Workshop Sciences Po

–

Protéger ses données

Benjamin Vialle
RSSI @CNIL
benjamin-vialle.net

Sciences Po, le 28 novembre 2016

Table des matières

Table des matières

Quelques mots . . .

. . .sur la CNIL

- Première autorité administrative indépendante créée par la loi du 6 janvier 1978.
- Ses missions : informer, réguler, protéger, contrôler, sanctionner, anticiper.
- « Droits informatique et libertés » : droit à la maîtrise, droit à l'information, droit d'accès, droit de rectification et de suppression, droit d'opposition, droit d'accès indirect .

La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Quelques mots . . .

. . .à propos de moi ⌣̈

- responsable de la sécurité des systèmes d'information de la CNIL ;
- ancien auditeur du service des contrôles de la CNIL ;
- ingénieur système et réseaux ;
- contributeur à l'éco-système du Logiciel Libre.

. . .sur l'objectif de l'atelier

- Protéger ses données et celles qui nous sont confiées.
- Communiquer et transmettre des données de manière sécurisée.
- Naviguer « de manière anonyme ».

Qu'est-ce qu'un Logiciel Libre ?

La définition de Wikipedia

Un logiciel libre est un logiciel dont l'utilisation, l'étude, la modification et la duplication en vue de sa diffusion sont permises, techniquement et légalement. Ceci afin de garantir certaines libertés induites, dont le contrôle du programme par l'utilisateur et la possibilité de partage entre individus.

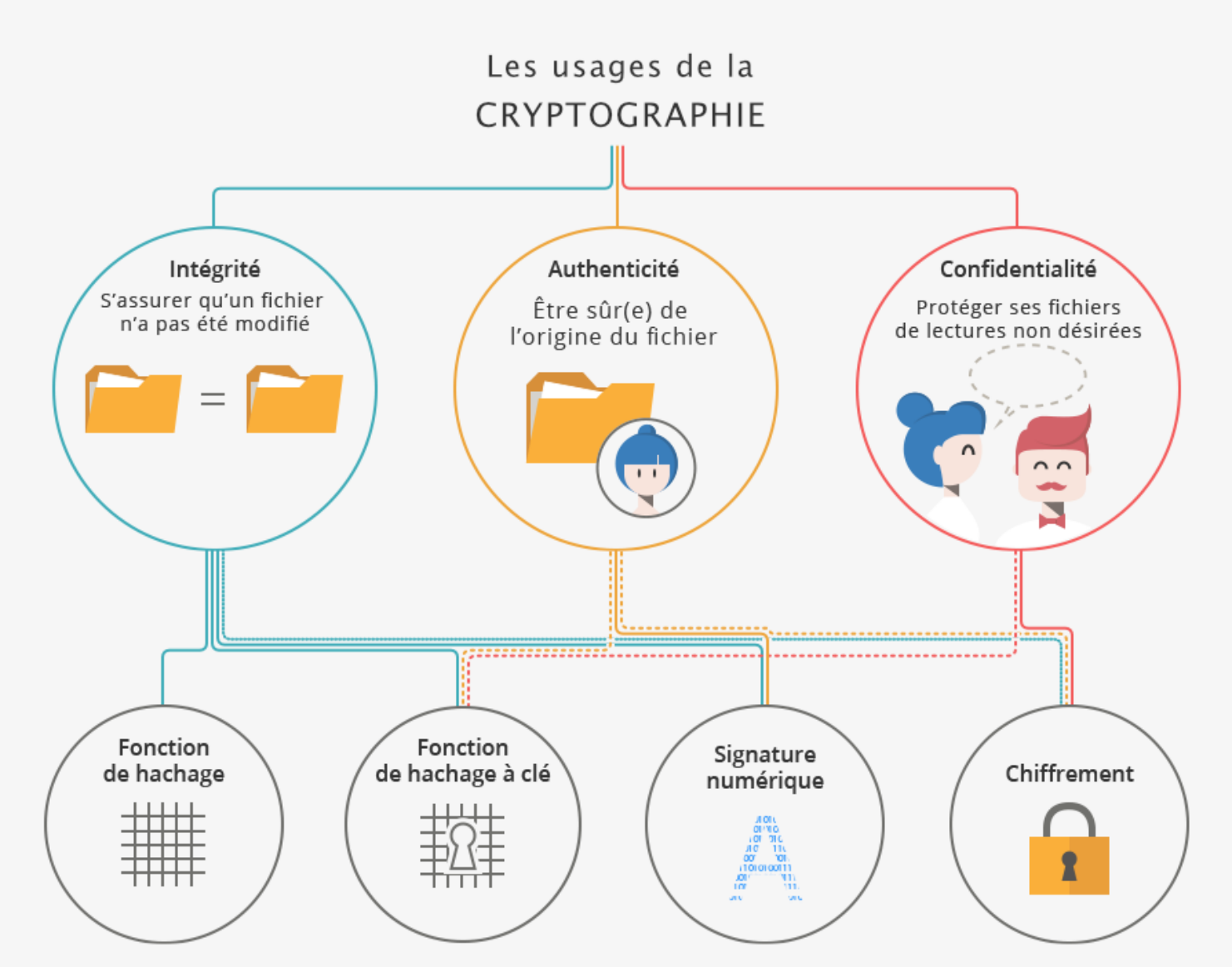
Qu'est-ce qu'un Logiciel Libre ?

la définition de la **Free Software Foundation**

Un Logiciel Libre doit conférer 4 libertés à son utilisateur :

- la liberté d'exécuter le programme, pour tous les usages ;
- la liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins ;
- la liberté de redistribuer des copies du programme (ce qui implique la possibilité aussi bien de donner que de vendre des copies) ;
- la liberté d'améliorer le programme et de distribuer ces améliorations au public, pour en faire profiter toute la communauté.

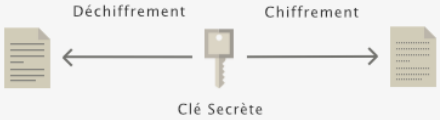
Grands principes de cryptologie et de chiffrement



Grands principes de cryptologie et de chiffrement

CONFIDENTIALITÉ

Comment fonctionne le CHIFFREMENT ?



CHIFFREMENT SYMÉTRIQUE

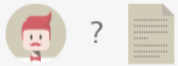
Le chiffrement symétrique permet de chiffrer et déchiffrer un fichier avec la même clé, dite secrète. Pour s'échanger un message il faut donc que les deux parties partagent la même clé.

