Sécurité informatique
M2 CCA
2014-2015
Confidentialité, HTTPS/TLS
Pascal Petit

Licence de ce document

- licence créative common BY-SA
- cf http://creativecommons.org/licenses/by-sa/4.0/
- pour réaliser ce document, j'ai utilisé le travail d'autres personnes que je remercie et qui sont citées :
  - soit directement si leur travail est utilisé tel quel
  - soit en bibliographie si leur travail m'a permis d'améliorer ma compréhension du domaine sans être utilisé directement
- un retour normal est de permettre à quiconque d'utiliser les éléments de ce document librement :
  - à condition de me citer
  - et de respecter les mêmes conditions d'utilisation
- parmi les sources utilisées, remerciements particuliers à
  - S. Bortzmeyer pour son blog (et ses tee-shirts :-)) : http://www.bortzmeyer.org/
  - V. Bernat pour son article sur PFS

De la faiblesse des mots de passe

- Face à la prolifération de la videosurveillance
- En cas d'utilisation d'un ordinateur non sur (virus, webcafé, ...)

double authentification

- fournir un mot de passe
- ET une information transmise ou calculée hors internet
- Exemple : double authentification de google
  - mot de passe
  - + code transmis par SMS ou calculé par application sur smartphone. code à usage unique
- permet la consultation en environnement hostile (keylogger, machine vérolée, yeux)

L'impact de l'espionnage

- vie privée
- protection des sources
- protection des intérêts économiques

Vie privée

- citer des éléments
- « je n'ai rien à cacher » :
  - faux
  - vis à vis de qui ?
  - je ne fais rien d'illégal
    - actuellement
    - mais la réglementation peut changer
    - les traces sur internet, chez les espions restent
- vidéo intéressante :
  - PSES2013, Numendil, « Si ! vous avez quelque chose à cacher », https://www.youtube.com/watch?v=BbkbdYoffX4

Protection des sources : fadettes

- fadette : relevé des appels téléphoniques entrants et sortants (métadonnées)
- sources :
  - 01/2012, plainte du monde suite à l'utilisation par le procureur de Marseilles de fadettes de ses journalistes : http://www.lefigaro.fr/flash-actu/2012/01/18/97001-20120118FILWWW00411-fadettemarseille-plainte-du-monde.php
  - 09/2010 : affaire Bettancourt : plainte du monde après l'utilisation de fadettes de ses journalistes

Protection des sources

- les journalistes sont des cibles
  - leurs sources sont en danger
  - exemple concret :
  - « The spy who came in from the code, How a filmmaker accidentally gave up his sources to Syrian spooks »
  - cf http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all

Protection des intérêts économiques

Données et métadonnées

- Données
- Métadonnées :
  - données permettant de définir ou décrire une données
- Exemples :

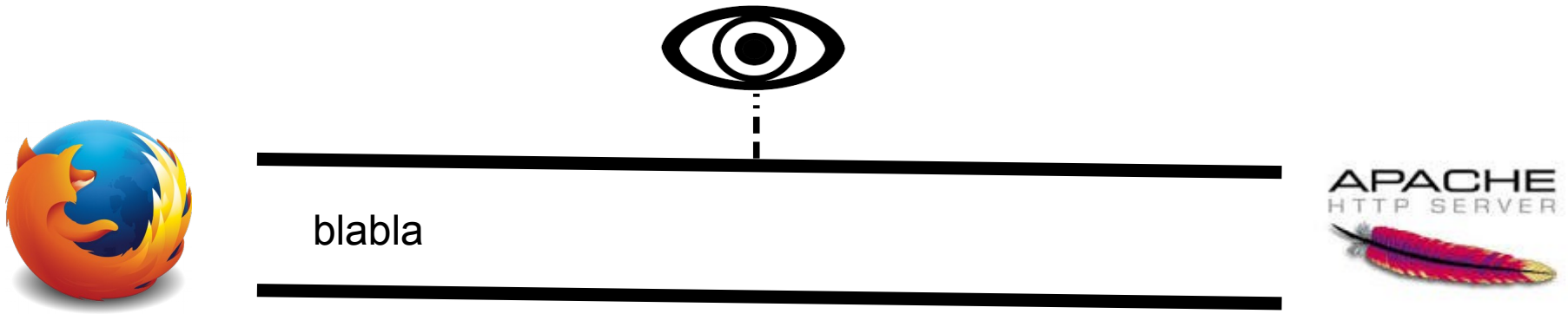
	donnée	**métadonnées**
photo	image	info exif, gps
appel téléphonique	conversation	date, No tel. appelant, appelé
mail	contenu du mail, fichiers joints, ...	entête
document bureautique	contenu du fichier	Fichier/Propriétés
mp3	son	tagID3

Les métadonnées c'est de l'espionnage (B. Schneier)

- embaucher un détective pour surveiller quelqu'un
  - où il est a été
  - à qui il a parlé
  - ce qu'il a regardé
  - comment il a occupé sa journée
- ce sont des métadonnées
- c'est de la surveillance
- source :
  - 23/09/2013, « Metadata Equals Surveillance », https://www.schneier.com/blog/archives/2013/09/metadata_equals.html

httpS: une solution

- httpS: web sécurisé (terme commercial et imprécis)
- httpS = http (WeB) + ssl/tls (chiffrement)
- Extension navigateur : httpseverywhere
- Tunnel chiffré en votre navigateur et le serveur



L'espion ne voit pas ce qui se passe dans le tunnel chiffré

TLS : services fournis

- modèle client/serveur
- confidentialité via un tunnel chiffré entre client et serveur
- Authentification du serveur (à partir de ssl v2)
- intégrité et identification de la source des données
- Authentification du client (optionnelle)

