Navigation et traces

- Introduction
- Les indiscrétions des navigateurs
- Analyse de trafic
- Incognito

Introduction

- Cet atelier aborde les traces que l'on peut laisser **à notre insu** en naviguant sur le web. Le cas des réseaux sociaux (facebook, myspace, etc) est à part.
- Rappel : web ≠ internet

  Web est un application d'internet parmi d'autre : courrier électronique, messagerie instantannée, news, ...

Les indiscrétions de navigateurs

- Historiques
- Cookies
- Sessions
- Cache
- Mots de passe
- Autres

Historiques

- Navigation : liste chronologique des site visités :
  - URL, nom du site, date et heure de visite.
  - Configuration de la durée de conservation.
  - Fichier places.sqlite.
  - Purge.

- Gestionnaire de téléchargements : fichier downloads.sqlite

Cookies

- Petits fichiers texte permettant la sauvegarde d'informations qui peuvent être personnelles, comme les mots de passe.
- Vente en ligne : sauvegarde du panier.
- Exemple :

  http://ent.uae.ac.ma/servlets-examples/servlet/CookieExample
- Pour firefox, ils sont stockés dans le fichier cookies.sqlite de votre profil.
- Configuration et purge possibles.
- Extension firefox : Extended Cookie Manager 0.9

Sessions d'identification

- Session limitée dans le temps pour les sites protégés par un système d'authentification.
- Déconnexion après un certain temps d'inactivité.
- Faire attention lors de la visite d'un site protégé sur une ordinateur public !
- Purge possible

Caches mémoire et disque

- Recopie intégrale en mémoire et sur le disque des pages visitées. But : économie de bande passante.
- Répertoire Cache de votre profil firefox about:cache
- Purge possibles.

Mots de passe

- Enregistrement des mots de passe des sites protégés
- Sans « mot de passe principal », ils sont stockés en clair !
- Fichier signons3.txt de votre profil Firefox. Le fichier key3.db est la clé de chiffrement. Dans Firefox 3.1, signons.sqlite.
- Purge et configuration possibles.

Autres

- Cache de recherches : search.sqlite
- Données de formulaires : formhistory.sqlite
- Signets : places.sqlite

Parades

- Purge à chaque sortie.
- Mode « privé » : Firefox 3.1, Safari, IE 8 : pas d'historiques, cookies en mémoire vive.

Analyse de trafic

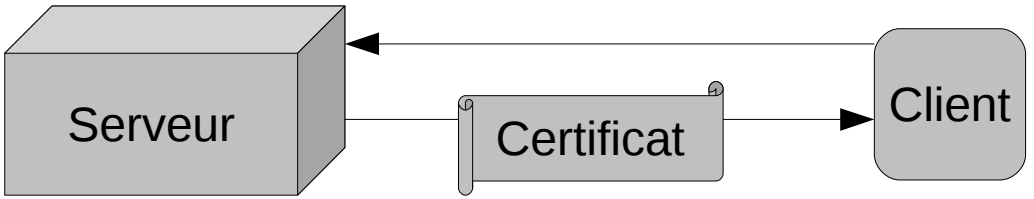
- HTTPS
- Tor, privoxy

HTTPS

- HTTPS (S pour « sécurisé ») est la combinaison de HTTP avec SSL ou TLS.
- Sécurisation des transferts et identification du site visité.
- Devrait être utilisé dans toutes les communication privées : banque, commerce en ligne, messagerie...

HTTPS (2)