MISE EN PRATIQUE

Alice vient d'enregistrer la liste des cadeaux de Noël de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accèder.

1. Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.

2. Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.



3. Malheureusement pour lui, Bob est incapable de lire la liste car il ne possède pas la clé secrète.

4. La liste est donc bien protégée. Seule Alice peut réussir à la déchiffrer et la lire !

CHIFFREMENT ASYMÉTRIQUE

Le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée.

La clé publique, accessible à tous, est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers, celle-ci étant connue que d'un seul individu.

MISE EN PRATIQUE

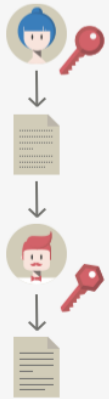
Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1. Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.

2. Elle l'envoie à Bob.

3. Bob reçoit le document et le déchiffre à l'aide de sa clé privée.

4. Une fois le document déchiffré, il rédige un article puis le publie dans son journal.



Grands principes de cryptologie et de chiffrement

AUTHENTICITÉ

Comment fonctionnent les SIGNATURES NUMÉRIQUES ?

SIGNATURE NUMÉRIQUE

Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

Le procédé repose sur un couple de clés : l'une est privée et connue uniquement de son détenteur, l'autre est publique et accessible à tous.

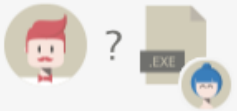
La signature est générée en utilisant la clé privée. La clé publique est utilisée pour vérifier cette signature. Cette vérification peut donc être effectuée par n'importe quelle personne ayant accès à la clé publique.

MISE EN PRATIQUE

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

1. Avant de publier librement son logiciel, Alice prend soin de le signer.

2. Bob vient de télécharger une copie du logiciel mais il veut s'assurer que cette copie provient bien d'Alice.



3. Bob utilise la clé publique d'Alice pour vérifier la signature de la copie.

4. Si la clé reconnait la signature, alors c'est une bonne copie !
Dans le cas contraire, Bob préfère ne pas prendre de risques. Il supprimera la copie.

Grands principes de cryptologie et de chiffrement

Pour en savoir plus

- Le site de la CNIL :

  `https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement`

- Le webdoc' de l'ANSSI

  `https://www.ssi.gouv.fr/actualite/crypto-le-webdoc/`

- le guide d'autodéfense numérique et son chapitre sur la cryptographie :

  `http://guide.boum.org/tomes/1_hors_connexions/1_comprendre/5_crypto_symetrique_et_hash/`

De l'intérêt de maîtriser les outils de cryptographie

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.
Edward Snowden, answering questions live on the Guardian's website [a]

a. http ://www.guardian.co.uk/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

De l'intérêt de maîtriser les outils de cryptographie

From : anon108@[redacted]
To : Micah Lee Date : Fri, 11 Jan 2013
Micah,
I'm a friend. I need to get information securely to Laura Poitras and her alone, but I can't find an email/gpg key for her.
Can you help ?

Message d'Edward Snowden à Micah Lee, journalist à **The Intercept** [a].

a. https://theintercept.com/2014/10/28/smuggling-snowden-secrets/

Table des matières

De l'intérêt de maîtriser les outils de cryptographie

Extrait du générique du film de Laura Poitras : CitizenFour

Disclaimer : il existe d'autres outils de chiffrement

Des outils pour mettre en œuvre des algorithmes

Il n'existe pas qu'un seul logiciel pour chiffrer ses données.
Ce qu'il est important de vérifier :

- La licence du logiciel : est-ce un Logiciel Libre ? Ai-je accès au code source ?
- Possibilité d'utiliser des algorithmes de chiffrement reconnus comme robustes avec des tailles de clefs suffisantes.
- L'environnement dans lequel j'utilise le logiciel est-il de confiance ?

Utilisation de Veracrypt

Pourquoi Veracrypt et pas Truecrypt ?

- VeraCrypt est un fork qui a été initialement publié le 22 juin 2013 pour faire suite au projet TrueCrypt interrompu subitement [a].
- Reprend le code ouvert de Truecrypt et l'améliore (correction de bugs, évolutions des algorithmes de chiffrement).
- Veracrypt a été audité par la société française QuarksLab à la demande de l'OSTIF (The Open Source Technology Improvement Fund) [b].

Récupérer Veracrypt : `https://veracrypt.codeplex.com/`

a. Selon les développeurs de Truecrypt, des interrogations sur la vérification du code initial de TrueCrypt ont été soulevées à la suite d'améliorations de sécurité mises en œuvre dans sa dernière version.

b. Les résultats de l'audit sont disponibles en ligne sur `https://ostif.org/the-veracrypt-audit-results/`

Utilisation de Veracrypt

Fonctionnalités de Veracrypt

- chiffrement de volume ;
- chiffrement de disques durs ou de partitions ;
- fonctionnalité de « déni plausible » [a] avec les containers cachés.

a. Le déni plausible est la possibilité pour une personne soupçonnée d'utiliser un logiciel de chiffrement de nier de manière tout à fait plausible l'existence d'un fichier chiffré créé par ce logiciel.

Utilisation de Veracrypt

À vous de jouer

Ce dont vous avez besoin :

- un ordinateur fonctionnant avec les systèmes d'exploitation Microsoft Windows, Mac OS X ou GNU/Linux ;
- le logiciel VeraCrypt ;
- une clef USB.

Utilisation de Veracrypt

Points d'attention

Lorsque vous utilisez VeraCrypt, pensez à :

- Choisir un mot de passe robuste : toute la sécurité de votre container chiffré repose sur ce mot de passe.
- Si vous décider de chiffrer l'intégralité de votre disque dur avec VeraCrypt, pensez à faire une sauvegarde (chiffrée) de vos données avant !
- En cas de transmission du mot de passe, faites le par un **autre canal** que celui par lequel vous avez transmis le container.