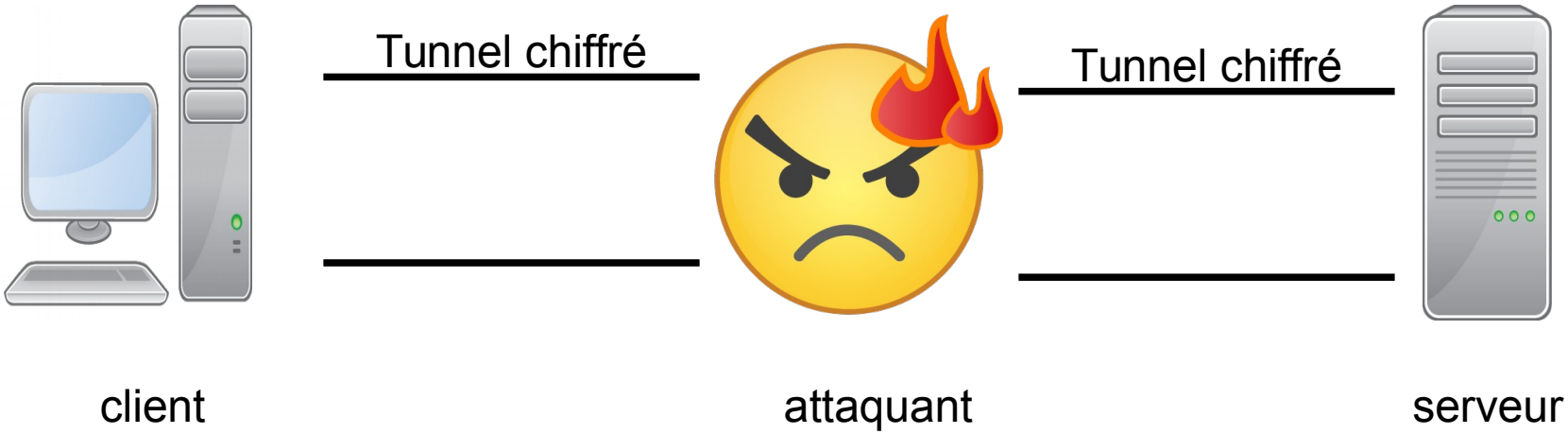
TLS : ce qu'il ne fait pas

- TLS ; c'est de l'informatique, pas de la magie. Il ne protège pas
  - si un programme espion tourne sur votre poste de travail
  - si le serveur est compromis
  - si les données envoyées sont compromises plus tard par l'incompétence de la société qui les gèrent
  - si vous ignorez les alertes sur le fait que le certificat du site distant est obsolète ou ne correspond pas au site ou est autosigné
  - exemple de compromission de données : Sony en 2011, 77 millions de comptes concernées (http://www.pcinpact.com/news/63279-sony-psn-qriocity-vol-donnees-bancaires-personnelles.htm)
  - 12/2013, 40 millions d'informations bancaires volées à la chaîne de grande distribution Target (USA) http://www.zdnet.fr/actualites/donnees-privees-le-piratage-de-target-encore-plus-grave-qu-annonce-39796580.htm et http://www.zdnet.fr/actualites/donnees-privees-target-confirme-le-vol-des-codes-pin-chiffres-39796624.htm

Authentification du serveur

- via des certificats X509 (rfc5280, https://tools.ietf.org/html/rfc5280) ;
- le serveur a un couple clé privée/clef publique. La clef privée est connue seulement du serveur ;
- un certificat associe une identité à une clef publique ;
- fournie la certitude (ahem!) que c'est bien la clef publique du serveur
- indispensable pour garantir :
  - qu'on se connecte sur le bon serveur et pas sur un serveur pirate (hameçonnage)
  - pour éviter les attaques « Man In the Middle » (MiM)

authentification serveur : MiM



Sans authentification du serveur, un attaquant peut se faire passer pour le serveur et en même temps, se connecter au serveur

- la clef publique qu'il envoie au client est la sienne (et pas celle du serveur)
- il espionne tout le trafic
- il peut modifier les données transmises

Les donnée sont chiffrées entre le client et l'attaquant et entre l'attaquant et le serveur

authentifier un serveur

- Crytpo asymétrique (à clef publique) :
  - le serveur a une clef privée connue de lui seul
  - la clef publique peut être donnée à tous
  - pour s'authentifier, le serveur démontre qu'il a la clef privée correspondant à la clef publique
- Problème :
  - la clef publique est-elle bien celle du serveur ?
  - si un attaquant nous fait croire qu'une clef publique est celle de du serveur, il peut se faire passer pour lui

Certifier une identité

Carte d'identité

Pascal PETIT
validité : 22/04/2011

Certifier une identité

certifier une identité

- les papiers d'identité permettent de certifier une identité
- la confiance repose sur :
  - l'émetteur du papier d'identité
  - les procédures qu'il suit (carte d'identité vs carte d'étudiant vs carte navigo vs bout de papier auto-imprimé)
  - l'impossibilité de créer de faux papiers
- de nombreux états, de nombreuses autorités de confiance
- peut-on faire confiance à un état si on a maille à partir avec ses services secrets ?

Certificat X509

- l'association d'une clef publique et d'une identité
- certifiée directement ou indirectement par une autorité de certification
- autorités de certifications reconnues :
  - de base dans le navigateur (nombreuses)
  - ou ajoutées manuellement
- la confiance repose :
  - sur la solidité des protocoles de crypto (être capable de faire un faux certificat ~ faire des faux papiers)
  - le sérieux et la fiabilité d'autorités de certifications
- avis personnel : ça ne marche pas bien

Exemples réels passés de problèmes avec les certificats

- les autorités ajoutées aux navigateurs et l'espionnage des entreprises
- idem mais via un vrai/faux certificat : quand l'état français joue avec le feu
- tunisie : quand une autorité de certification nationale aide les services secrets
- Diginotar : piratage d'une autorité de certification

Man In the Middle

- dans le monde, 1800 entités capables d'émettre des certificats pour n'importe quel domaine et reconnues par les navigateurs
- cf IMC 2013, « Analysis of the HTTPS Certificate Ecosystem », Z. Durumeric, J. Kasten, M. Bailey, J.A. Halderman (University of Michigan) , http://conferences.sigcomm.org/imc/2013/papers/imc257-durumericAemb.pdf

TLS et la NSA : PFS

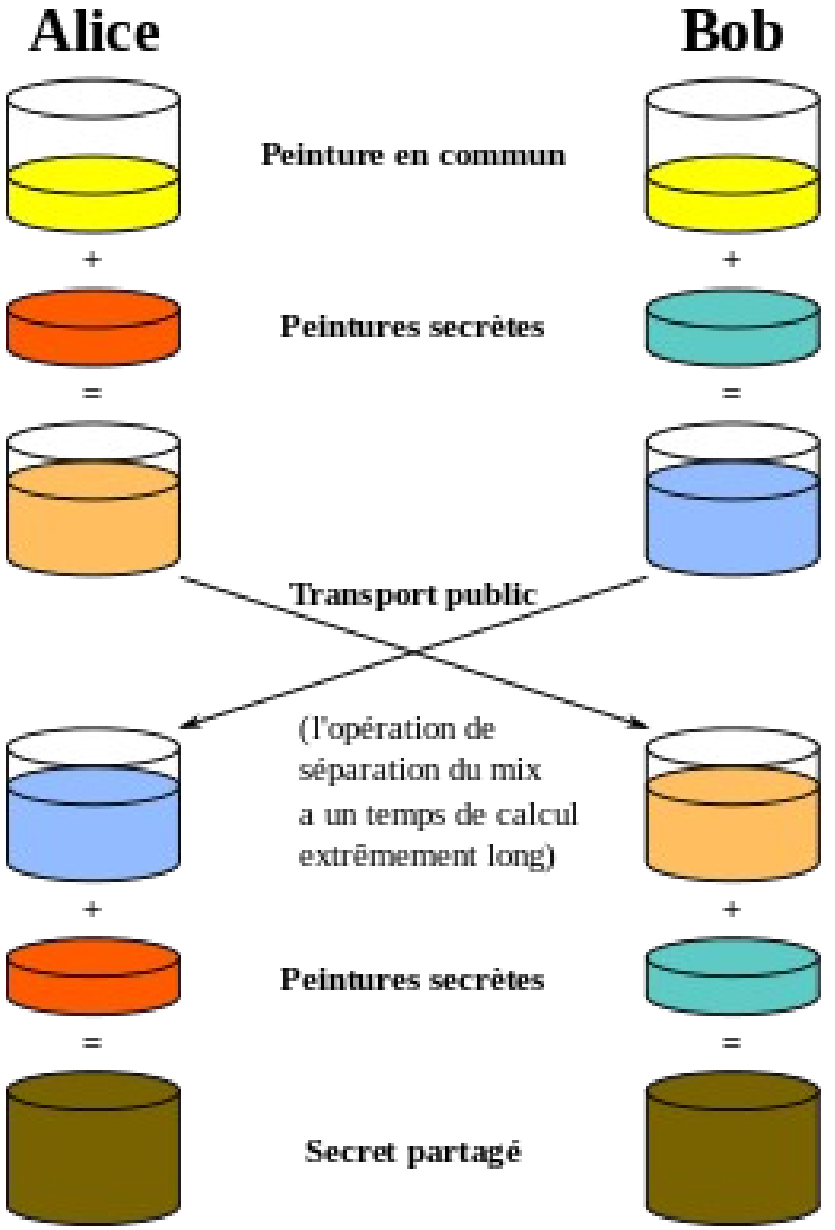
- de base, TLS utilise le certificat pour :
  - authentifier le serveur
  - chiffrer un secret partagé, clef du chiffrement symétrique
- conséquence
  - posséder la clef privée du serveur => déchiffrer le trafic
    - obtenir les éléments permettant de le faire
    - en temps réel ou via un enregistrement de tout le trafic
  - la NSA (& Co) peut obtenir cette clef privée légalement
- source :
  - [VB2011] « SSL/TLS & Perfect Forward Secrecy » de V. Bernat, http://vincent.bernat.im/fr/blog/2011-ssl-perfect-forward-secrecy.html

