Chiffrer les données

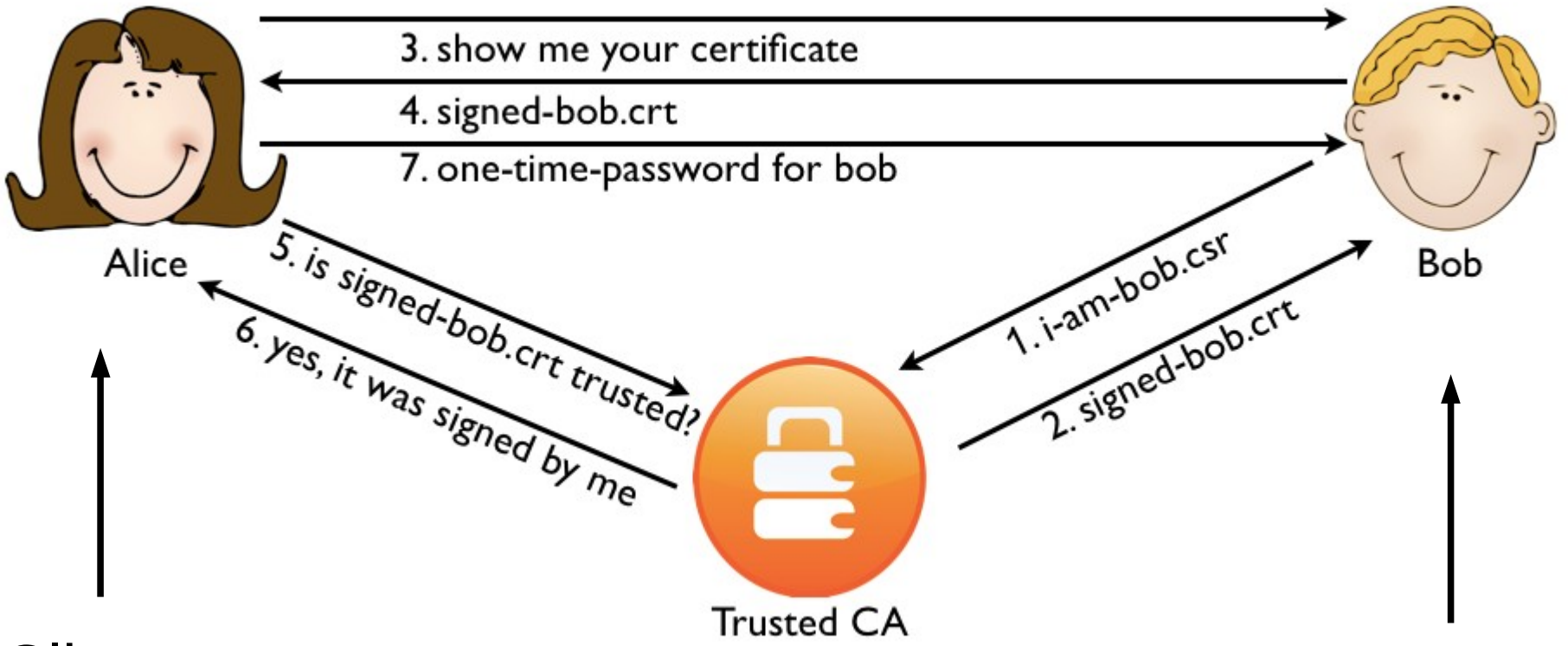
- Sur le réseau
  - Protocoles SSL, SSH, IPsec
- Sur les fichiers
- Sur les systèmes de fichiers

Secure Socket Layer SSL

HTTPS, SMTPS, LDAPS, POP3S, IMAPS,
VPN OpenVPN

- Authentification avec certificat numérique
  {clé publique, noms, localisation, …, signature}
- Confidentialité
  → il faut chiffrer les données
- Intégrité
  → utilisation de fonction de hachage