Table des matières

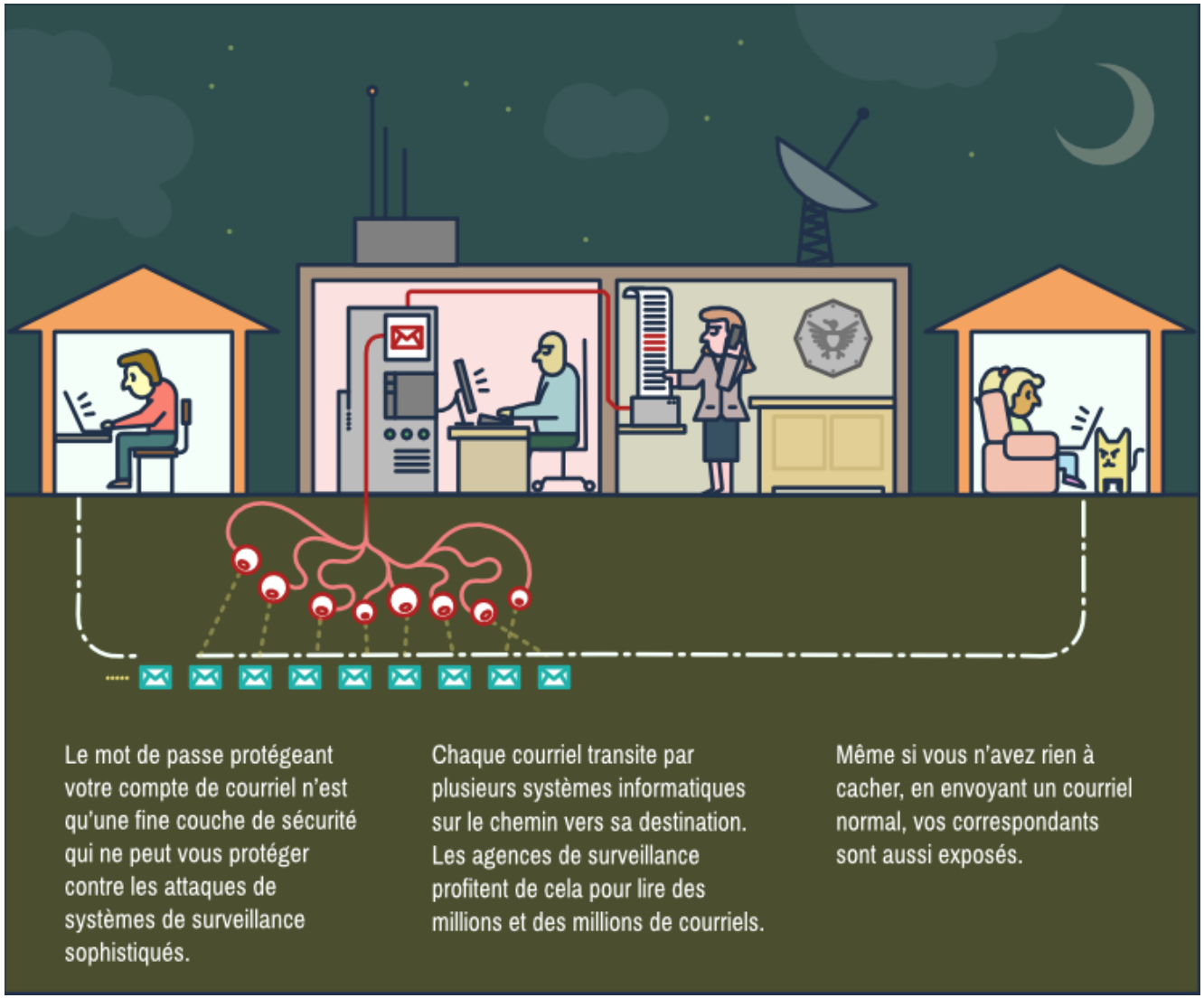
Chiffrement des courriels

Utilisation du chiffrement asymétrique pour garantir la confidentialité des échanges

Le chiffrement asymétrique est plus pratique dans le cas de la messagerie :

- Pas besoin de transmettre la clef de déchiffrement par un autre canal.
- Ajoute une chaîne de confiance et l'authenticité des échanges.

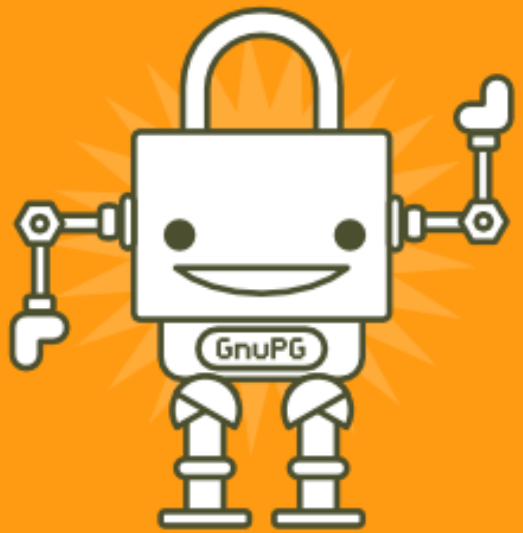
Le principe


Le mot de passe protégeant votre compte de courriel n'est qu'une fine couche de sécurité qui ne peut vous protéger contre les attaques de systèmes de surveillance sophistiqués.
Chaque courriel transite par plusieurs systèmes informatiques sur le chemin vers sa destination. Les agences de surveillance profitent de cela pour lire des millions et des millions de courriels.
Même si vous n'avez rien à cacher, en envoyant un courriel normal, vos correspondants sont aussi exposés.

Le principe

Récupérez votre vie privée avec GnuPG !

Tout ce dont vous avez besoin est un simple programme appelé **GnuPG**.
Il chiffre votre courriel en un code que seul le destinataire peut lire.



GnuPG fonctionne sur presque tous les ordinateurs et smartphones. Il est sous licence libre, et ne coûte rien. Chaque utilisateur possède une paire unique **clef publique - clef privée.** Ces clefs sont des suites de nombres aléatoires.