Solution : Diffie Hellman

- se mettre d'accord sur une donnée secrète commune
- en échangeant des messages public
- l'attaquant peut voir les messages publics mais ne peut en déduire le secret commun

Diffie Hellman

- principe :
  - Alice a une donnée secrète (couleur orange)
  - Bob a une donnée secrète (couleur bleue)
  - transmise mélangée à une donnée publique (couleur jaune)
  - le secret commun est :
    - Alice : orange+(jaune+bleu)
    - Bob : bleu + (jaune+orange)
  - principe : impossible de séparer des couleurs mélangées



source : wikimedia

Repérage par son adresse IP

- L'adresse IP de votre ordinateur (ou du proxy de sortie) est connue du destinataire (cf http://ifconfig.me)
- Moyen pour vous tracer
- Pour vous géolocaliser
- Pour interdire certains services selon les pays
- Solution : VPN (Virtual Private Network)

VPN

- Être ailleurs tout en étant ici :
  - Permettre à l'ordinateur d'un salarié d'être vu comme étant sur le réseau de l'entreprise
  - Faire passer tout son trafic internet par le VPN et être vu comme venant de l'extrémité du VPN
    - Pour se protéger de l'espionnage du réseau local où est notre ordinateur en profitant du tunnel chiffré du VPN
    - Pour contourner la geolocalisation IP
- Trafic chiffré entre vous et le serveur VPN
- Ajoute un réseau virtuel entre vous et un serveur ou réseau distant

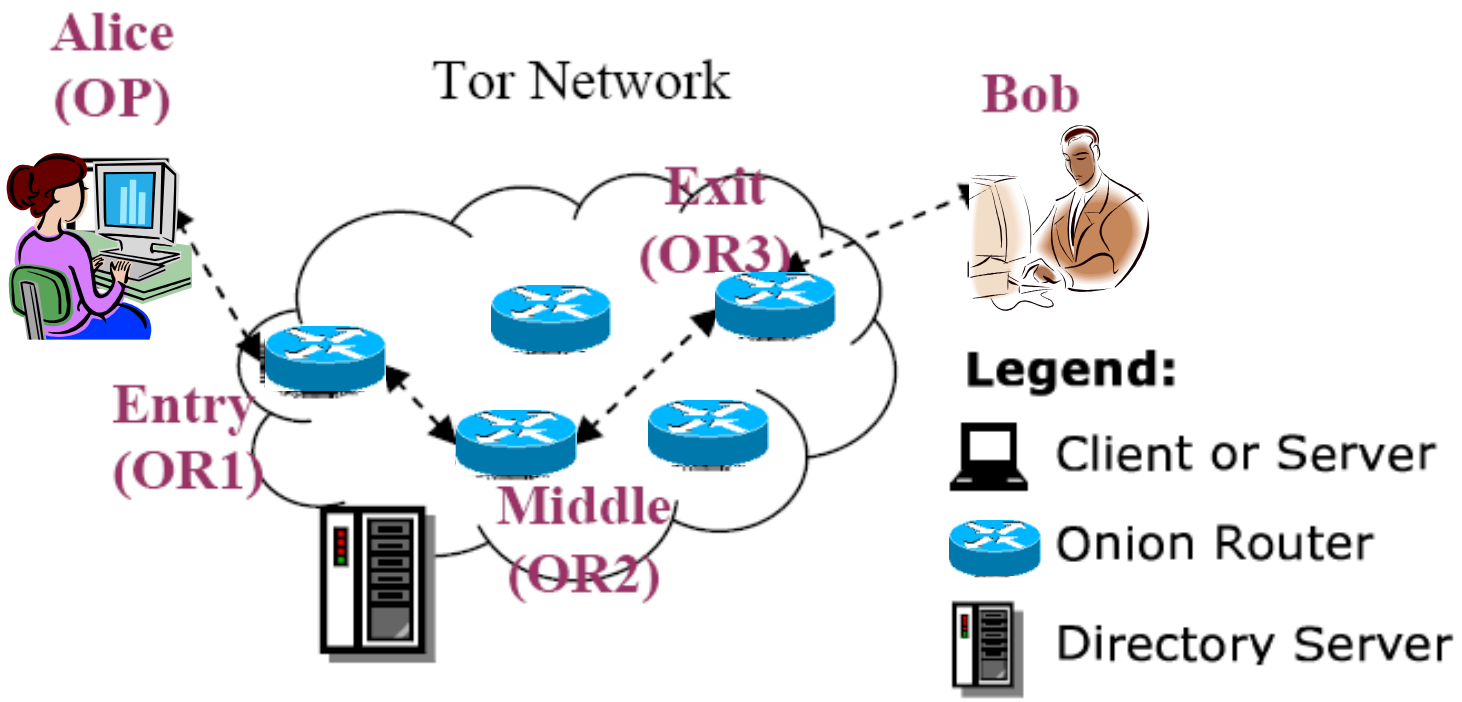
TOR : The Onion Routeur

- Comment se protéger de l'espionnage par le fournisseur de service ? Par le stockage des métadonnées
  - Google stocke les recherches que vous faites
  - Facebook (et google et …) veut tout savoir de vous. Il suffit d'aller sur une page avec un bouton « j'aime »
  - Ces données pourront servir à d'autres que google/facebook à l'avenir
- Des solutions techniques, des solutions politiques (exemples : caméra en ville, reconnaissance faciale, de plaques minéralogiques,...)

