKS
- SOCKS ?
  - Couche session
  - Protocole facilitant le routage de paquets entre les applications client/serveur via un serveur proxy
- Onion Proxy (OP)
  - Récupère les directories
  - Crée et utilise des circuits
  - Gère les connexions des applications utilisateurs
- Directory server (serveur d'annuaires)
  - Référence les ORs connus

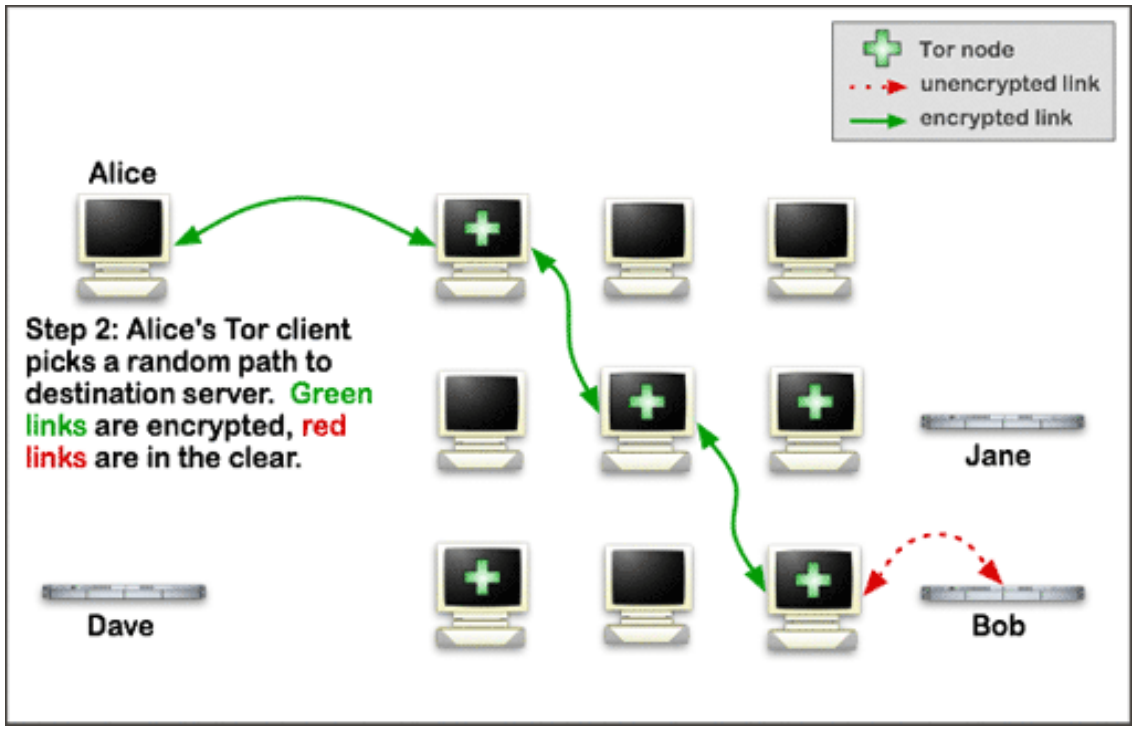
Objectifs de conception

- Objectifs
  - Déployabilité
  - Facilité d'utilisation
  - Flexibilité
  - Conception simple
- Non-objectifs
  - Non peer-to-peer
  - Pas sécurisé contre les attaques de bout en bout
  - Non soucieux de l'anonymat des protocoles transportés
  - Non stéganographique