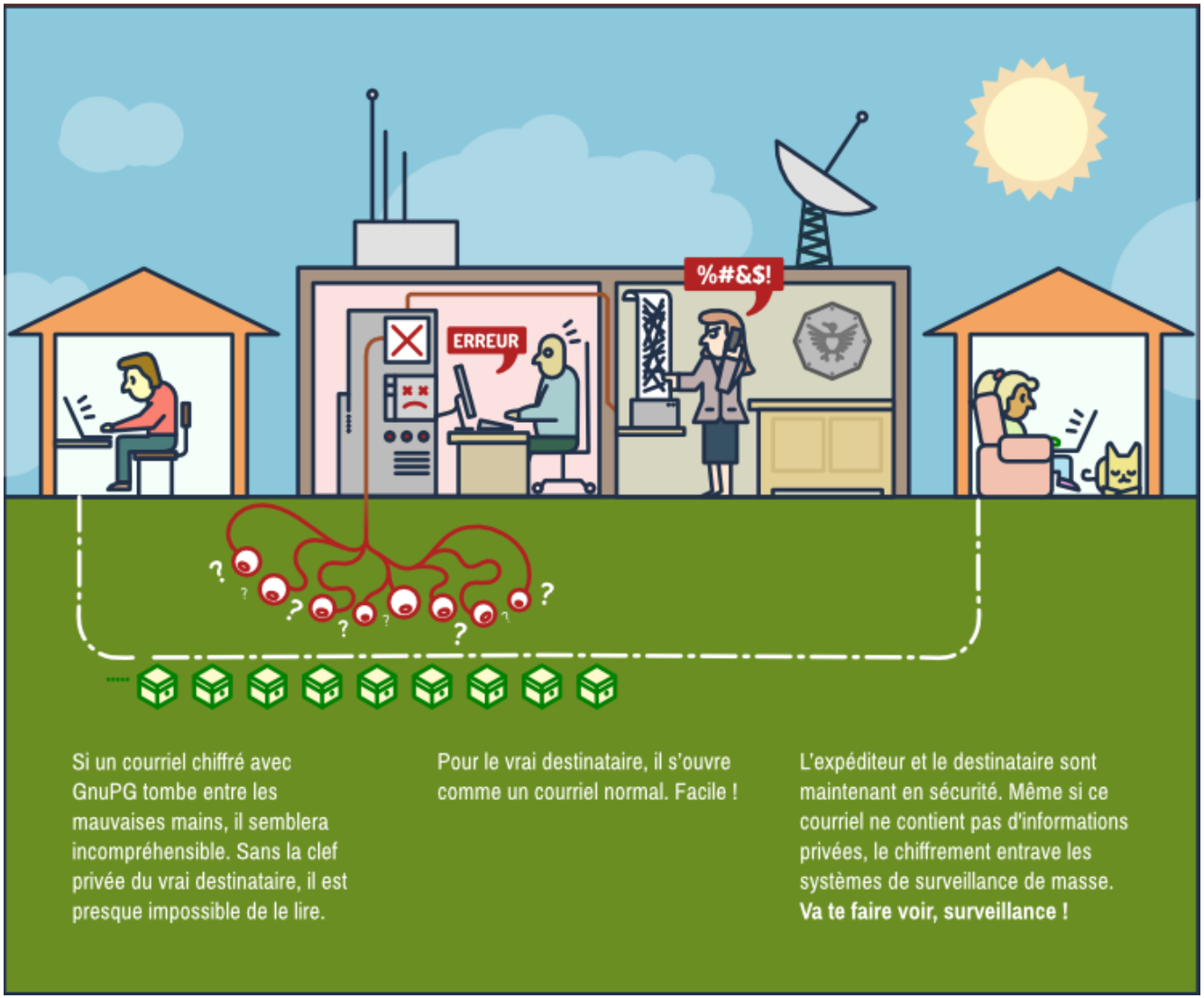
Le principe


PUBLIQUE
VOTRE CLEF PUBLIQUE
Votre clef publique n'est pas comme une clef physique, parce que vous la partagez. Elle est stockée sur un serveur en ligne, où chacun peut la rechercher et la télécharger.
Cette clef est utilisée, avec GnuPG, pour chiffrer les courriels qui vous seront envoyés.
PUB

Le principe


PRIVÉE
VOTRE CLEF PRIVÉE
Votre clef privée ressemble plus à une clef physique, car vous la conservez avec vous (sur votre ordinateur).
À l'aide de GnuPG et de votre clef privée, vous pouvez décoder les courriels chiffrés qui vous sont envoyés.
PRIV

Le principe


%#&$!
ERREUR
Si un courriel chiffré avec GnuPG tombe entre les mauvaises mains, il semblera incompréhensible. Sans la clef privée du vrai destinataire, il est presque impossible de le lire.
Pour le vrai destinataire, il s'ouvre comme un courriel normal. Facile !
L'expéditeur et le destinataire sont maintenant en sécurité. Même si ce courriel ne contient pas d'informations privées, le chiffrement entrave les systèmes de surveillance de masse.
Va te faire voir, surveillance !

Le principe


GnuPG est un **logiciel sous licence libre** ; Il est totalement transparent et tout le monde peut le copier ou faire sa propre version. Cela le rend plus sûr vis-à-vis de la surveillance qu'un logiciel privateur (comme Windows ou Word). Plus d'infos sur **FSF.org**.
Pour nous protéger de la surveillance, nous devons apprendre à utiliser GnuPG et **échanger nos clefs publiques** en même temps que nos adresses de courriel.
Des milliers de personnes utilisent déjà GnuPG, des activistes, des journalistes, des lanceurs d'alertes ou des gens de tous les jours. Chaque personne l'utilisant renforce notre communauté, et montre aux agences de surveillance que nous sommes prêts pour la riposte.
Apprenez l'autodéfense courriel. Abordez GnuPG en 30 minutes sur
EmailSelfDefense.FSF.org/fr
Copyright 2014 Free Software Foundation.
Remix encouragé ! Prenez la source à l'URL ci-dessus.
Conception de l'infographie et du guide par **Journalism++** - Traduction par **Framasoft**

Mise en œuvre

Pré-requis :

Microsoft Windows

- client de messagerie Mozilla Thunderbird ;
- GPG4Win ;
- plugin Enigmail pour Mozilla Thunderbird.

MacOS et GNU/Linux

- client de messagerie Mozilla Thunderbird ;
- GPG s'il n'est pas installé par défaut ;
- plugin Enigmail pour Mozilla Thunderbird.

Mozilla Thunderbird :
`https://www.mozilla.org/fr/thunderbird/`
GnuPG : `https://gnupg.org/download/index.html`
Enigmail :
`https://www.enigmail.net/index.php/en/download`

Étape 1 – Rassemblez les outils

Étape 1 – Rassemblez les outils

1.A Configurez votre logiciel de messagerie avec votre compte de courriel.

1.B Le cas échéant, installez GnuPG.

1.C Installez le module Enigmail pour votre programme de messagerie.

