Mémo : des solutions pour protéger sa vie privée et ses communications

Données personnelles

- Fournisseur de service local : Grésille, cf. `https://www.gresille.org/services/`
- Autres : riseup (USA), autistici (Italie), cf. « chatons » de Framasoft
- Autohébergement facilité : Yunohost & **La brique Internet** `http://labriqueinter.net`
- Liste de logiciels pour l'autohébergement :
  - Calendriers et contacts : davical, radicale, baikal
  - Messagerie instantanée : prosody, ejabberd, openfire
  - Serveurs de mail : postfix, exim, opensmtpd, dovecot, cyrus
  - Webmail : Roundcube, mailpile
  - Partage de fichiers et « cloud » : owncloud, seafile, jyraphe, dropcenter, coquelicot
  - Sauvegardes : unison, backupninja, attic-backup, duplicity
  - Site Web, blog : wordpress, drupal, pluxml
  - Travail collaboratif :
    - Wikis : dokuwiki, yeswiki
    - Pads : etherpad-lite, pastebin, gobby (sur réseau local)
    - cf. `https://www.gresille.org/publications/edition_collaborative/`
- Différentes machines pour l'autohébergement : raspberrypi, olimex LIME et LIME2, cubox, cubieboard, bananapi, pine64, fitpc…

Communications

- FAI associatif local : Rézine (ou d'autres de la FFDN : `http://db.ffdn.org`)
  - Tunnels chiffrés (VPN) et **brique Internet**
  - Accès radio
  - Accès DSL
- Navigateurs Web : Firefox, Chromium, torbrowser.
  - Https everywhere (passage en https dès que possible)
  - uBlock Origin (blocage de publicités)
  - Privacy Badger (blocage de mouchards)
  - Adguard (détection et blocage de mouchards, trackers, phishing, balises FB/Google, systèmes d'analyse (google analytics)…), équivalent de Ghostery qui n'est pas libre
  - cf. `https://www.gresille.org/publications/firefox/`
- Pour sécuriser ses communications :
  - Monter des tunnels chiffrés (OpenVPN, ssh, IPSec)
  - Chiffrement de bout en bout : https pour le web, OpenPGP (gpg) pour les mails et OTR (gpg) intégré aux clients IRC ou Jabber
  - Anonymisation : Tor

Sur sa machine

- Essayer d'avoir du matériel libre
- Passer à un système libre : GNU/Linux ou *BSD (éthique, confiance, communauté et continuité…), la Guilde (`http://www.guilde.asso.fr`) ou Démo-Tic (`http://www.demo-tic.org/`) peuvent aider
- Gérer ses mots de passe et les chiffrer : keepassx + passifox (module pour firefox qui interroge keepassx pour s'authentifier sur des sites web facilement) ou pass + PassFF (module pour firefox)
- Chiffrer son disque dur : cryptsetup
- Clients mails : Thunderbird / claws / …
- Client pour gérer des abonnements (syndication, rss, atom) : Firefox avec ou sans extension (genre Brief), Liferea, Thunderbird
- Messagerie instantanée (jabber et/ou irc) : pidgin, xchat, psi, Thunderbird
- Tails : une distribution libre qui efface toute trace sur la machine et utilise Tor

Mémo : des solutions pour protéger sa vie privée et ses communications

Données personnelles

- Fournisseur de service local : Grésille, cf. `https://www.gresille.org/services/`
- Autres : riseup (USA), autistici (Italie), cf. « chatons » de Framasoft
- Autohébergement facilité : Yunohost & **La brique Internet** `http://labriqueinter.net`
- Liste de logiciels pour l'autohébergement :
  - Calendriers et contacts : davical, radicale, baikal
  - Messagerie instantanée : prosody, ejabberd, openfire
  - Serveurs de mail : postfix, exim, opensmtpd, dovecot, cyrus
  - Webmail : Roundcube, mailpile
  - Partage de fichiers et « cloud » : owncloud, seafile, jyraphe, dropcenter, coquelicot
  - Sauvegardes : unison, backupninja, attic-backup, duplicity
  - Site Web, blog : wordpress, drupal, pluxml
  - Travail collaboratif :
    - Wikis : dokuwiki, yeswiki
    - Pads : etherpad-lite, pastebin, gobby (sur réseau local)
    - cf. `https://www.gresille.org/publications/edition_collaborative/`
- Différentes machines pour l'autohébergement : raspberrypi, olimex LIME et LIME2, cubox, cubieboard, bananapi, pine64, fitpc…

Communications

- FAI associatif local : Rézine (ou d'autres de la FFDN : `http://db.ffdn.org`)
  - Tunnels chiffrés (VPN) et **brique Internet**
  - Accès radio
  - Accès DSL
- Navigateurs Web : Firefox, Chromium, torbrowser.
  - Https everywhere (passage en https dès que possible)
  - uBlock Origin (blocage de publicités)
  - Privacy Badger (blocage de mouchards)
  - Adguard (détection et blocage de mouchards, trackers, phishing, balises FB/Google, systèmes d'analyse (google analytics)…), équivalent de Ghostery qui n'est pas libre
  - cf. `https://www.gresille.org/publications/firefox/`
- Pour sécuriser ses communications :
  - Monter des tunnels chiffrés (OpenVPN, ssh, IPSec)
  - Chiffrement de bout en bout : https pour le web, OpenPGP (gpg) pour les mails et OTR (gpg) intégré aux clients IRC ou Jabber
  - Anonymisation : Tor

Sur sa machine

- Essayer d'avoir du matériel libre
- Passer à un système libre : GNU/Linux ou *BSD (éthique, confiance, communauté et continuité…), la Guilde (`http://www.guilde.asso.fr`) ou Démo-Tic (`http://www.demo-tic.org/`) peuvent aider
- Gérer ses mots de passe et les chiffrer : keepassx + passifox (module pour firefox qui interroge keepassx pour s'authentifier sur des sites web facilement) ou pass + PassFF (module pour firefox)
- Chiffrer son disque dur : cryptsetup
- Clients mails : Thunderbird / claws / …
- Client pour gérer des abonnements (syndication, rss, atom) : Firefox avec ou sans extension (genre Brief), Liferea, Thunderbird
- Messagerie instantanée (jabber et/ou irc) : pidgin, xchat, psi, Thunderbird
- Tails : une distribution libre qui efface toute trace sur la machine et utilise Tor