

# Tails

Journées Federez

10 mars 2018

# DISCLAIMER

Ces slides sont basées sur celles d'intrigeri, core-dev de Tails. Les fautes et autres bêtises sont de moi.

# WHOAMI

- Julien (jvoisin) Voisin
- [dustri.org](https://dustri.org)

# WHOAMI



# CE MATIN...

“La vie privée, c’est compliqué”

# TAILS ?

The Amnesic Incognito Live System

<https://tails.boum.org/>

# UN SYSTÈME D'EXPLOITATION LIVE

- Fonctionne sur quasiment n'importe quel ordinateur
- Démarre depuis un DVD, une clef USB, ou une carte SD

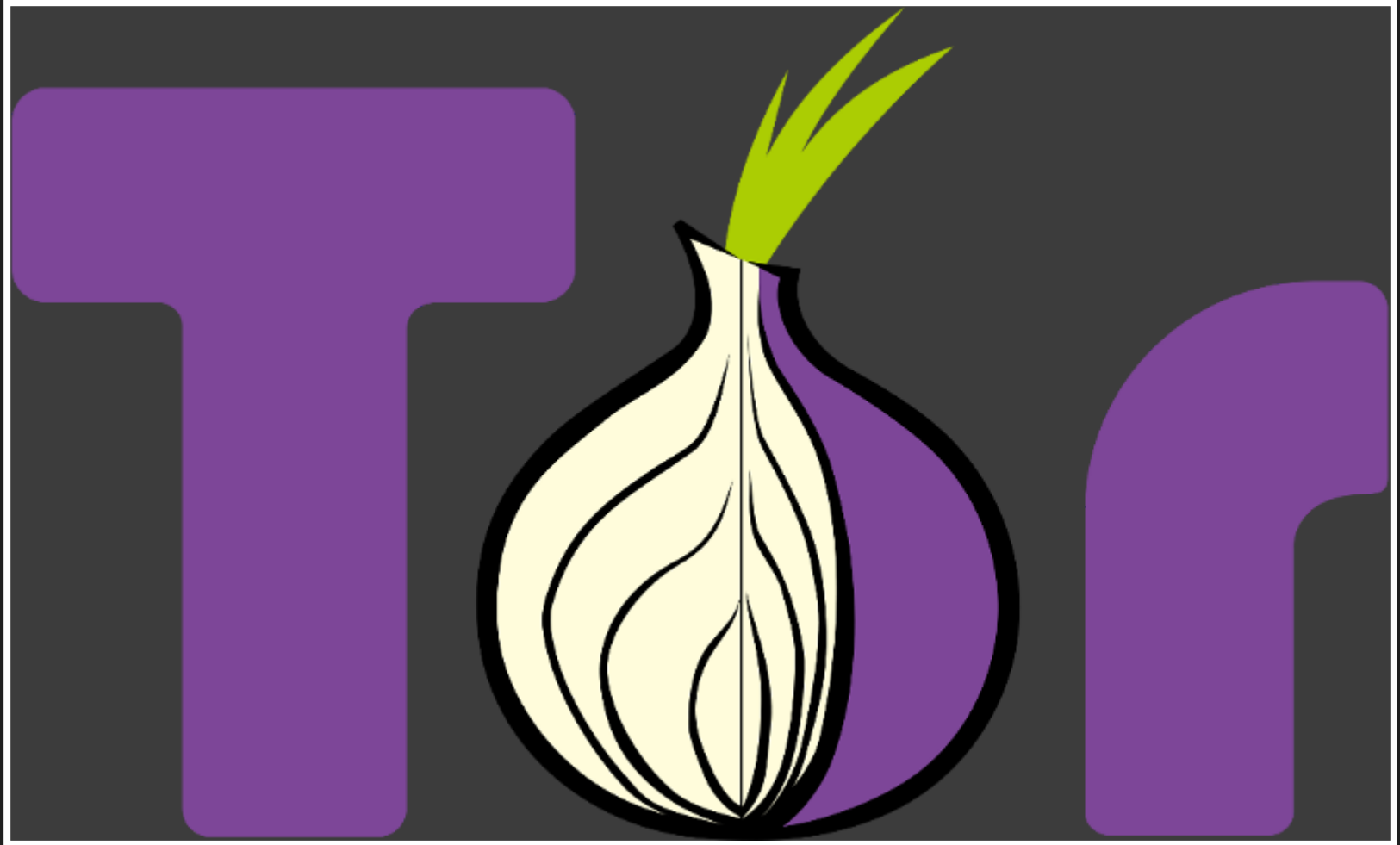
# PRÉSERVER SON INTIMITÉ, SA SÉCURITÉ ET SON ANONYMAT