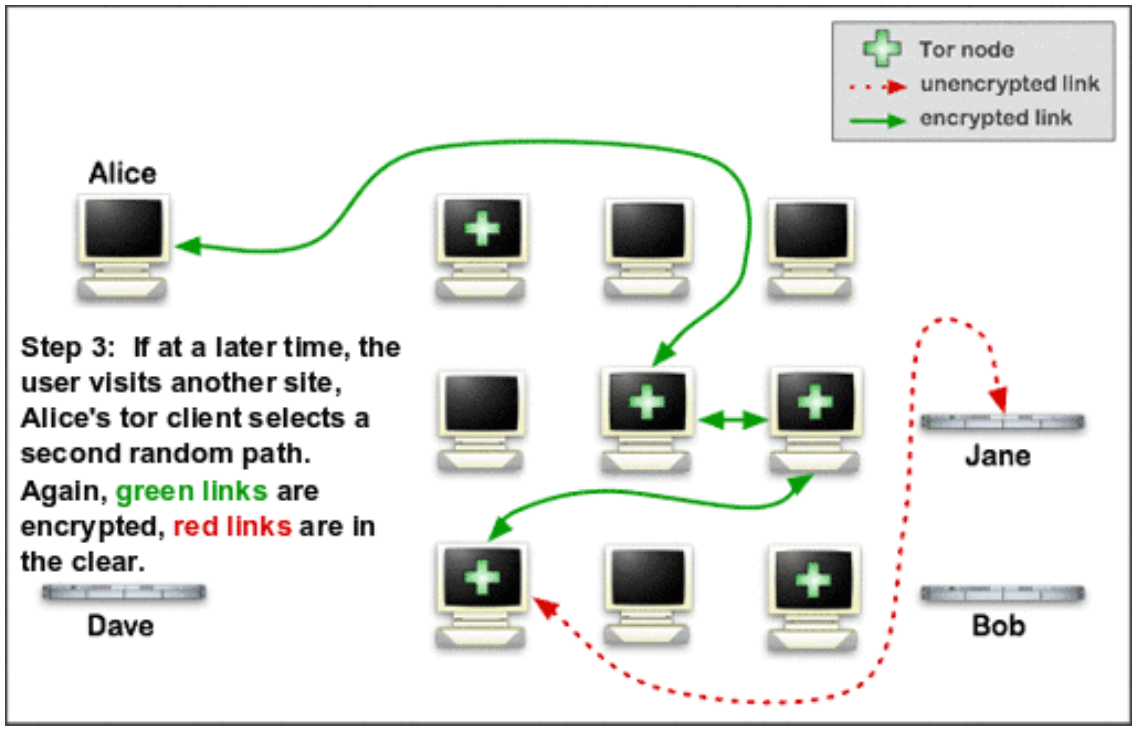
Principe


Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Dave
Jane
Bob

Principe


Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Principe


Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Dave
Jane
Bob

Circuits

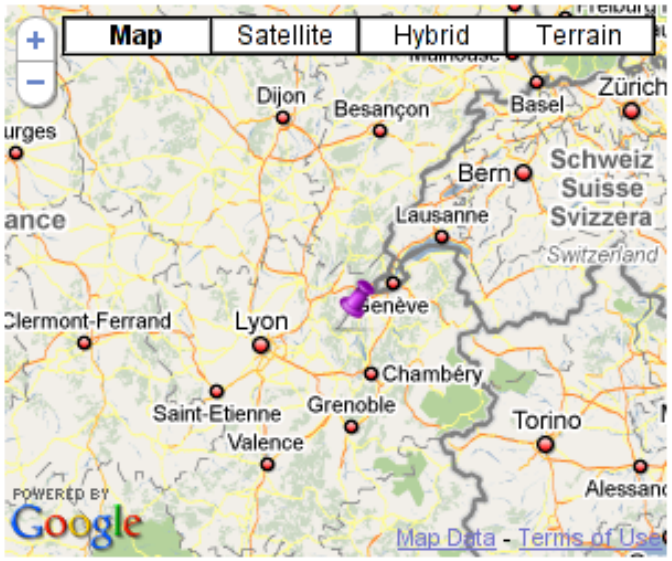
- Plusieurs flux TCP multiplexés sur un circuit
  - Efficacité et anonymat
- Durée de vie limitée
- OP choisit les noeuds du circuit
- Construits de façon incrémentale

Chez moi.

Your IP address is 79.87.147.220

(Now detects many proxy servers)

GoToMyPC TRY IT FREE



IP Address Location: Culoz, Rhone-Alpes France

Tools

IP Lookup
Blacklist Check
Trace Email
Visual Traceroute
Traceroute

79.87.147.220 Trace Now

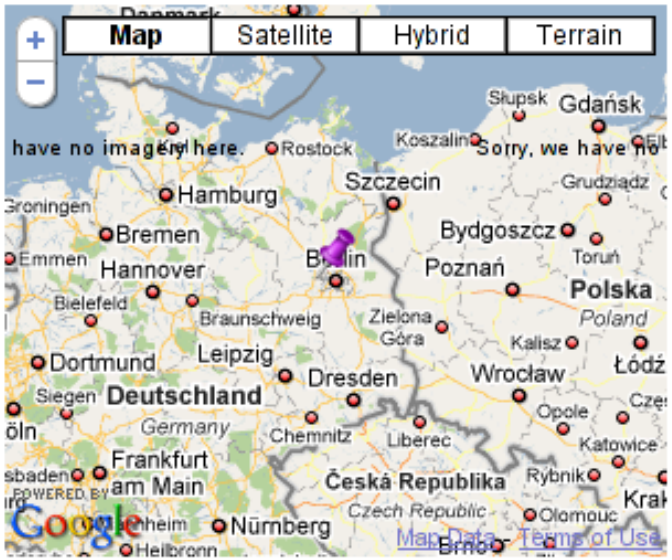
IP Lookup now shows ISP, Organization, Proxy Status, and Connection Type!

Chez les autres

Your IP address is 85.214.73.63

Suspected proxy server or network sharing device. (details)
(Now detects many proxy servers)

Anytime.



IP Address Location: Berlin, Berlin Germany

Tools

IP Lookup
Blacklist Check
Trace Email
Visual Traceroute
Traceroute

85.214.73.63 Trace Now

IP Lookup now shows ISP, Organization, Proxy Status, and Connection Type!

Chez les autres

Your IP address is 192.251.226.206

Suspected proxy server or network sharing device. (details)
(Now detects many proxy servers)

Anytime.

Tools
IP Lookup
Blacklist Check
Trace Email
Visual Traceroute
Traceroute

192.251.226.206 Trace Now

IP Lookup now shows ISP, Organization, Proxy Status, and Connection Type!

IP Address Location: Rietberg, Nordrhein-Westfalen Germany

Chez les autres

Your IP address is 208.75.212.156

Suspected proxy server or network sharing device. (details)
(Now detects many proxy servers)