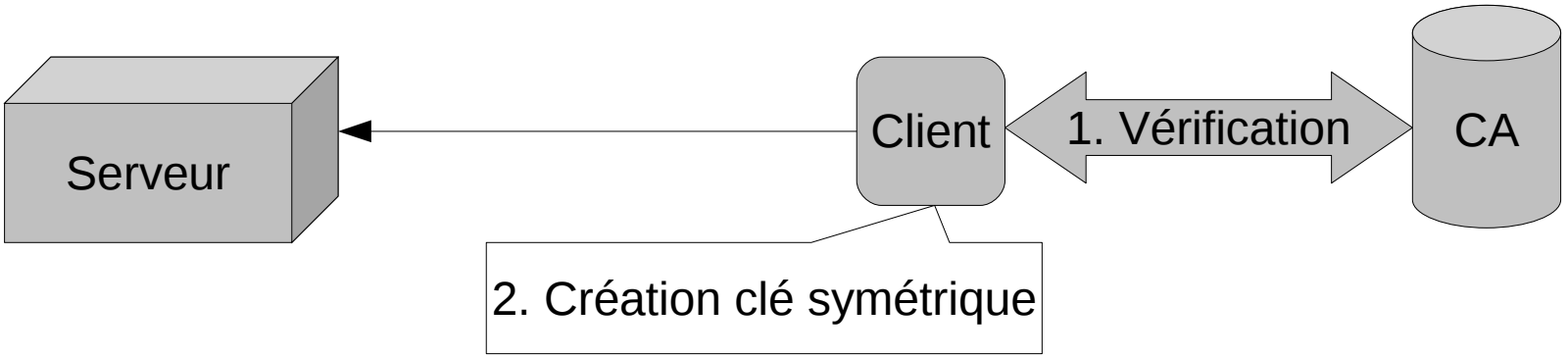
- Fonctionnement



  - Le client se connecte en https au serveur, et demande de s'authentifier. Il lui envoie la liste des cryptosystèmes qu'il supporte.
  - Le serveur renvoie un certificat SSL au client. Ce dernier contient la clé publique du serveur – signée ou non, et le cryptosystème choisi.

HTTPS (3)

- Fonctionnement



  - Le cas échéant, le client vérifie la validité du certificat – l'authenticité du site chez l'autorité de certification, crée un clé de session pseudo aléatoire, la chiffre avec la clé publique du serveur, et lui envoie.
  - Le serveur déchiffre la clé symétrique avec sa clé privée. Les communications chiffrées peuvent alors commencer.

HTTPS (4)

- Avantage : cryptographie hybride, combinaison entre un algorithme asymétrique et un algorithme symétrique, ce dernier étant bien plus efficace.
- Deux types de certificat :
  - auto-signés, permettent la confidentialité de échanges,
  - signés par un organisme de certification, permettent la confidentialité des échanges, et l'identification du site visité.
- Méthode ne permettant pas l'anonymat !

Tor, Privoxy

- Tor (The Onion Router) est un réseau de tunnels virtuels. Son but est de transmettre permettre des communications TCP avec un anonymat relatif.
- Privoxy est un proxy web filtrant. Il permet un filtrage avancé des pages visitées : cookies, publicité, pop-up...