TOR : The Oignon Router

- Objectifs :
  - transmettre de manière anonyme des flux TCP
    - chiffre les requêtes entre vous et TOR ;
    - camoufler votre IP au service destination ;
    - seul le routeur de sortie peut avoir accès à votre requête mais ne sait d'où elle provient ;
    - seul le routeur d'entrée peut savoir quelle est la machine source de la requête.
- Moyens :
  - chiffrement en couche
  - un ensemble de routeurs camouflant l'ip source des connexion TCP qu'ils transmettent : proxy

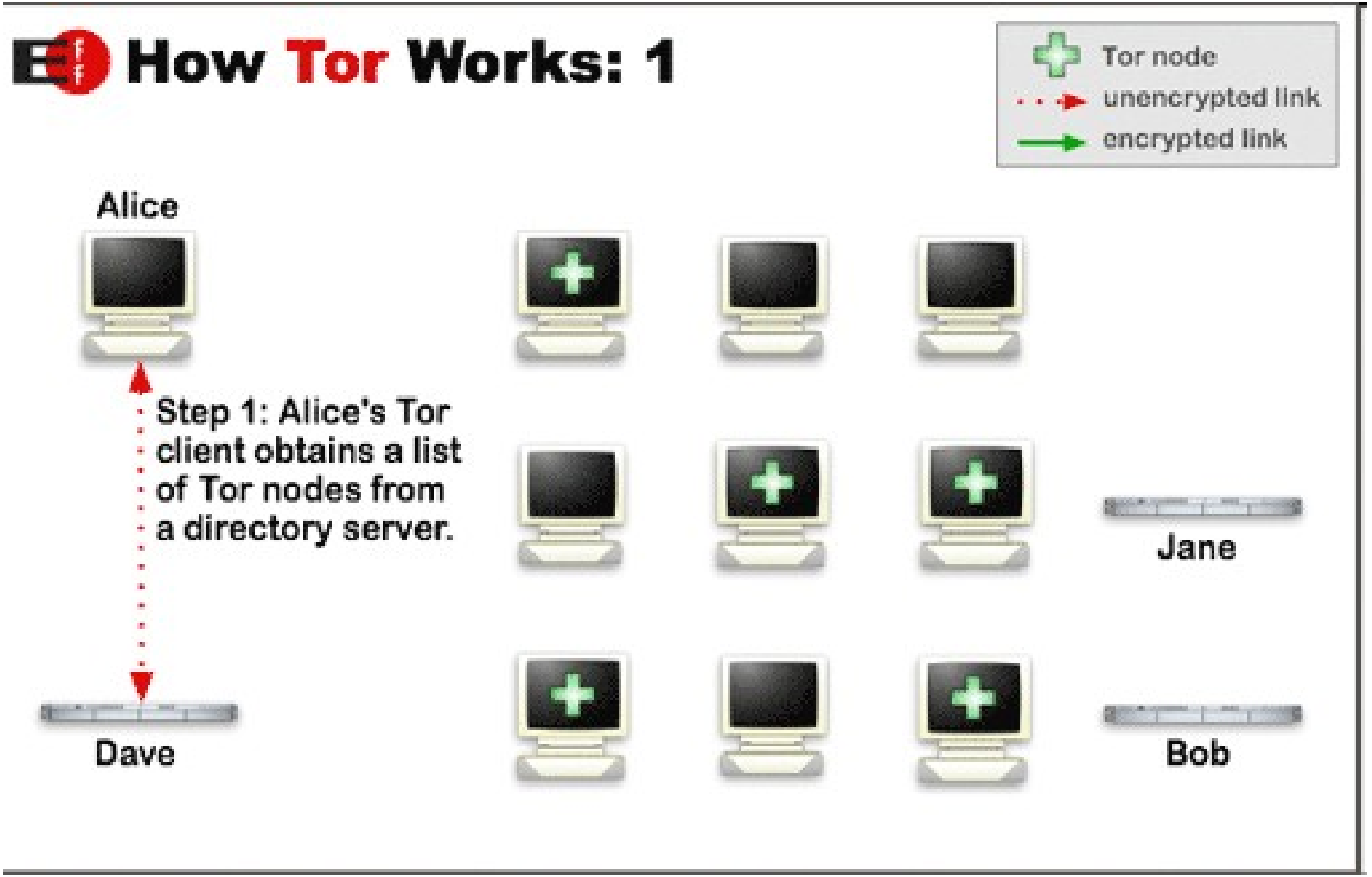
Composants de Tor



- **Client**: L'utilisateur du réseau TOR, envoie une requête au serveur Bob
- **Server**: une application TCP cible sur le serveur Bob
- **Tor (onion) router**: un proxy spécial qui relaie la requête
- **Directory server**: serveur fournissant des informations sur les routeurs TOR

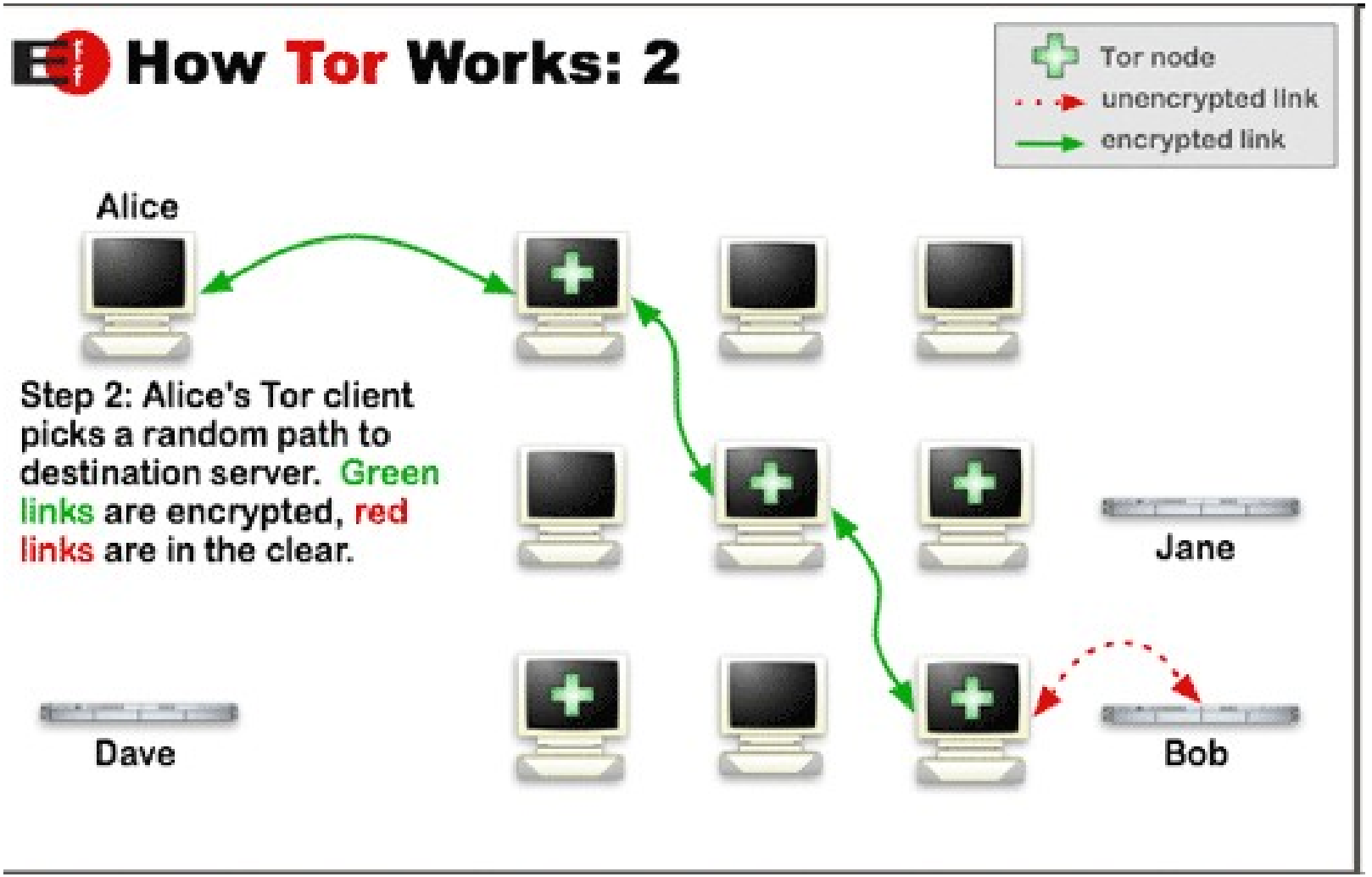
source:
http://www.cse.unr.edu/~mgunes/cpe401/cpe401sp11/student/tor.ppt

How does Tor work?