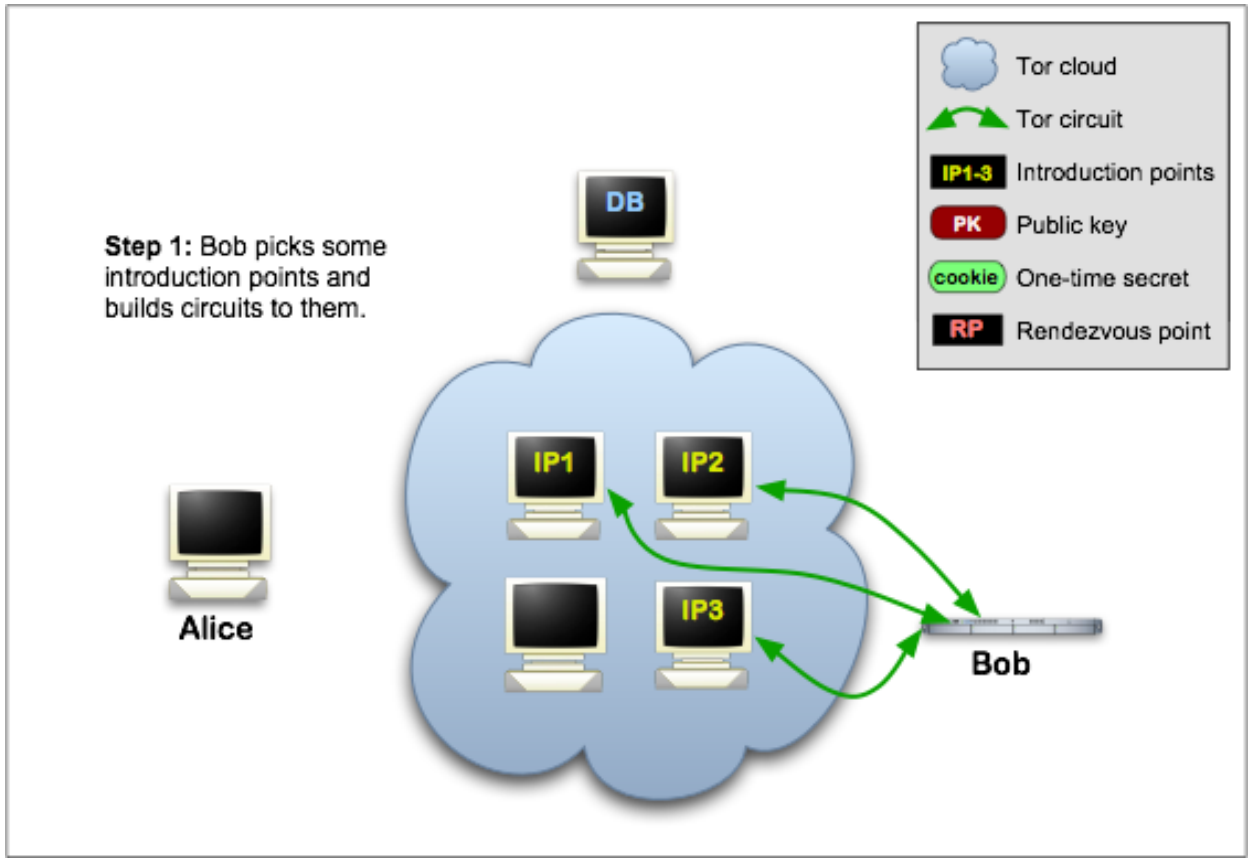
IP Address Location: Troy, New York United States