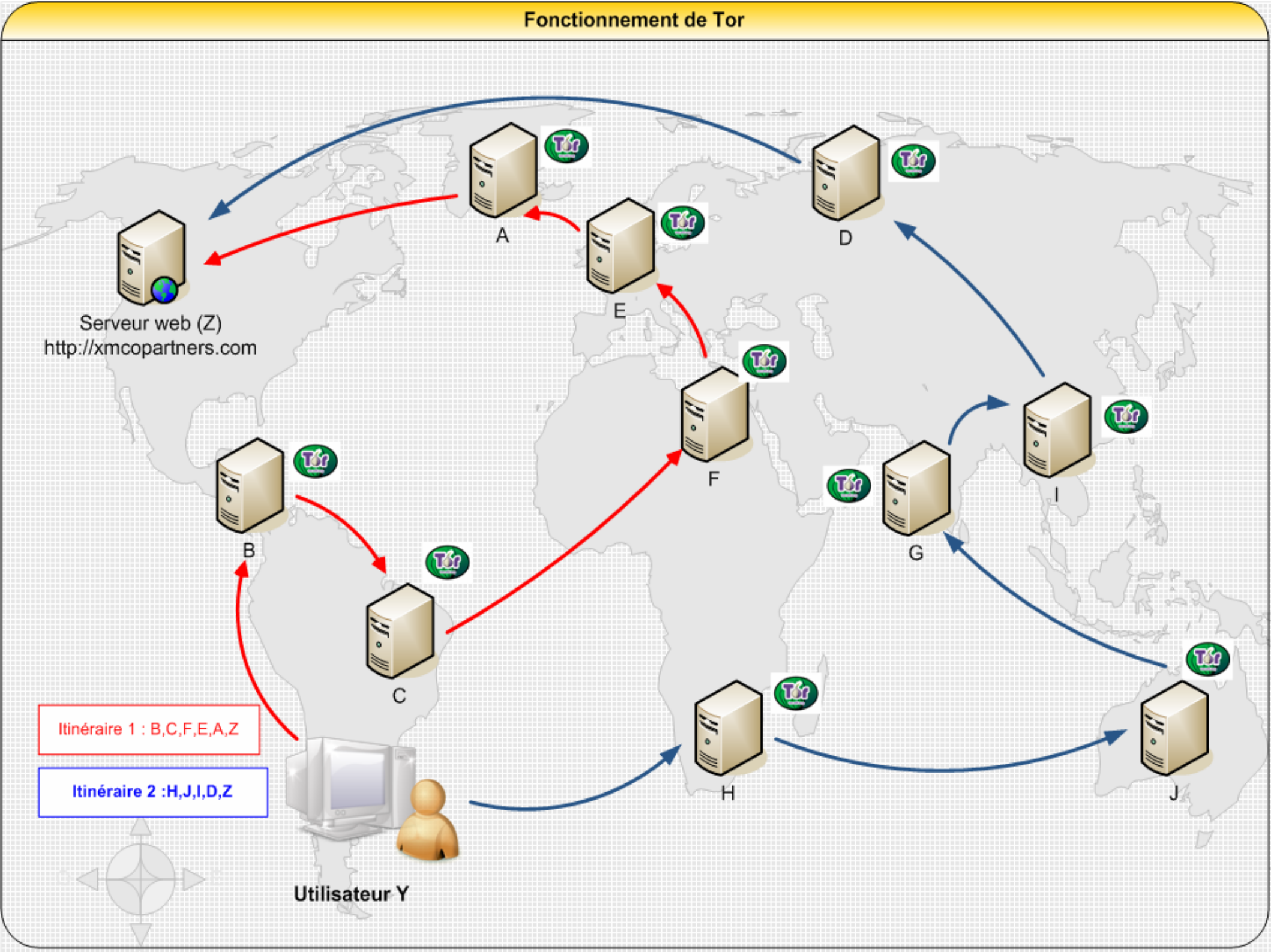
Tor, Privoxy (2)

- Principe : faire rebondir l'échange TCP au sein d'internet afin que des analyses de trafic ne puissent identifier l'utilisateur
- Construction d'un chemin aléatoire – une suite de noeuds tor. Chaque nœud ne connaît que son prédécesseur et son successeur
- Cryptographie hybride.
- Le noeud de sortie (« exit node ») envoie la requête en clair au serveur.

Tor, Privoxy (3)