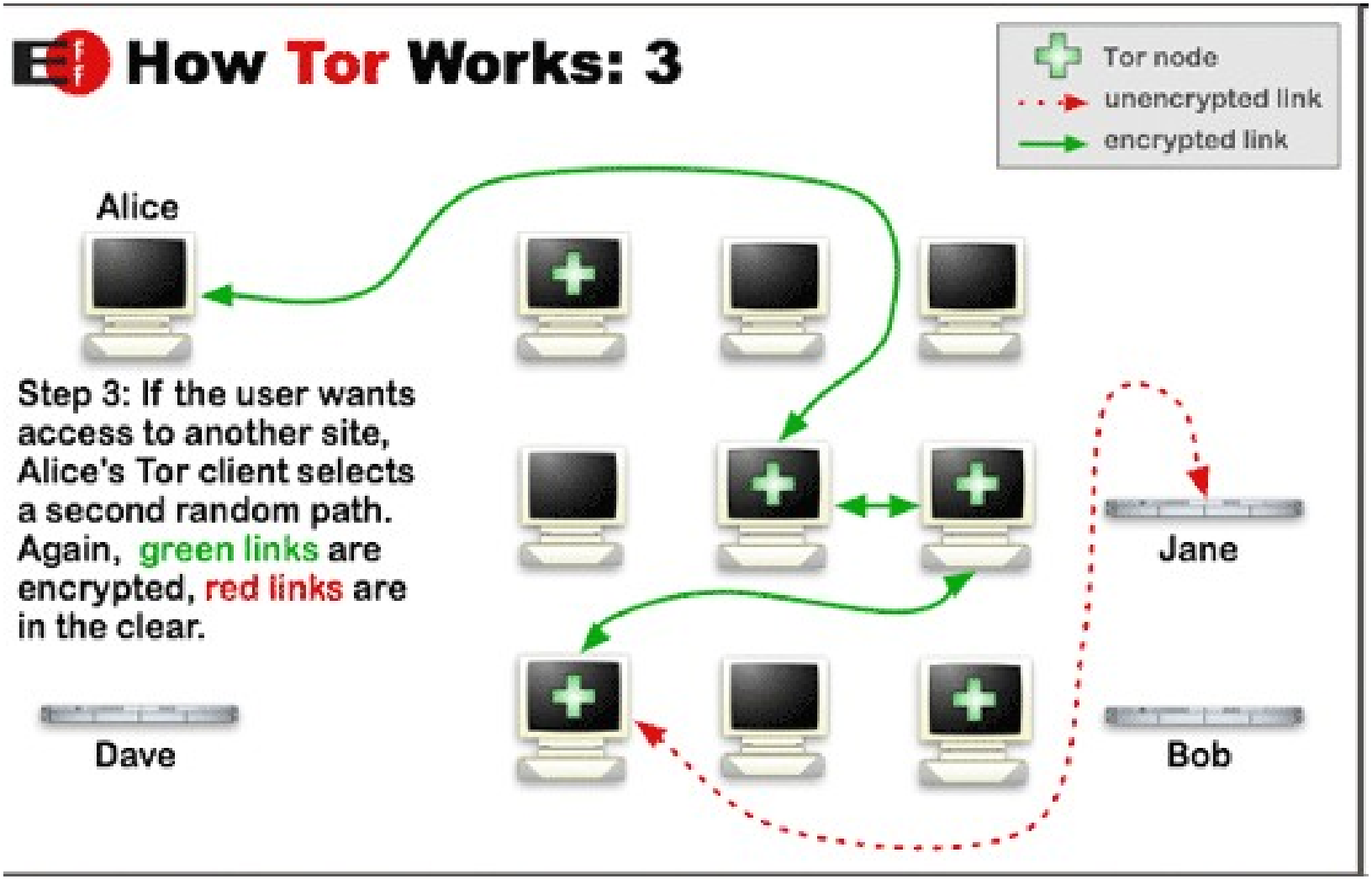
source:
http://www.cse.unr.edu/~mgunes/cpe401/cpe401sp11/student/tor.ppt

How does Tor work?



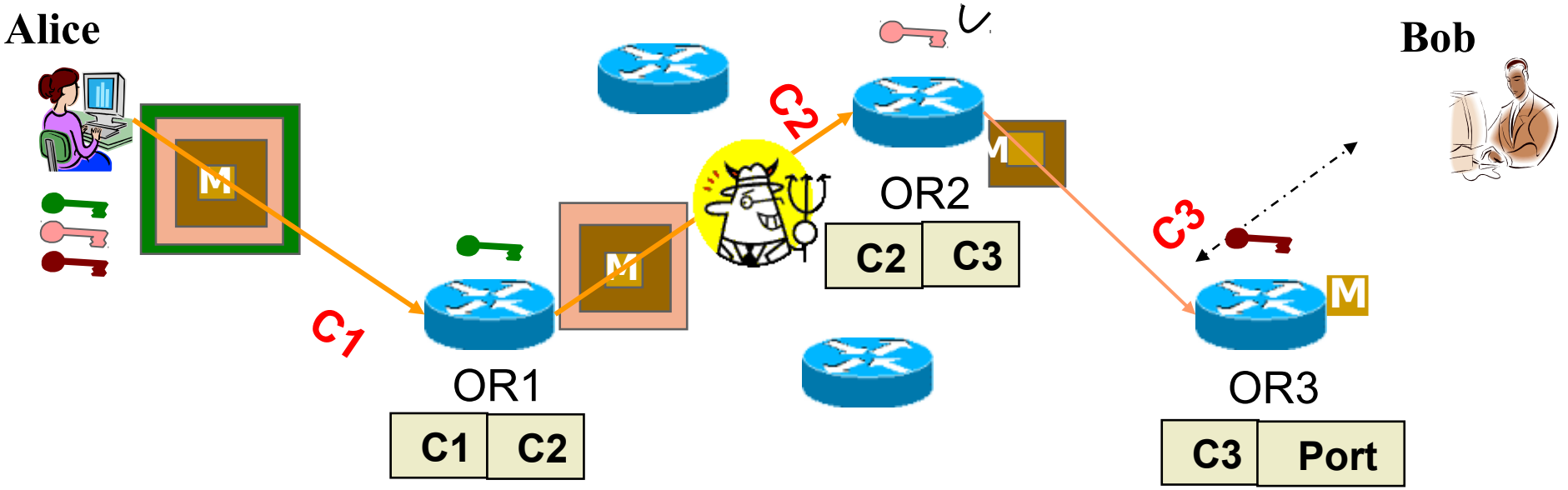
source:
http://www.cse.unr.edu/~mgunes/cpe401/cpe401sp11/student/tor.ppt