Tools
IP Lookup
Blacklist Check
Trace Email
Visual Traceroute
Traceroute

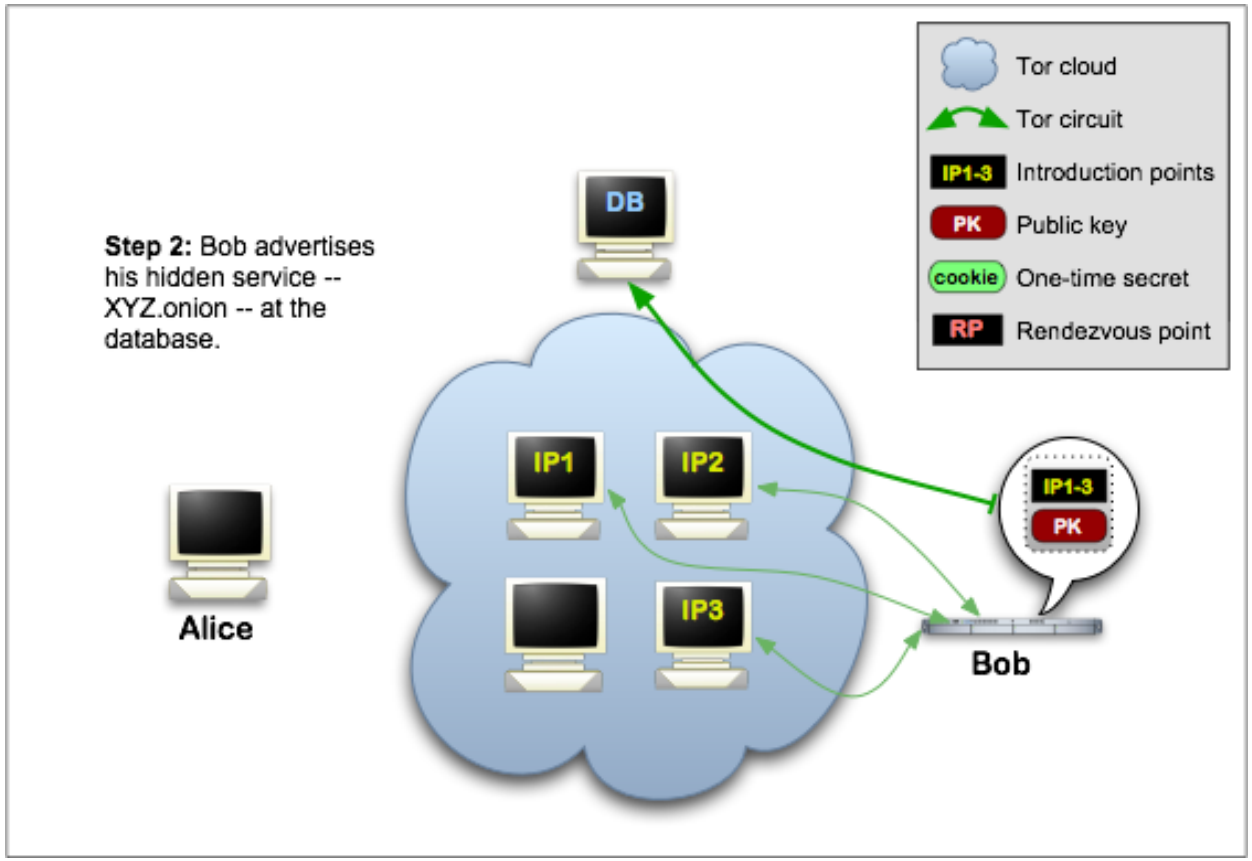
208.75.212.156 Trace Now

IP Lookup now shows ISP, Organization, Proxy Status, and Connection Type!