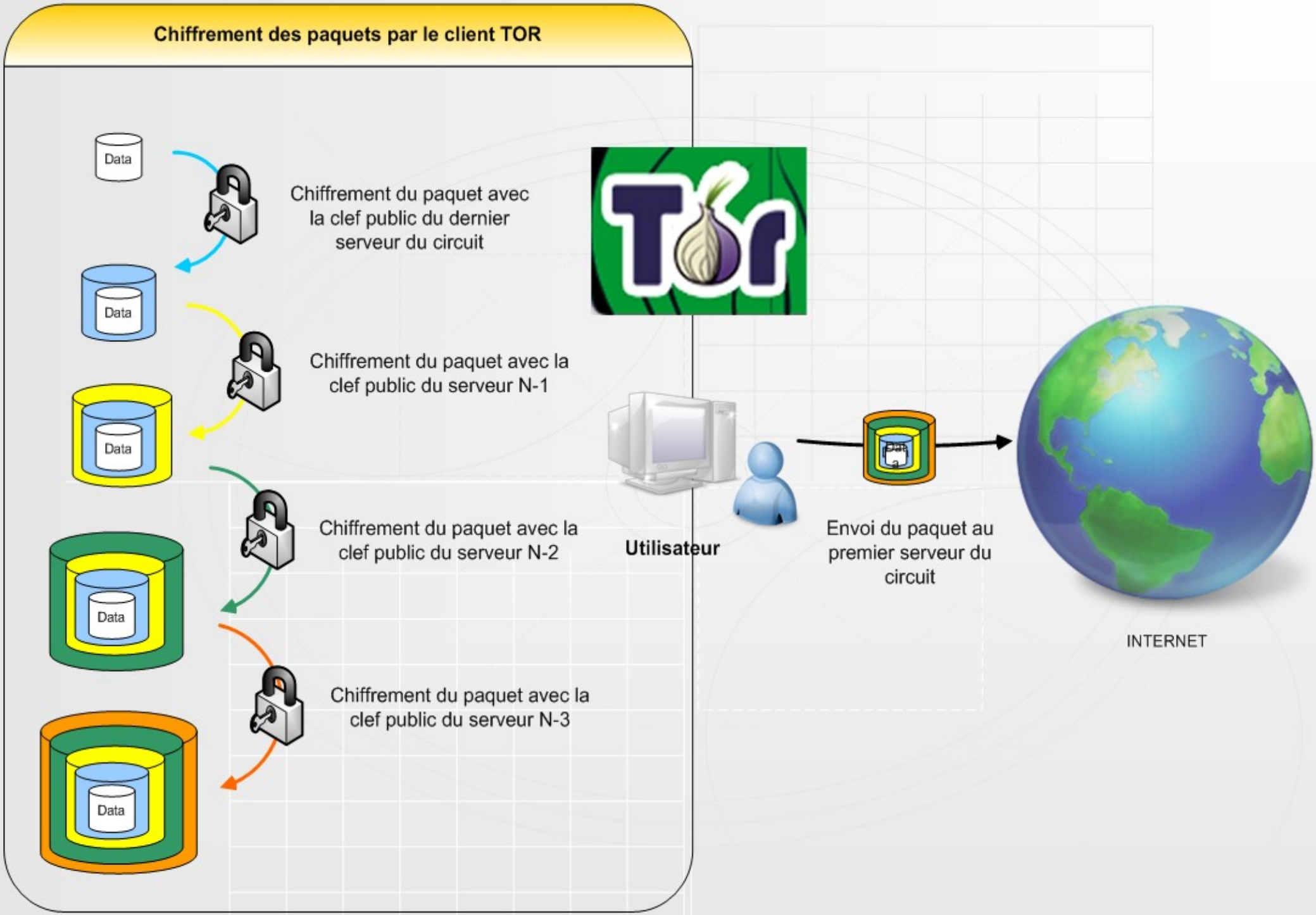
- Fonctionnement : construction du circuit
  - Le client demande à un serveur « annuaire » la liste des nœuds tor, et leur clé publique respective.
  - Le client choisit un chemin aléatoire, qui pourra changer au bout d'un certain intervalle de temps.
  - Le client distribue à chaque noeud une clé symétrique, chiffrée avec la clé publique du noeud.
  - Finalement, chaque nœud a une clé symétrique qui lui est propre, et ne connaît que son successeur et son prédécesseur au sein du circuit.