How does Tor work?



source:
http://www.cse.unr.edu/~mgunes/cpe401/cpe401sp11/student/tor.ppt

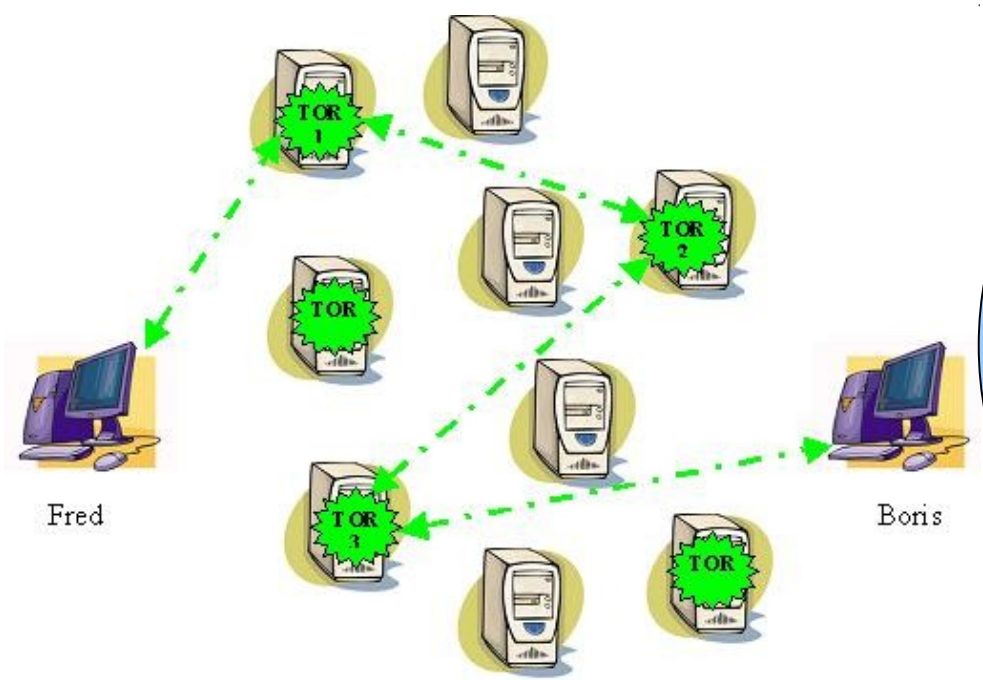
How Tor Works? --- Onion Routing

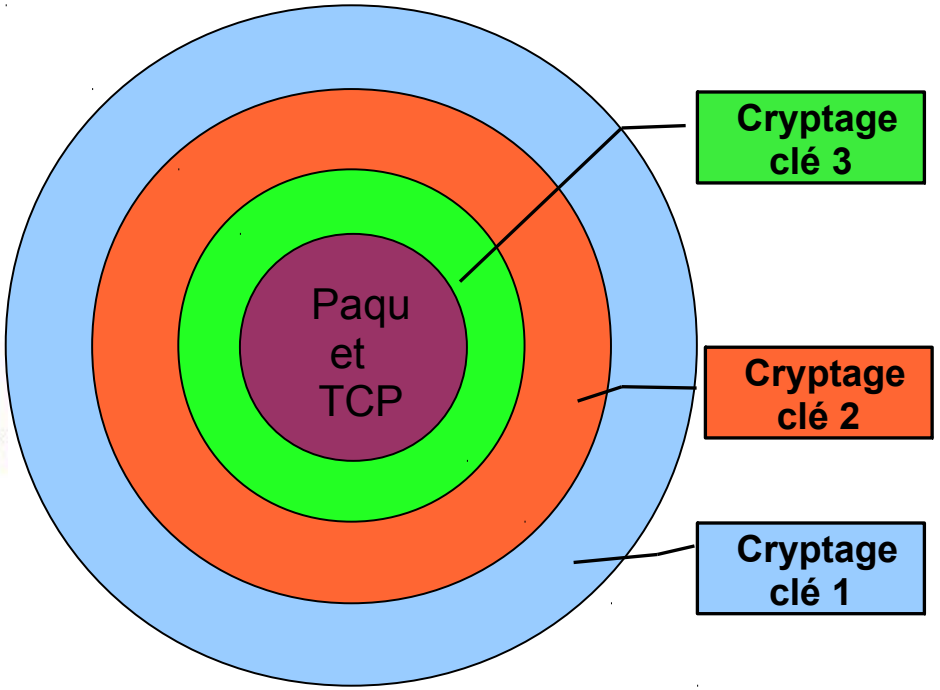


- un circuit est créé pas à pas
- chiffrement en couches d'oignons
  - Alice négocie une clef avec chaque routeur via diffie-hellman
  - chaque routeur ne connaît que son prédécesseur et son successeur
  - quand un routeur déchiffre le message, il y trouve :
    - un paquet chiffré et l'adresse du routeur suivant
  - seul le routeur de sortie peut voir le message mais il ne sait pas d'où il vient