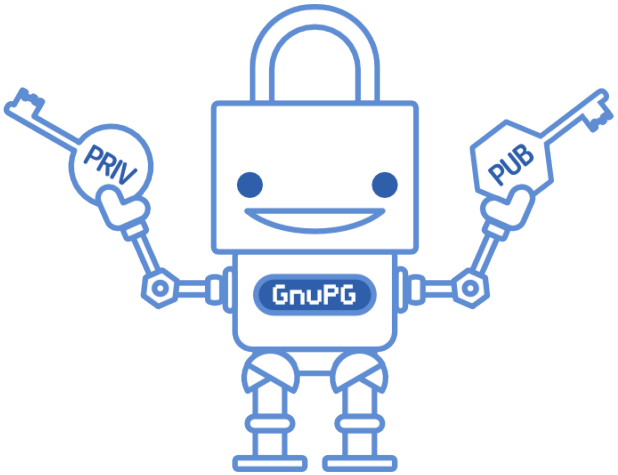
Étape 2 – Fabriquez vos clefs

Étape 2 – Fabriquez vos clefs

2.A Créez une paire de clefs.

2.B Partagez votre clef publique.

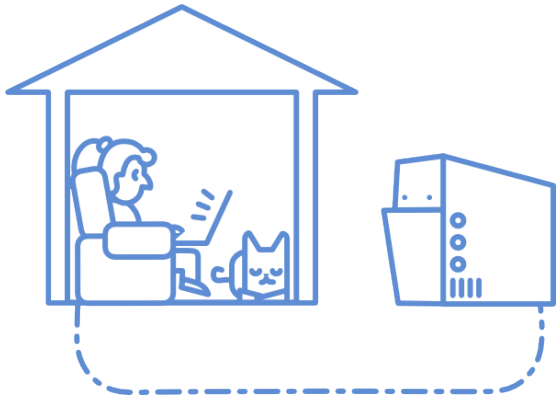
2.C Envoyez votre clef publique sur un serveur de clefs.



Étape 3 – Essayez !

Étape 3 – Essayez !

- 3.A Envoyez votre clef publique à votre destinataire.
- 3.B Envoyez un courriel de test chiffré.
- 3.C Recevez une réponse.
- 3.D Envoyez un courriel de test signé.
- 3.E Recevez une réponse.



Écrivez à Edward, il vous répondra !

Envoyez votre clef publique par courriel à Edward `edward-en@fsf.org` ou `edward-fr@fsf.org` et vous pourrez discuter avec lui !

Utilisation de GnuPG

Points d'attention

Lorsque vous chiffrez vos courriels avec OpenPGP, pensez :

- à protéger votre clef privée. La confidentialité de vos échanges et l'authenticité de vos messages repose sur votre clef privée ;
- à choisir un mot de passe robuste : la sécurité de votre clef privée repose sur ce mot de passe ;
- à l'objet du message qui n'est pas chiffré ;
- que l'adresse du destinataire n'est pas chiffrée : on connaît l'existence d'échanges entre vous et votre destinataire (mais pas le contenu).

Utilisation de GnuPG

Pour aller plus loin

Découvrez la ≪ toile de confiance ≫

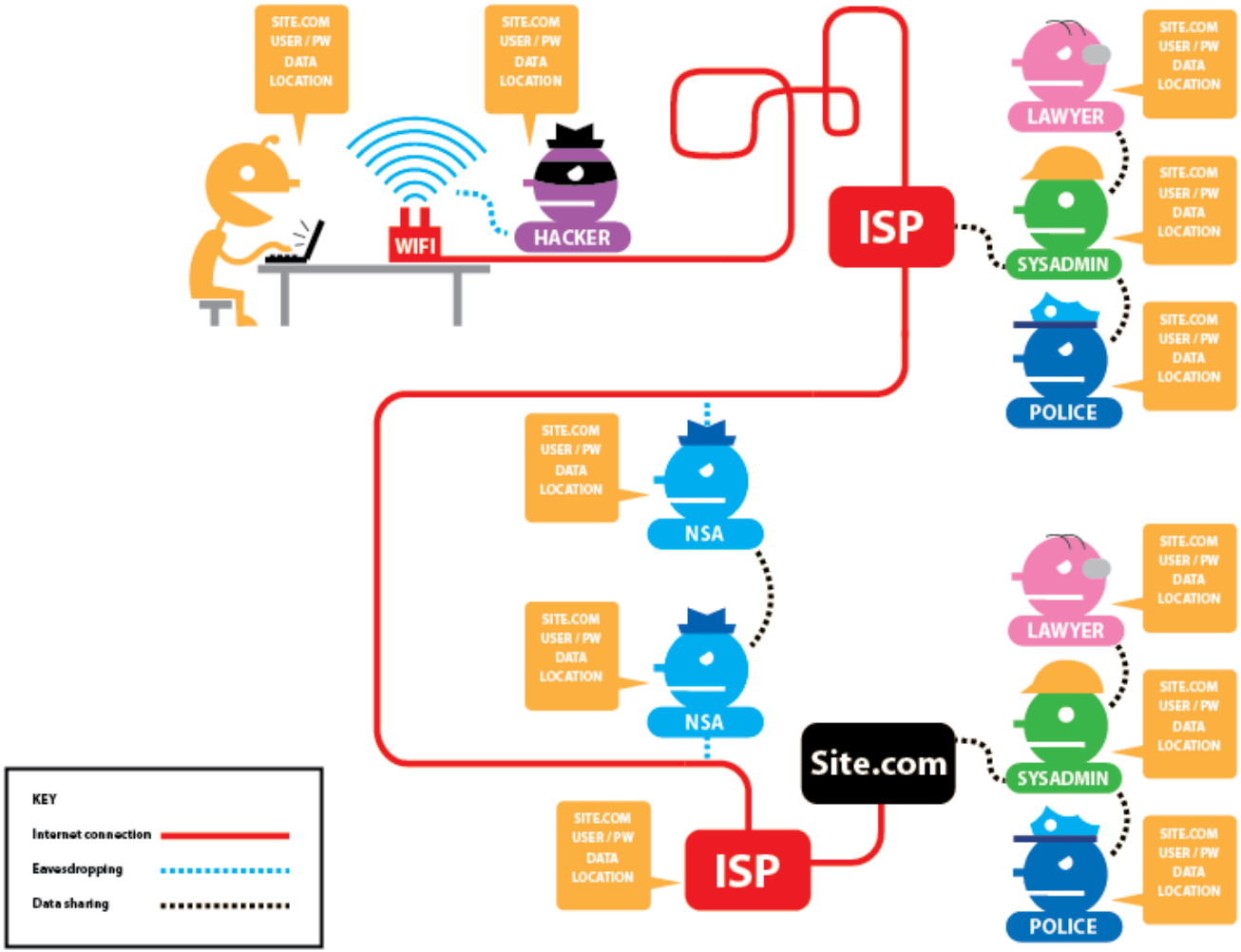
- Signez une clef

Les bonnes pratiques :