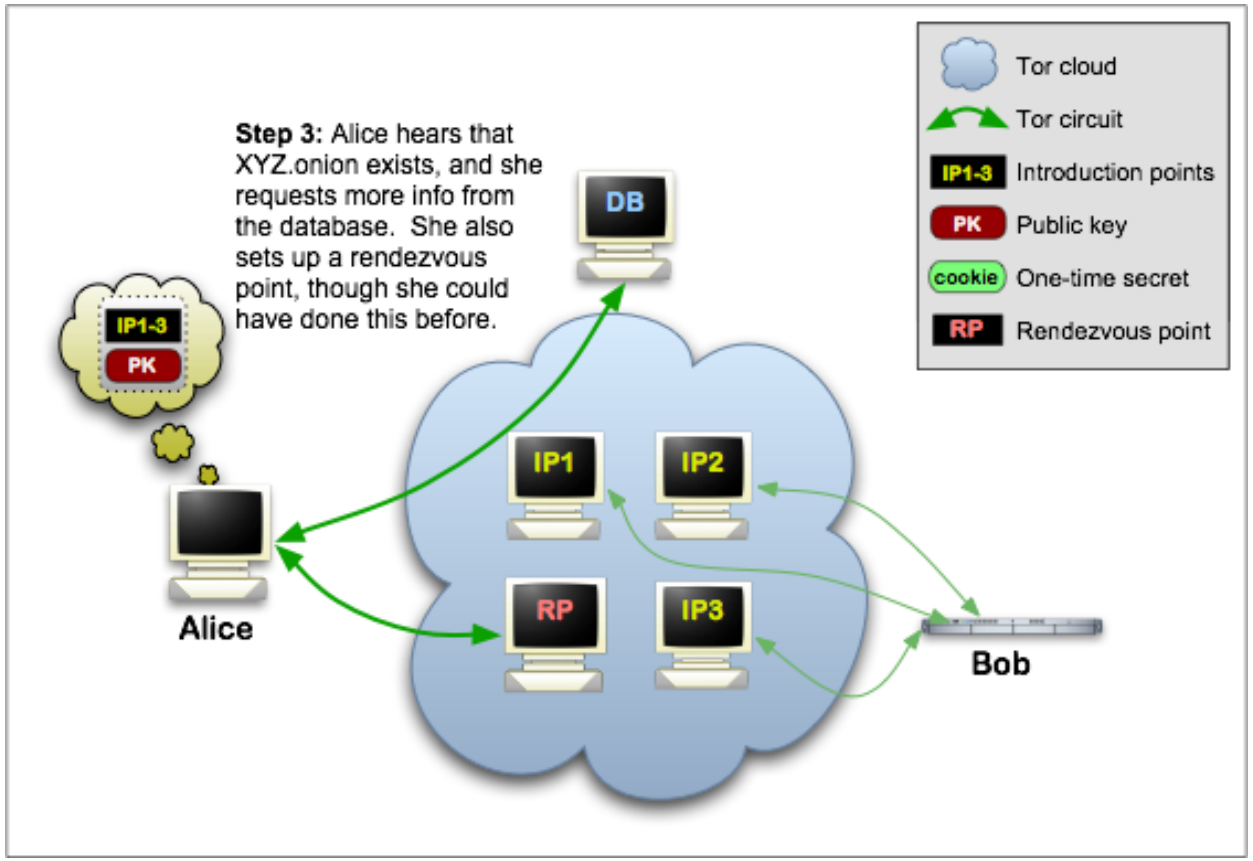
Les services cachés



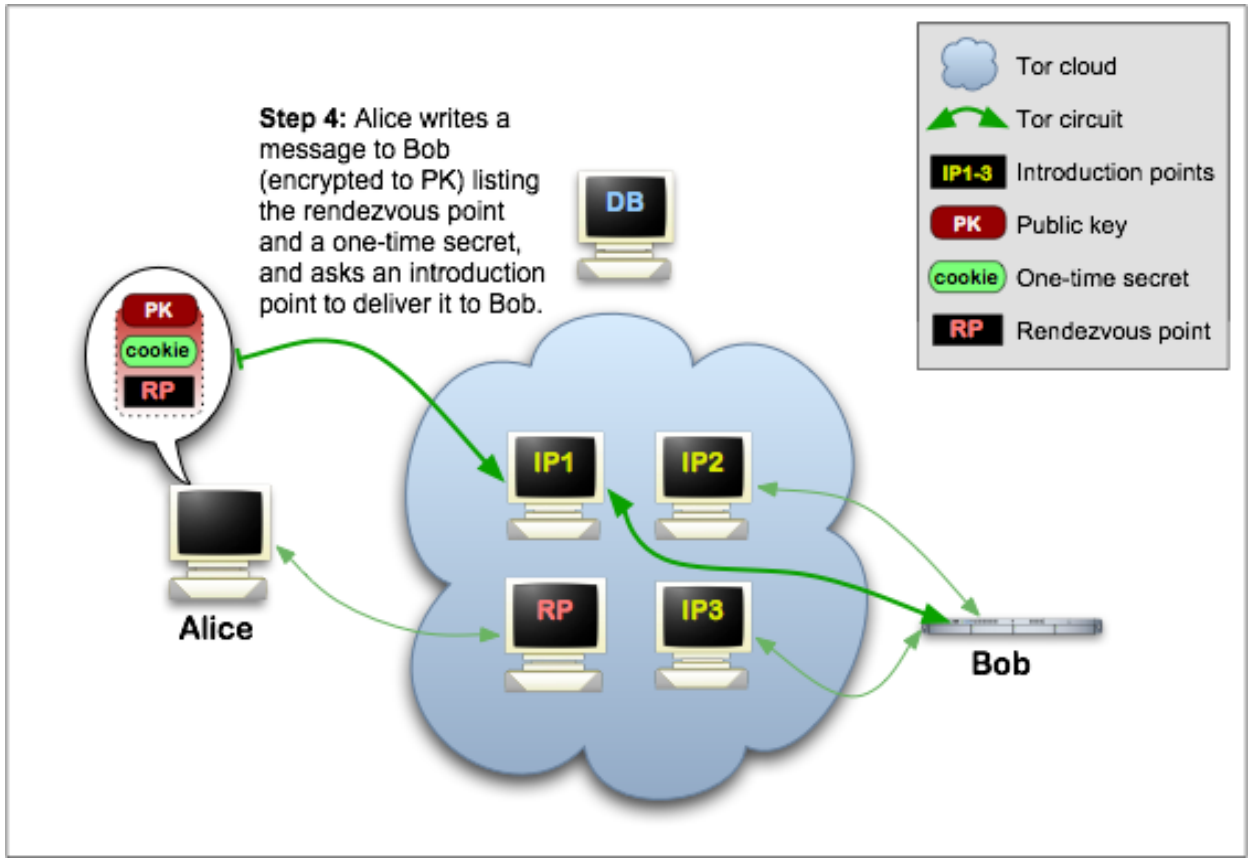
Les services cachés



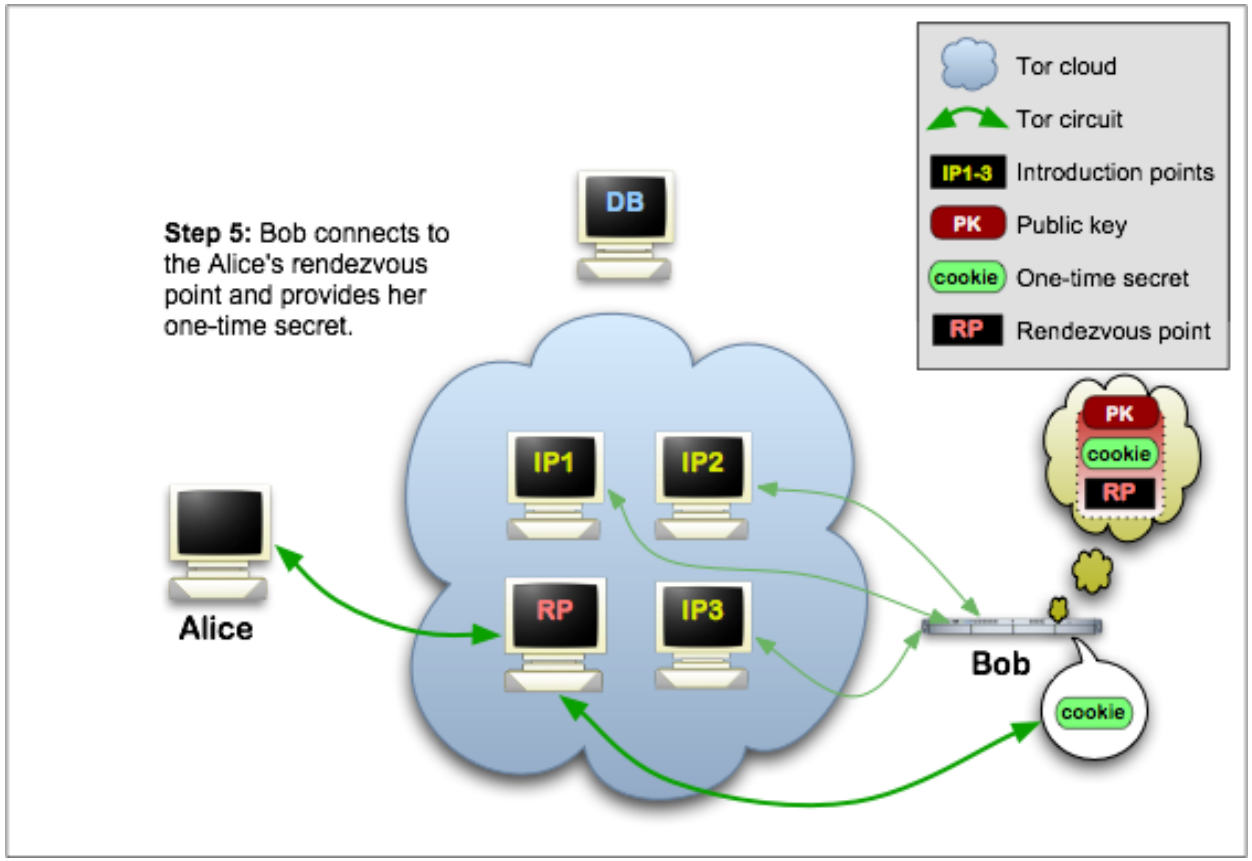
Les services cachés



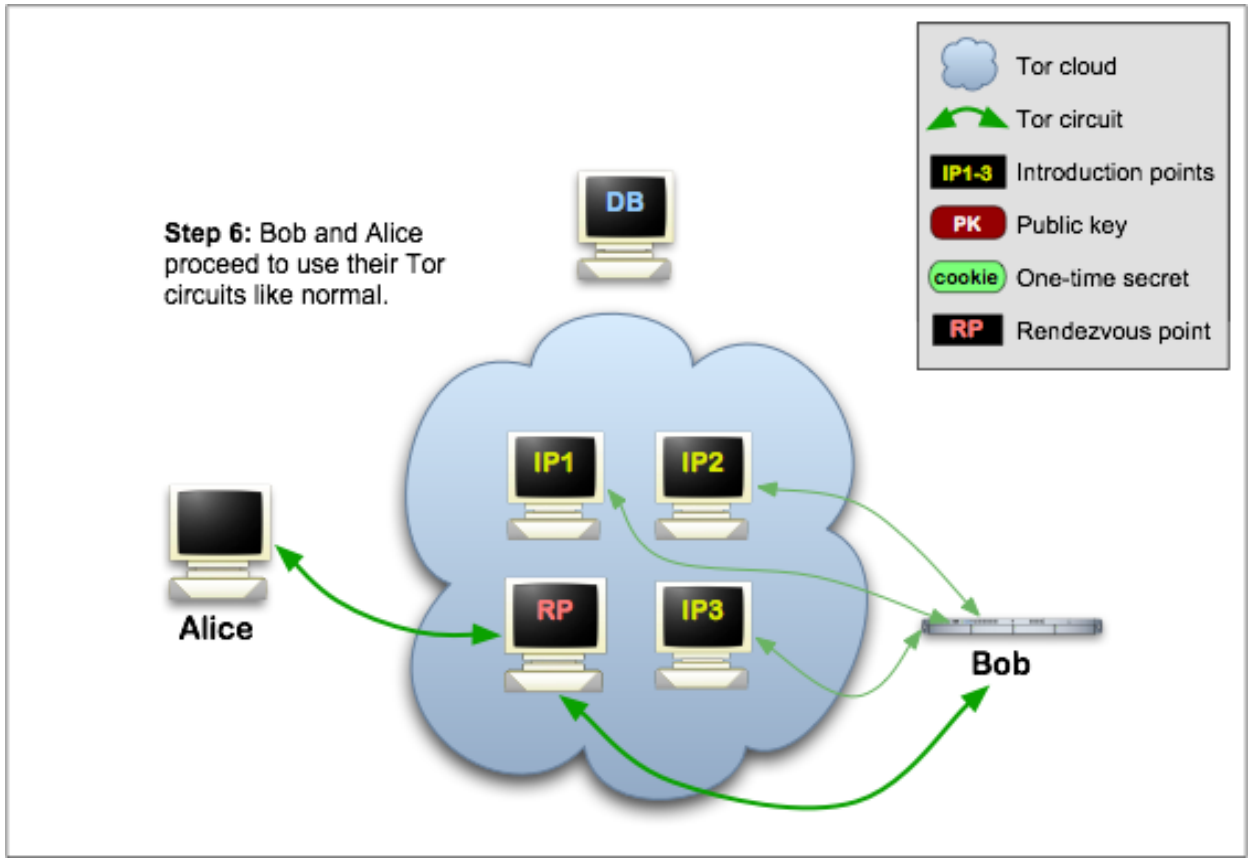
Les services cachés



Les services cachés



Les services cachés



Précisions

- ORs maintiennent des connexions TLS vers les autres ORs
- Cellules de taille fixe
- Chaque OR
  - Identity key : longue durée de vie, signe les certificats TLS, les router descriptors (et directories)
  - Onion key : courte durée de vie, utilisée lors de l'établissement de circuits
  - Clés éphemères entre noeuds (circuit)
  - Clés de lien négociées par TLS

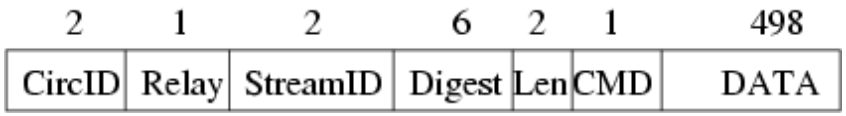
Cellules

- 512 octets
- CircID propre à chaque connexion (OR-OR ou OR-OP)
- Deux types de cellule
  - Cellules de contrôle
  - Cellules de relai
- Cellules de contrôle

  - CMD : padding, create/created, destroy

Cellules

- Cellules de relai



  - Données de bout en bout
  - CMD : relay data, relay begin/relay connected, relay teardown, relay extend/relay extended, relay truncate/relay truncated, relay sendme, relay end
  - Digest : contrôle d'intégrité + identifie l'OR ciblé