source:
http://www.cse.unr.edu/~mgunes/cpe401/cpe401sp11/student/tor.ppt

TOR : the oignon routers



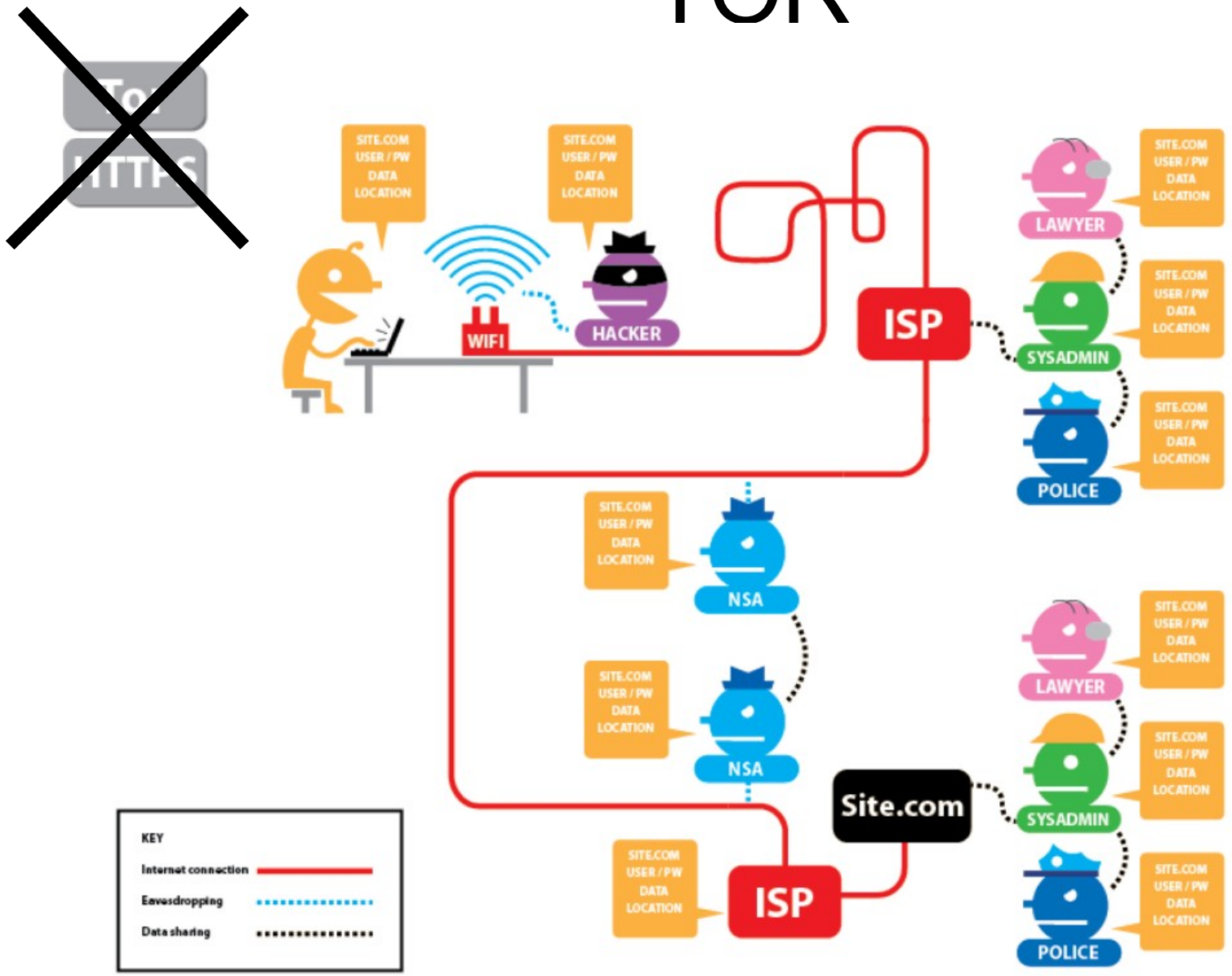


source des images :
http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2007/Bouillin-Morvan/internet_anonymat.ppt

Tor : sécurité

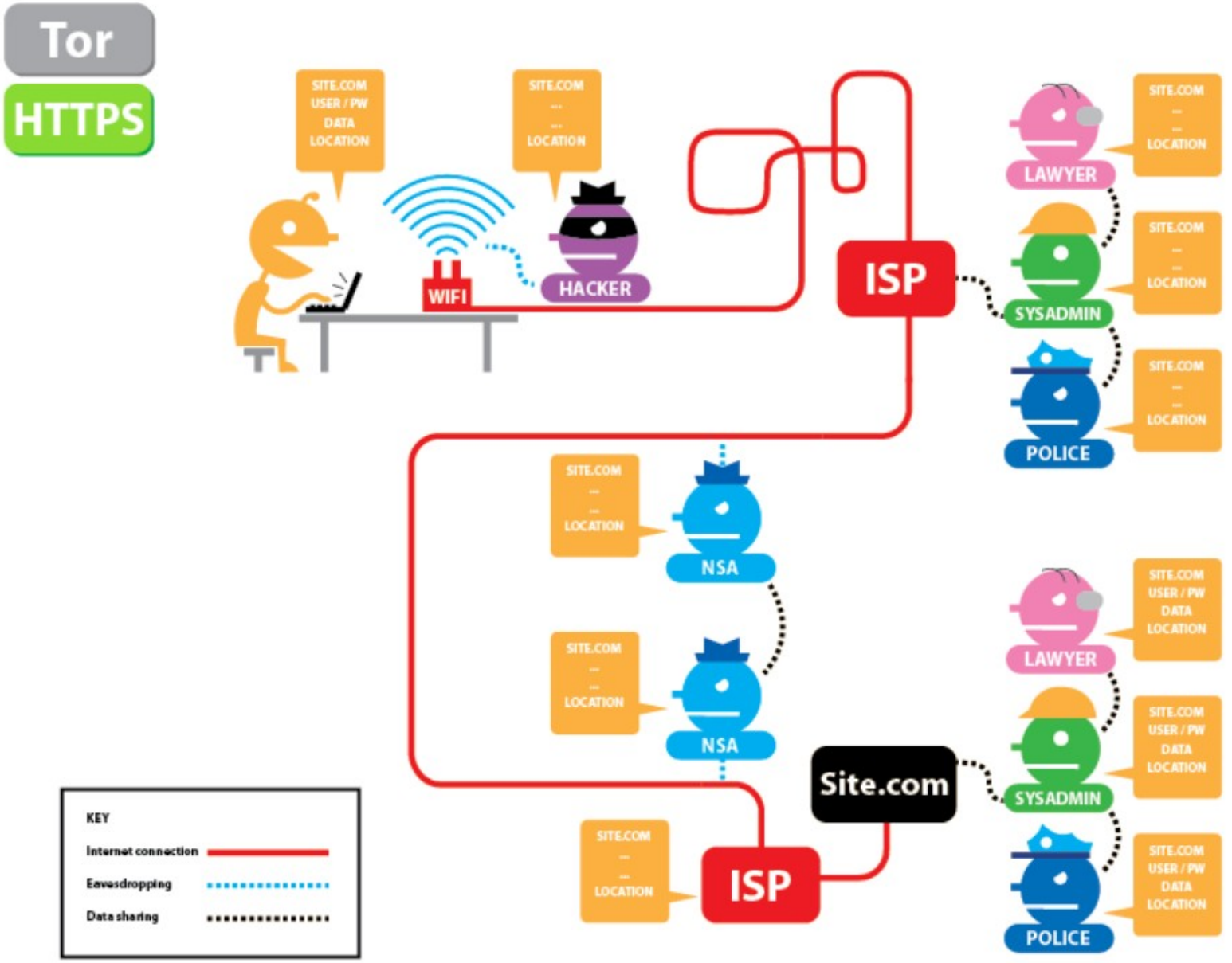
- votre ip source est cachée à la destination
- seul le routeur de sortie voit vos données
- la destination et la requête sont cachées entre vous et le premier routeur TOR
- ne protège pas si l'attaquant :
  - peut écouter le réseau en tout point
- MAIS
  - outils (navigateur) ou protocoles (ftp) envoient dans les requêtes beaucoup d'informations à votre insu (cf http://www.cnil.fr/vos-libertes/vos-traces et panopticlik https://panopticlick.eff.org/)
  - votre dns local peut connaître les sites consultés
- Solution :
  - privoxy : un proxy qui nettoie les requêtes WeB
  - Mon conseil : une clef bootable dédié : tails (cf tails.boum.org)