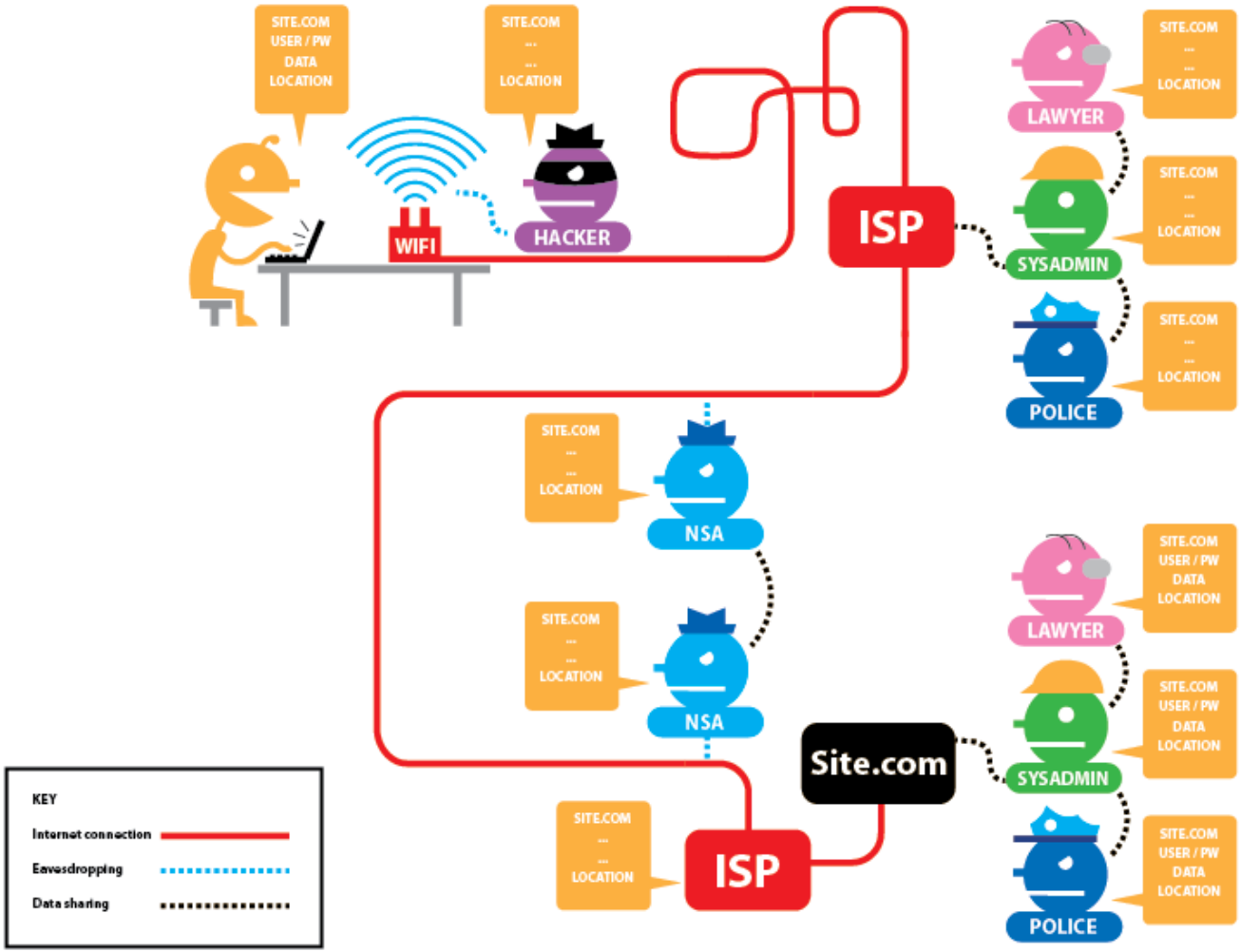
- Quand dois-je chiffrer ? Quand dois-je signer ?
- Soyez attentifs aux clefs non valides.
- Sauvegardez votre certificat de révocation en lieu sûr.
- Agissez rapidement si quelqu'un s'empare de votre clef privée.
- GnuPG et le webmail.