- Aucune trace sur l'ordinateur utilisé, sauf celles demandées **explicitement**
- Mises à jour automatiques incrémentales
- Utiliser internet de manière anonyme et contourner la censure : toutes les connexions sortantes vers Internet sont anonymisées par Tor



# Tor

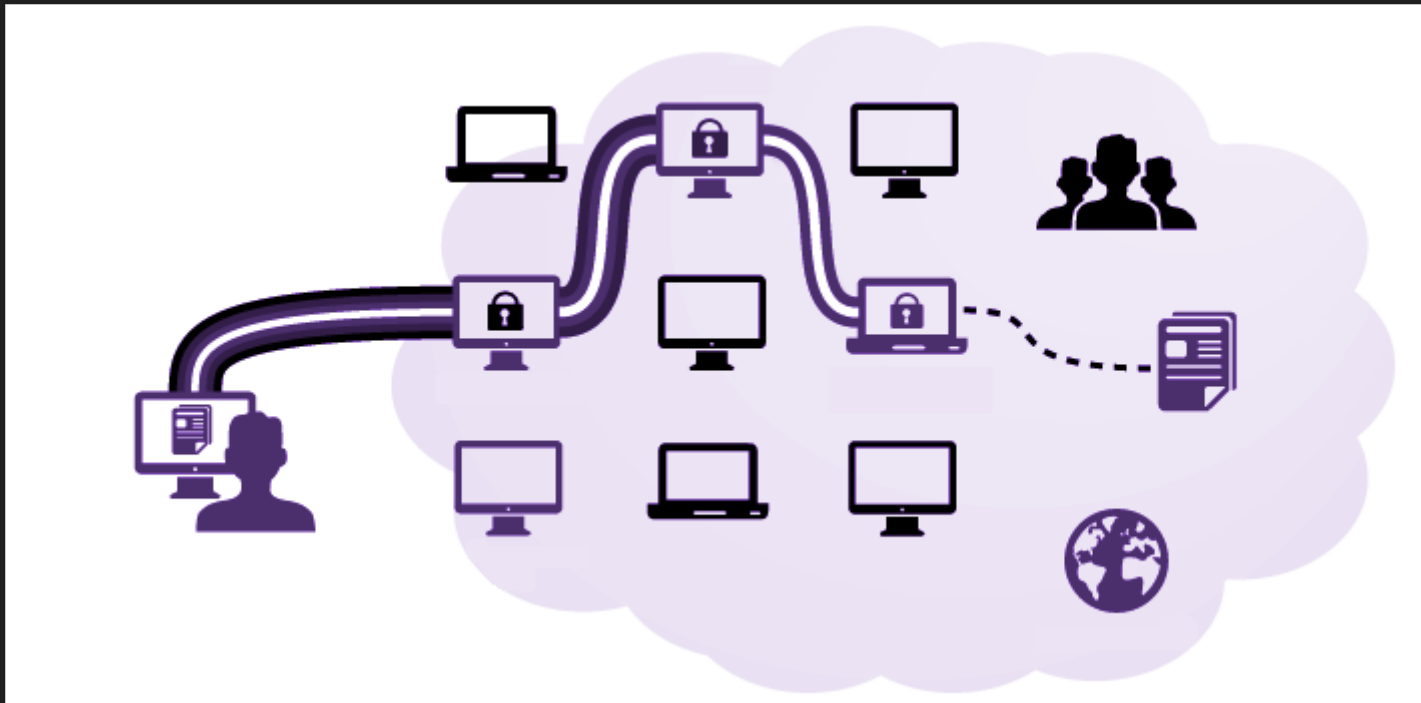
# TOR ?