Secure Socket Layer SSL



Client

Serveur

Tiers de confiance

Secure Socket Layer SSL

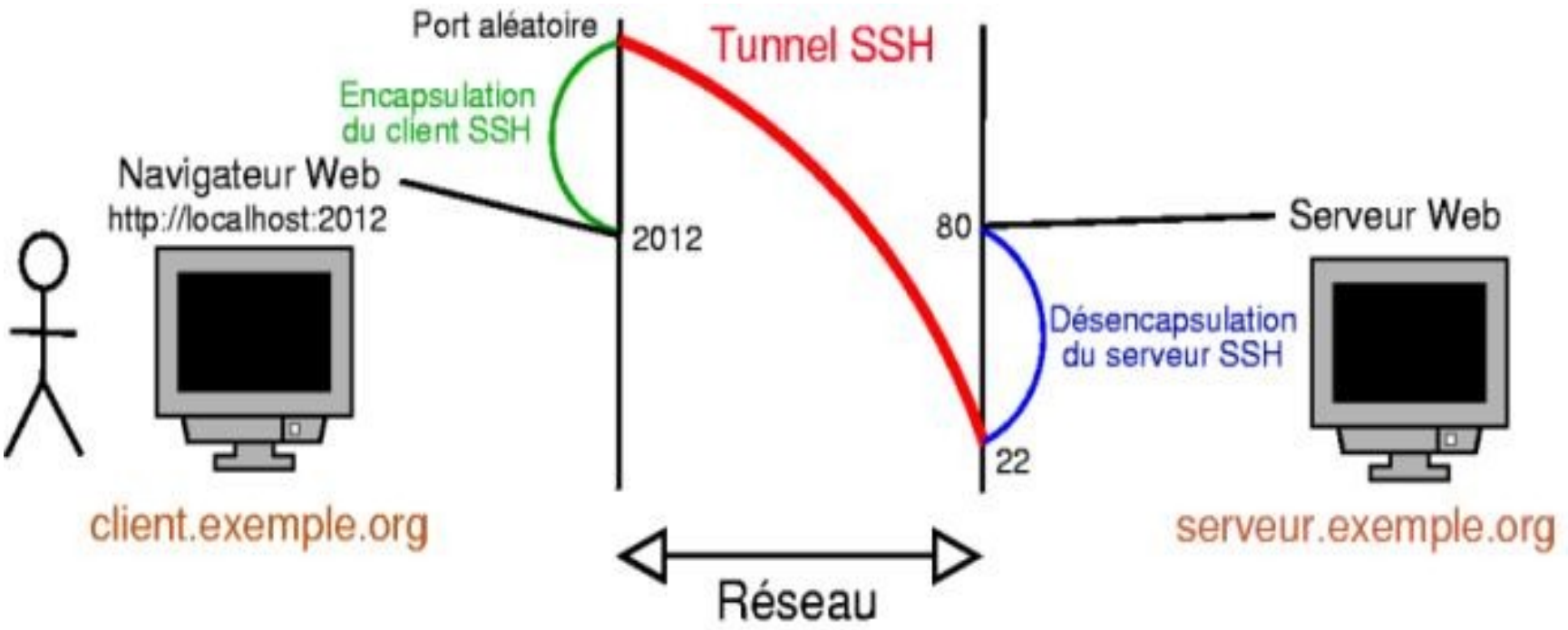
Protocole simplifié

1) Le client fait une demande de transaction sécurisée au serveur.
2) Le serveur envoie son certificat.
3) Le client vérifie que le certificat délivré est valide. Si la vérification est correcte alors le client envoie au serveur une clé symétrique chiffrée à l'aide de la clé publique du serveur qui sera donc le seul à pouvoir déchiffrer.
4) Cette clé sera utilisée pour échanger les données en toute sécurité.

Secure Shell : SSH

- Protocole de communication (utilise SSL)
- Programme qui utilise le protocole
- Cryptographie asymétrique puis symétrique
- Utilisations
  - Shell
  - Copie (scp), synchronisation (rsync) de fichiers
  - Tunnels
  - Monter un répertoire distant

Secure Shell : SSH



http://formation-debian.via.ecp.fr/ssh.html

IPsec

Internet Protocol Security

Niveau 3 du modèle OSI (couche réseau)

Utilisation de certificat

Traversée des NAT avec encapsulation

Lanceurs d'alerte

Anything to say?, une oeuvre de l'Italien Davide Dormino

PRISM

- Cible : des personnes vivant hors des États-Unis
- la NSA dispose d'un accès direct aux données hébergées par Google, Facebook, Apple, Microsoft, Yahoo, Skype, AOL…
- captation des métadonnées des appels téléphoniques aux États-Unis
- la NSA a développé de multiples méthodes de contournements des cryptages SSL

XKeyscore

- collecte quasi-systématique des activités de tout utilisateur
- 700 serveurs localisés dans des dizaines de pays
- 20 To / jours

- Données : 3 à 5 jours / Metadonnées : 30 jours
- Données intéressantes : 5 ans
- Chiffres 2013

Bullrun

- casser les systèmes de chiffrement
- Intervention sur les normes
- Intégration de portes dérobées
- Collaboration avec fournisseur de services
- Utilisation de superordinateur (force brute)
- Cyberattaques / espionnage (vol de clés)
- => le NIST : ~~Special Publication 800-90A~~
- => RSA Security : ~~B-SAFE~~

Sphère de sécurité : Safe Harbor

Un cadre juridique définit par le Département du commerce des États-Unis qui permet aux entreprises américaine de se conformer à la directive européenne sur la protection des données personnelles (2001).

Le 6 octobre 2015, la Cour de justice de l'Union européenne invalide l'accord Safe Harbor.

USA PATRIOT Act

Uniting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **Act** of 2001 (26 octobre)

Les services de sécurité américains peuvent accéder aux données à caractère personnel

Cela concerne les données hébergées

- sur le continent américain par n'importe quelle société
- par des sociétés de droit américain n'importe où

http://www.fincen.gov/statutes_regs/patriot/

Loi de programmation militaire LPM

pour les années 2014 à 2019

- Promulguée le 19/12/2013
- Article 20 : Pour les finalités énumérées à l'article L. 241-2, peut être autorisé **le recueil**, auprès des opérateurs de communications électroniques [...], des **informations** ou **documents** traités ou conservés par leurs réseaux ou services de communications électroniques, [...] au recensement de l'ensemble des **numéros d'abonnement** ou de **connexion** d'une personne désignée, à la **localisation** des équipements terminaux utilisés ainsi qu'aux communications d'un abonné [...]
- Décret d'application signé le 24 décembre 2014

Loi relative au renseignement

Promulguée le 24 juillet 2015

Installation de boite noire chez les opérateurs

Logiciels espions

IMSI-catchers

Large critique des organisations civiles

Confidentialité

Expliquer en quoi la réunion des trois conditions suivantes permet un bon niveau de confidentialité.

- Utiliser le chiffrement de bout en bout
- Utiliser un système décentralisé
- Utiliser les logiciels libres