Table des matières

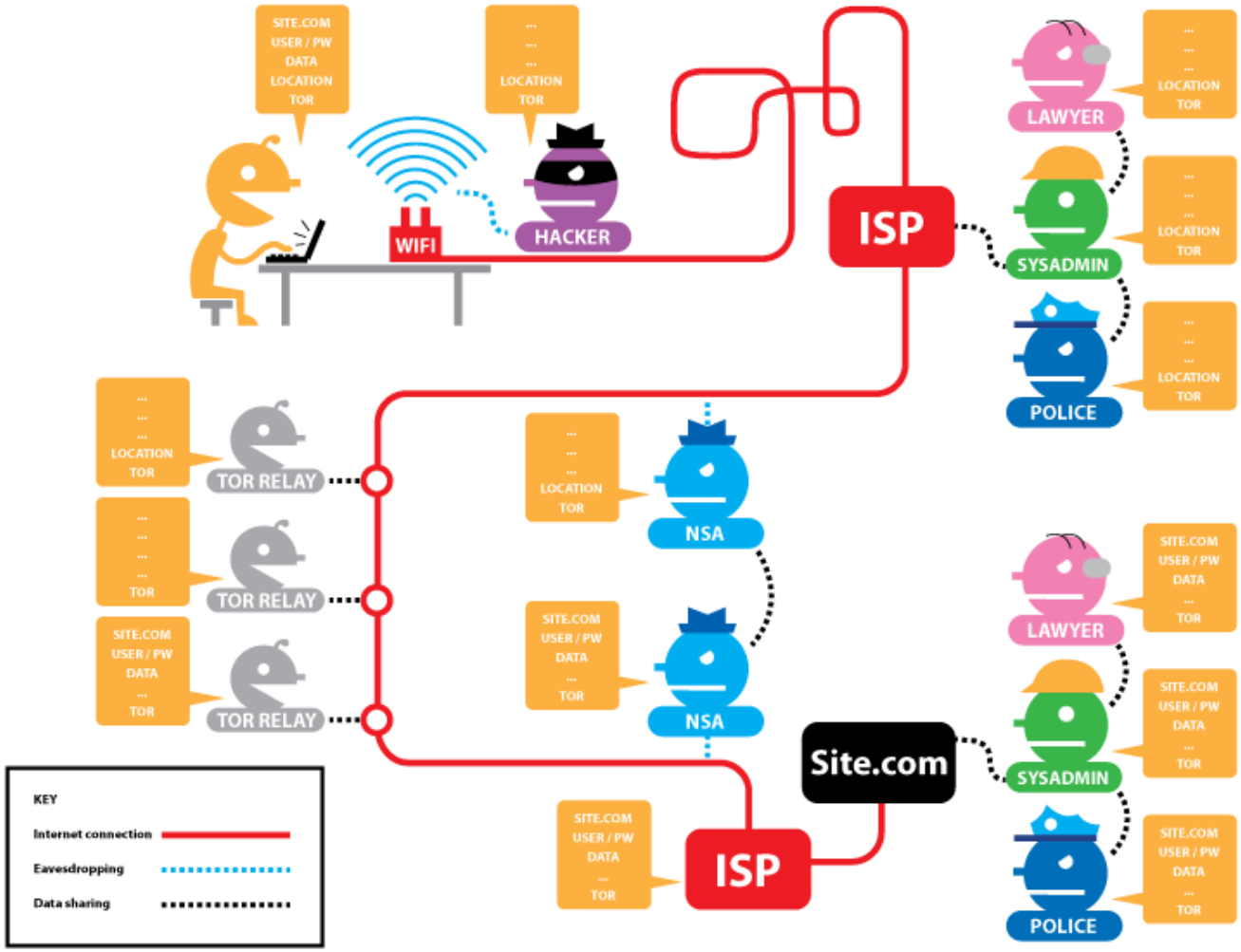
Navigation sans TOR ni HTTPS



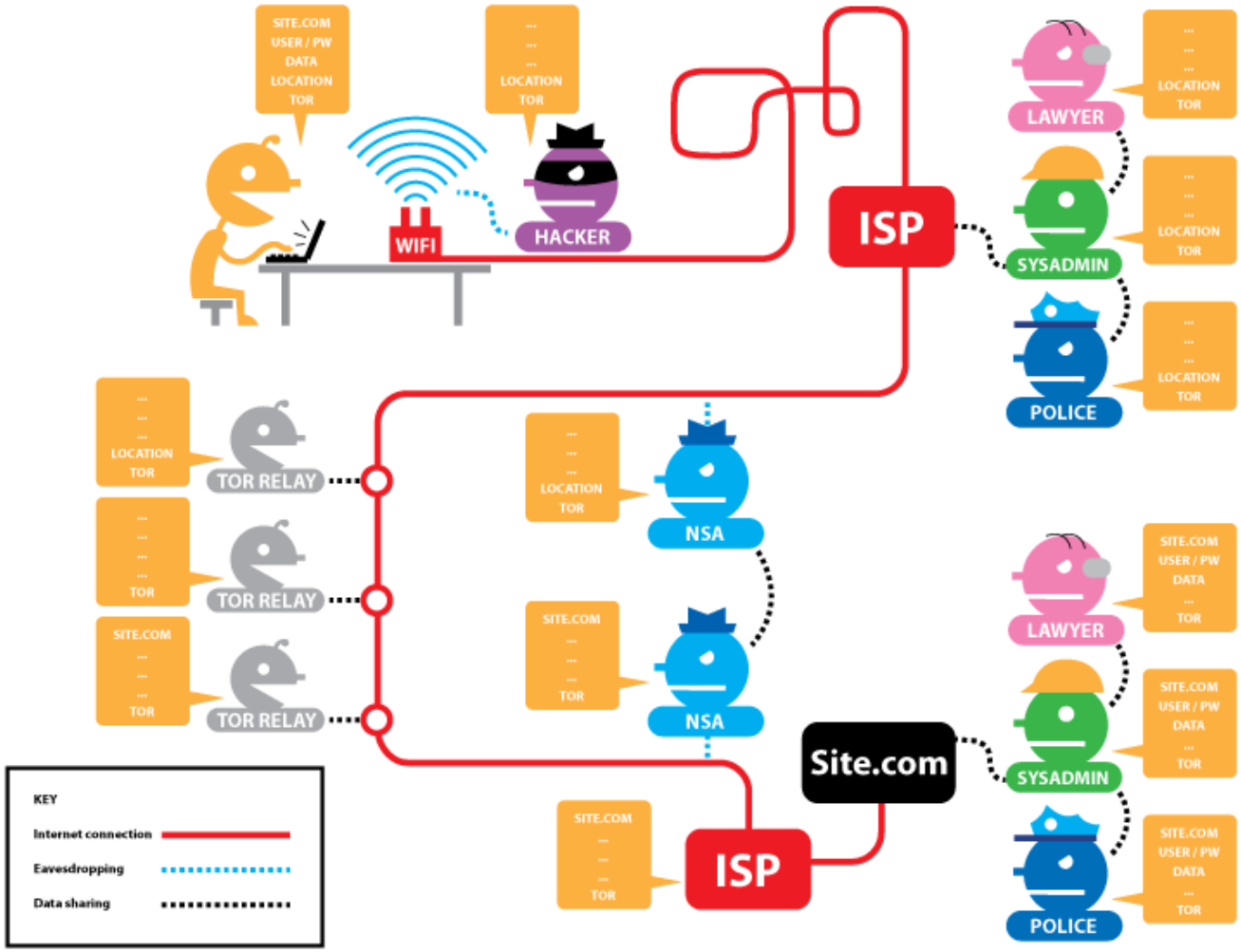
Navigation sans TOR et en HTTPS



Navigation avec TOR sans HTTPS



Navigation avec TOR et en HTTPS

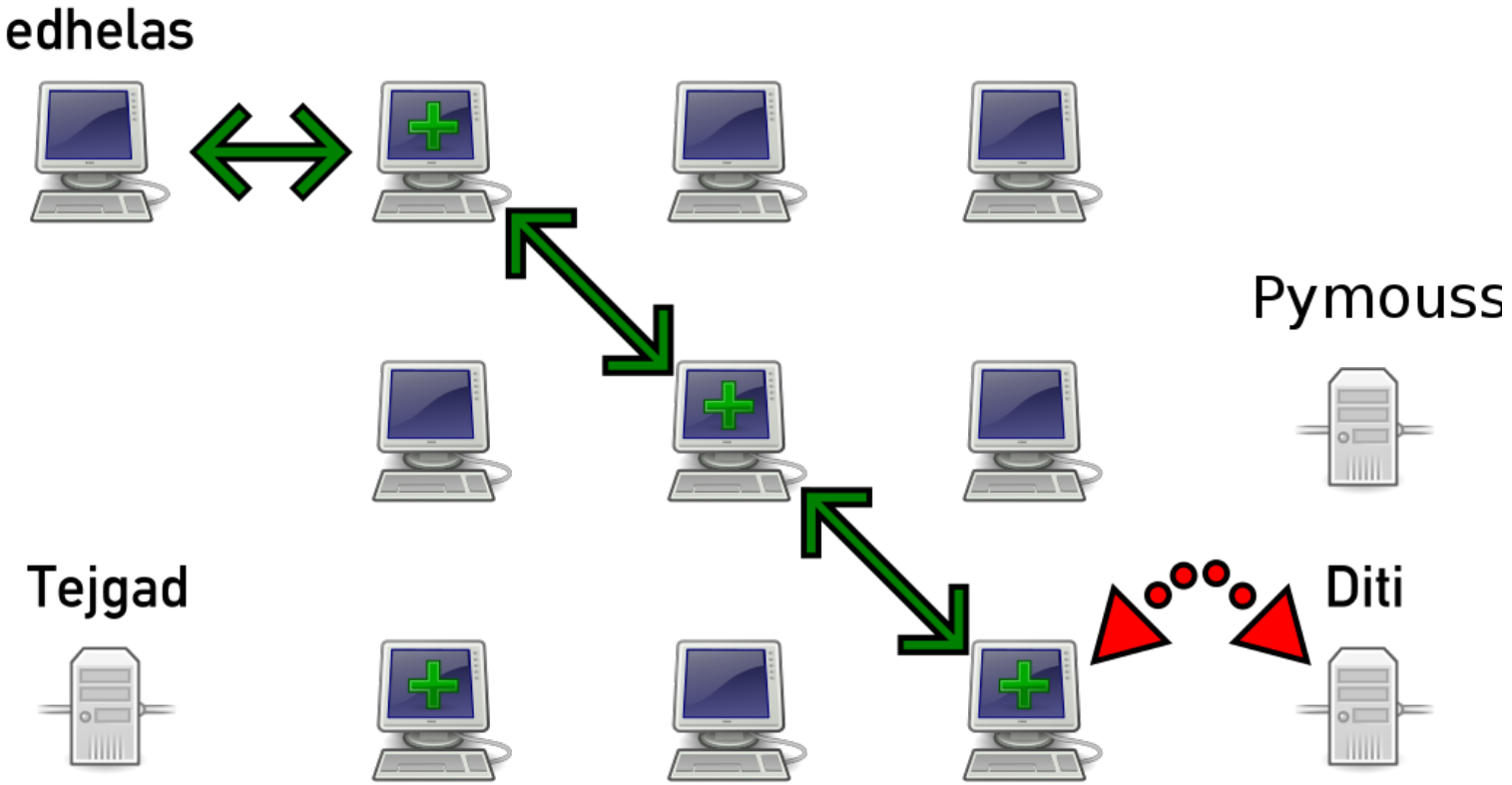


Principe de fonctionnement du réseau Tor

Principe de fonctionnement du réseau Tor

- Tor est un réseau informatique superposé mondial et décentralisé.
- Il se compose d'un certain nombre de serveurs, appelés nœuds du réseau et dont la liste est publique.
- Ce réseau permet d'anonymiser l'origine de connexions TCP.
- le projet Tor développe également un navigateur Web basé sur Firefox, Tor Browser, ainsi que d'autres applications spécialement modifiées pour préserver l'anonymat de leurs usagers.
- L'implémentation de référence du protocole s'appelle tor, c'est un logiciel libre sous licence BSD révisée.

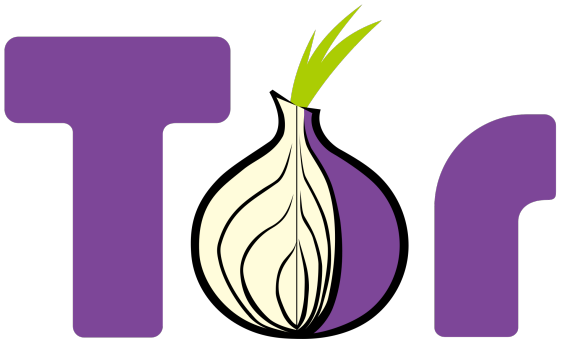
Principe de fonctionnement du réseau Tor



Installation de Tor browser

Tor Browser

Après téléchargement et décompression de Tor Browser, il suffit de lancer Tor Browser pour se voir connecté au réseau Tor



Où récupérer Tor browser ?