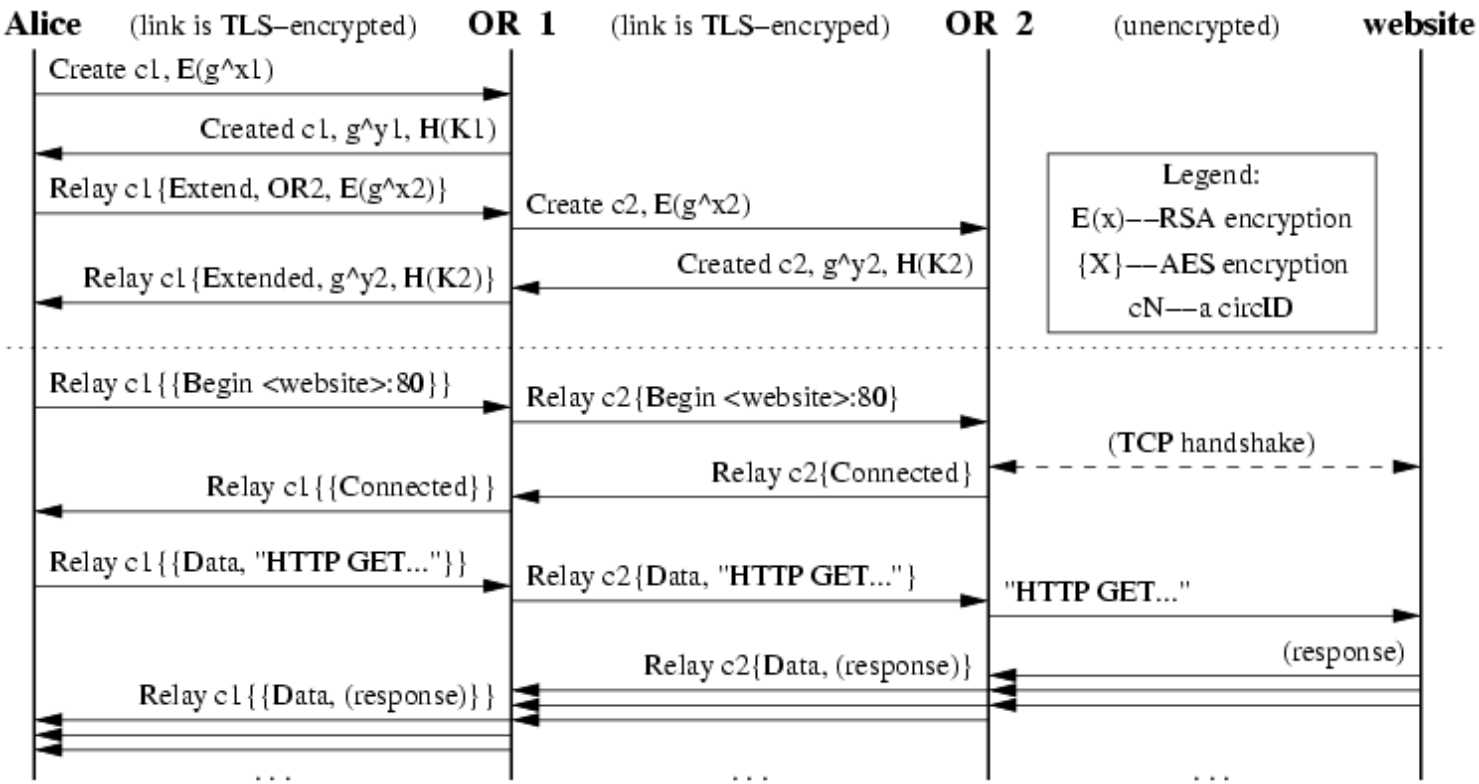
Circuit

- Plusieurs streams sur un même circuit
  - Construction d'un circuit "coûteuse"
- Circuits construits avant besoin
  - Eviter les délais au moment du besoin
  - Impact sur l'utilisation minimal
- OPs construisent de nouveaux circuits périodiquement
  - Anciens supprimés si utilisés
- Leaky pipe

Construction de circuits

- Construits de façon incrémentale
  - Diffie-Hellman
  - Négociation de clé symétrique avec chaque OR
- Utilisation des cellules de contrôle et de relai

Construction d'un circuit



Construction d'un circuit

- Authentification unilatérale
- Pour envoyer une cellule de relai à un OR précis :
  - Alice calcule le digest
  - Chiffre itérativement entête + données de relai
- Alice a la possibilité de choisir plusieurs points de sortie
  - Avoir des points de sortie différents sans recréer complètement des circuits
  - Exit policies

Ouverture de flux

- Application d'Alice demande à l'OP (via SOCKS)
- OP choisit le dernier circuit créé et choisit un OR comme point de sortie
- OP envoie un *relay begin* avec un nouveau *stream ID* aléatoire
- Le point de sortie répond par un *relay connected* après la négociation TCP
- OP notifie l'application via SOCKS du succès
- OP relaie les données dans des cellules *relay data*

Directory servers

- Noeuds spécifiques et redondants
- Référencent les ORs connus
  - Router descriptors (clés, exit policy, adresse, bande passante, ...)
- Clients doivent vérifier que les directories sont les mêmes sur d'autres serveurs
- Accessibles en HTTP
- $\Rightarrow$ Bootstrapping

Directory servers

- http ://moria.seul.org :9032/tor/status/authority

Example

r xposeIG2K 4P7wXEQ57as+boBhCuCIn0fyvzA laBwFecFIQnUW1deF2D1W0tBSng
2010-01-11 18 :50 :42 85.171.182.65 9001 0
s Exit Fast Running Valid
opt v Tor 0.2.1.20