Espionnage sans HTTPS, sans TOR

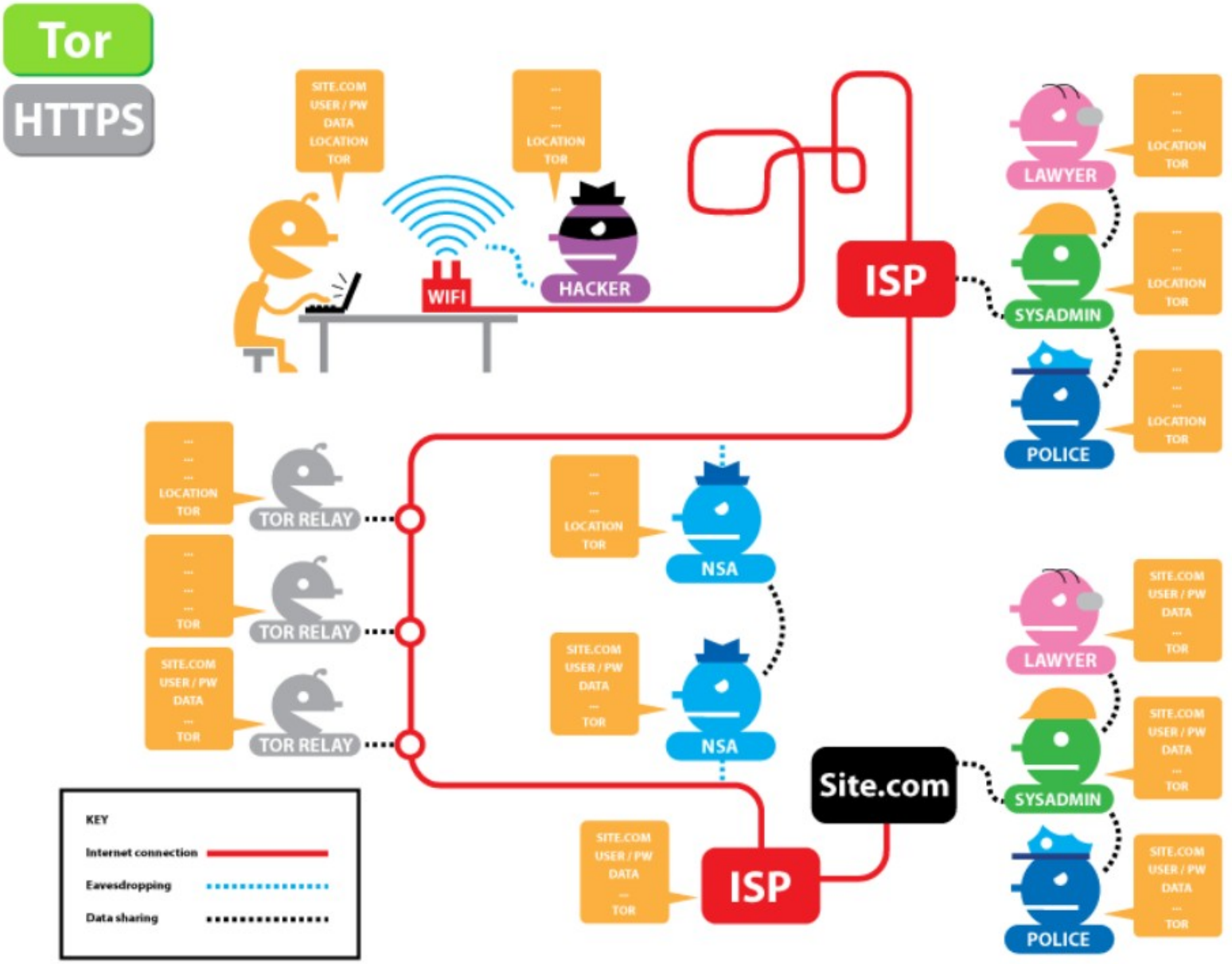
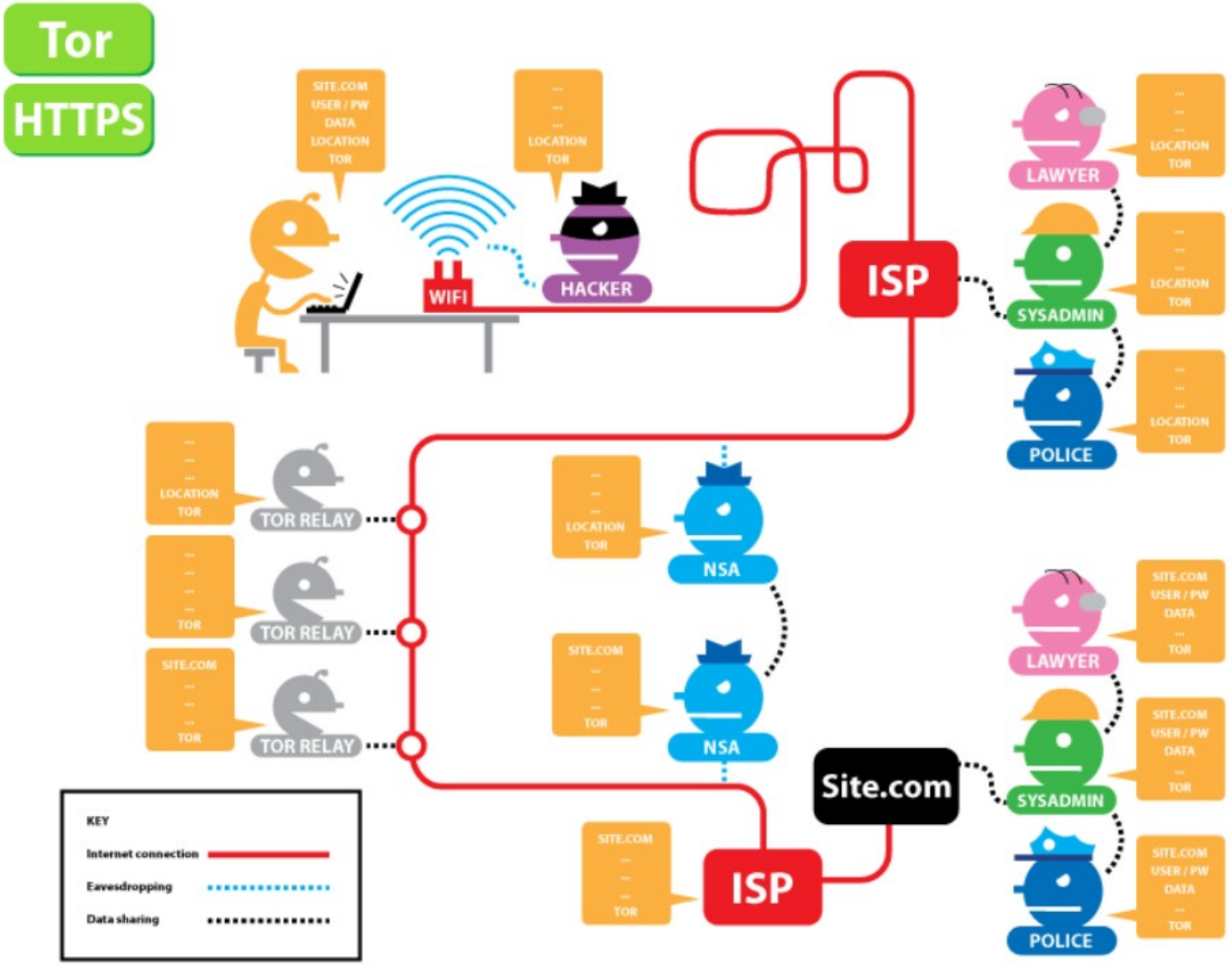


Source : https://www.eff.org/pages/tor-and-https

Espionnage avec HTTPS, sans TOR



Espionnage sans HTTPS, avec TOR



Espionnage avec HTTPS, avec TOR