Téléchargement de Tor browser à partir du site officiel du projet tor `https://www.torproject.org`

Table des matières

Quelques liens pour aller plus loin

https://controle-tes-donnees.net

- Ne laissez plus de traces sur Internet
  - utilisez et configurez un navigateur libre : Firefox ;
  - utilisez un moteur de recherche qui ne vous surveille pas ;
  - maîtrisez les traces que vous laissez en améliorant Firefox ;
  - naviguez en ne laissant aucune trace avec Tor.
- Gardez vos échanges confidentiels :
  - chiffrez vos discussions instantanées et appels vidéo avec Jitsi ;
  - choisissez un fournisseur d'email qui vous laisse le contrôle.
- Reprenez la main sur tous vos outils :
  - reprenez le contrôle de votre ordinateur avec GNU/Linux.
- maîtrisez toutes vos données en les hébergeant vous-même :
  - facilement, sur un NAS ;
  - sur un PC ou un raspberry, avec un OS dédié ;
  - sur un PC, avec un GNU/Linux paramétré par vos soins.

Quelques liens pour aller plus loin

https://emailselfdefense.fsf.org/fr/

5 étapes pour sécuriser ses échanges par courrier électronique

1. rassemblez les outils ;
2. fabriquez vos clefs ;
3. essayez ;
4. découvrez la toile de confiance ;
5. les bonnes pratiques.

Conclusion

Merci ☺

CNIL.

Des questions ?