Example

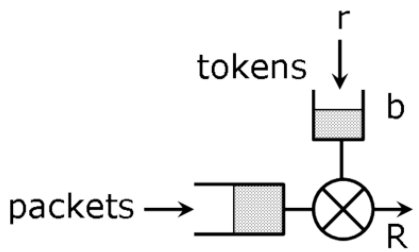
~/xpose $ cat authority |grep Running|wc -l
1754

Exit policies

- Améliorer le confort des utilisateurs voulant faire tourner des ORs
- Type d'ORs
  - *Open exit* nodes
  - *Middleman* nodes
  - *Private exit* nodes
- Restrictions de services
- $\Rightarrow$ Port 25 bloqué (spam)

Contrôle du débit

- Permet d'améliorer le confort des utilisateurs mettant des ORs à disposition
- Tocken bucket
  - Limite le débit moyen
  - Permet des bursts



- Service préférentiel pour les services interactifs
  - Basé sur la fréquence des cellules envoyées pour le stream concerné

Contrôle de congestion

- Exemple lorsque trop d'utilisateurs utilisent deux OR pour leurs circuits
- Délégation à TCP du séquencement, du renvoi...
- Se fait sur les cellules *relay data*
- Gestion de la congestion
  - Au niveau des circuits
  - Au niveau des flux
- Dans les deux cas, deux fenêtres
  - *packaging window* : quantité de cellules relayables vers l'OP depuis un flux TCP
  - *delivery window* : quantité de cellules relayables vers un flux un TCP

Contrôle de congestion

- Lorsqu'une cellule est envoyée, la fenêtre correspondante est décrémentée
- Envoi d'une cellule *relay sendme* lorsque nombre suffisant de cellules reçues
  - Circuits $\Rightarrow$ *streamID* de 0
  - Flux $\Rightarrow$ attente du flush sur le flux TCP
- Réception d'une cellule *relay sendme* incrémente sa fenêtre de *x*

Presque

- Requête DNS
  - Volonté de joindre ce serveur
- Cookies HTTP
- $\Rightarrow$ Privoxy
- Anonymat renforcé lorsqu'un OR local est utilisé
  - Premier OR peut être compromis

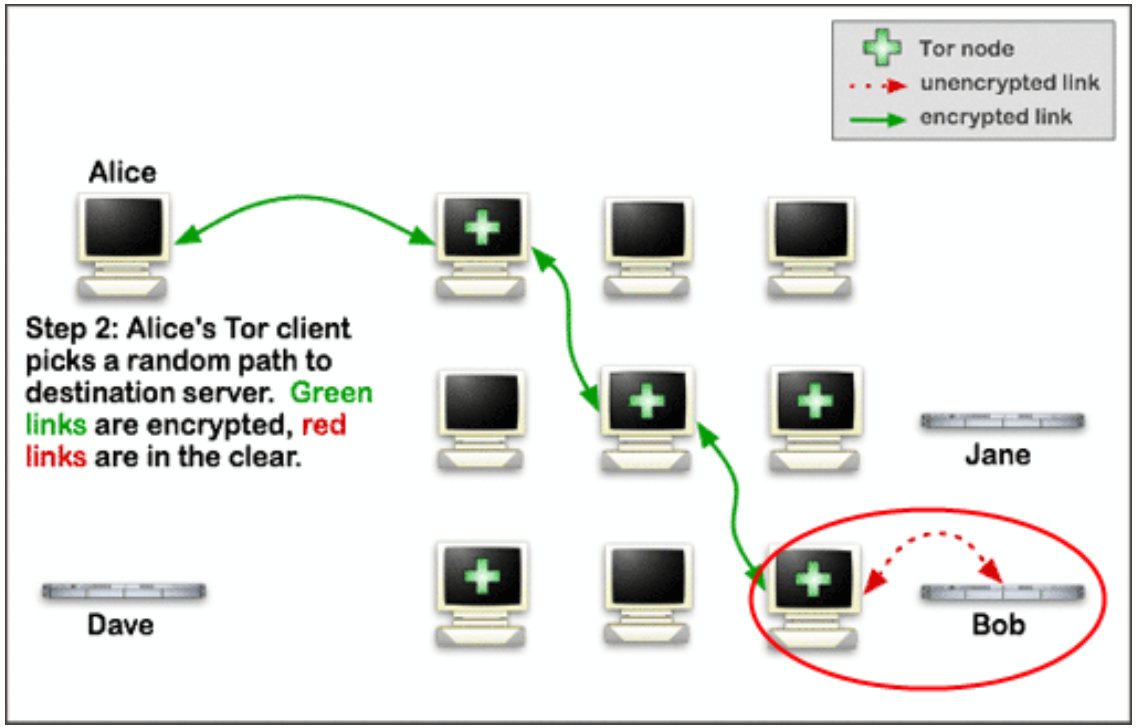
Attaques possibles

- Attaques passives
  - Observation
  - Corrélation de timing de bout en bout
- Attaques actives
  - Attaques de "marquage"
  - Faire tourner un OR hostile
- Attaques sur le service d'annuaires
  - Corrompre un directory server
  - Détruire le service (directory servers)
- Attaques contre les points de rendez-vous
  - Flood de requête d'introduction
  - Compromettre un point d'introduction

Anonymat n'est pas confidentialité

- Hack of the year 2007
- Monsieur qui apparait avec des comptes du gouvernement
- Spéculations sur son mode opératoire (man in the middle, etc.)
- LE maillon faible !

Anonymat n'est pas confidentialité



$\Rightarrow$ Chiffrement bout-à-bout comme TLS

Bibliographie

- http ://www.hatswitch.org/~nikita/
- http ://www.torproject.org/
- http ://www.xmcopartners.com/article-tor.html

Merci de votre attention

Questions ?