Fonctionnement de Tor

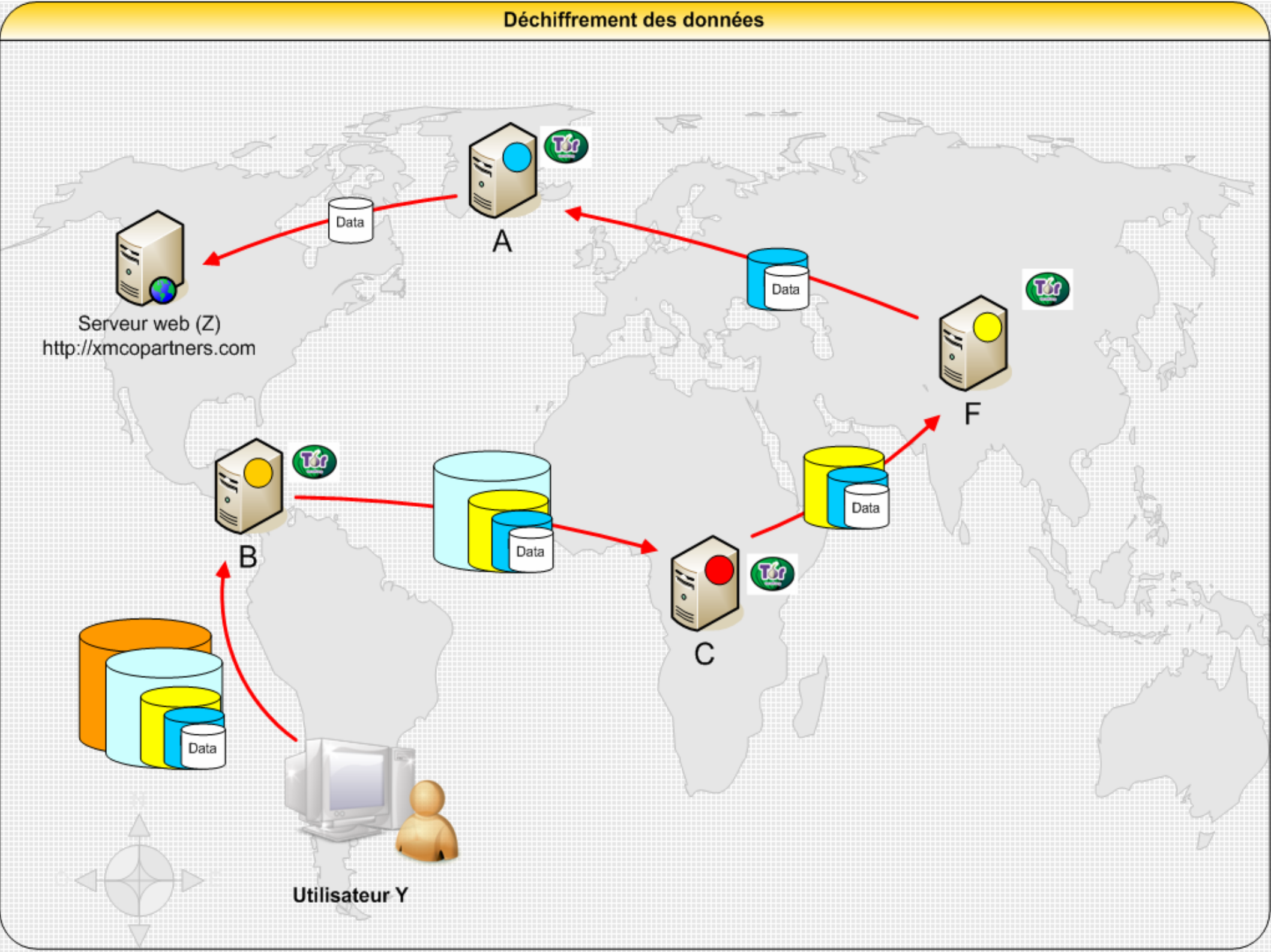


Tor, Privoxy (4)

- Fonctionnement : échange de paquets
  - À l'envoi d'un paquet, le client doit chiffrer le paquet autant de fois qu'il y a de nœuds dans le chemin choisi, dans l'ordre inverse du chemin.
  - Analogie avec l'oignon.
  - Chaque nœud déchiffre le paquet (« pêle l'oignon »). Le dernier nœud obtient donc le paquet original.
  - Le serveur voit la requête comme venant du nœud de sortie.


Chiffrement des paquets par le client TOR
Data
Chiffrement du paquet avec la clef public du dernier serveur du circuit
Data
Chiffrement du paquet avec la clef public du serveur N-1
Data
Chiffrement du paquet avec la clef public du serveur N-2
Data
Chiffrement du paquet avec la clef public du serveur N-3
Data
Utilisateur
Envoi du paquet au premier serveur du circuit
INTERNET

Déchiffrement des données



Tor, Privoxy (5)

- Les limites
  - Flash, Java : utilisation de NoScript et FlashBlock.
  - Le noeud de sortie voit le paquet en clair, si HTTPS n'est pas utilisé pour la communication avec le serveur.
  - Si une organisation a un très grand nombre de nœuds sur le réseau, l'anonymat est compromis.
  - Certains sites refusent le trafic venant d'un nœud tor.

Tor, Privoxy (6)

- Installation - Debian et dérivées :
  - **# aptitude install tor privoxy vidalia**
  - **# aptitude install tork**
  - Édition du fichier /etc/privoxy/config :

    forward-socks4a / localhost:9050

    listen-address
- Installation – Windows : paquet « tout en un »
- Configuration du proxy Firefox.
- Utilisation de TorButton ou SwitchProxy.

Incognito

- Live CD orienté anonymat.
  - Utilisation de Tor, Privoxy.
  - Aucune écriture sur le disque dur.

Références

- http://fr.wikipedia.org/wiki/Secure_Sockets_Layer
- http://www.torproject.org
- http://www.xmcopartners.com/article-tor.html
- http://www.informationprivacy.org/en/anonymous_web_surfing/tor/weaknesses_of_tor
- http://www.anonymityanywhere.com/