# TOR!

- Un *réseau*
  - mondial
  - décentralisé
  - permettant l'anonymat
- Un *logiciel*
  - libre
  - mufti-plateformes
  - documenté et spécifié

# TOR, MAIS ENCORE ?



# MAIS ÇA AIDE LES MÉCHANTS !

Pas d'inquiétude, ils s'en sortent très bien sans nous.

# QUELQUES CHIFFRES

- 800 nœuds de sortie
- 6000 relais
- 2000 bridges
- 220Gbit/s de bande passante

# REVENONS À TAILS



# Tails



# TAILS ?

The Amnesic Incognito Live System

<https://tails.boum.org/>

# RICHE EN FONCTIONNALITÉS

- Création de médias: audio, video, texte, images, ...
- Outils de **chiffrement** fort: email, chat, documents, ...
- **Partage** de documents de manière anonyme

# AUTRES CARACTÉRISTIQUES

- Tails est né en 2009
- Traduit dans de nombreuses langues
- Logiciel libre, développement public et ouvert : Git, Redmine, réunions et roadmap
- Documentation de design :  
<https://tails.boum.org/contribute/design/>

# ... ET ÇA MARCHE ?

- D'après la NSA (merci Edward Snowden), oui :

*(S//REL) Tails: Complete Bootable OS  
on CD for anonymity - includes Tor  
(S//REL) Adds Severe CNE misery to  
equation*

*Near-total loss/lack of insight to target  
communications, presence*

# ... ET ÇA MARCHE ?

- Bruce Schneier, décembre 2013 :

*“What do I trust? I trust, I trust Tails, I trust GPG [...]”*

# ... ET ÇA MARCHE ? (CONST.)

- Bruce Schneier, décembre 2013 :

*I use it. Initially I would boot my regular computer with Tails on a USB stick, but I went out and bought a remaindered computer from Best Buy for \$250 and now use that.*

# Challenges

# CADENCE & POPULARITÉ

- Une nouvelle version toutes les 6 semaines
- Environ 20.000 boots par jour, ce nombre double tout les 8 mois
- 10.000 téléchargements de la clef de signature par mois



# RESSOURCES ET TEMPS LIMITÉ

- Tails avance, principalement avec du bénévolat
- Une équipe de *core dev* anonymes, mystérieux, formidables et adorables
- 2800 commits par une quinzaine de personnes sur les derniers 6 mois
- Il y a beaucoup à faire

# Interlude technique

# PARLONS UN PEU DE TECHNIQUE

Le côté social de Tails est passionnant, mais le côté technique n'est pas forcément en reste.

# COMMENT ÇA SE PASSE, LES TESTS ?

- Cucumber pour faire du BDD
- Sikuli pour tester les interfaces graphiques
- KVM pour de la virtualisation imbriquée
- Des tests en boîte noire
- Des gens pour tester le reste

# ET POUR L'INFRASTRUCTURE ?

- Infrastructure as code
- Puppet partout
- Les contributions sont, ici aussi, les bienvenues

# ET POUR LA SÉCURITÉ PURE ET DURE ?

- Persistence du PRNG
- Persistence du cache de Tor
- Persistence de bridges
- Builds reproductibles

# TRUCS ET ASTUCES

- Tails s'éteint dès que la clef usb est retirée
- Tails écrase sa RAM en s'éteignant
- Spoofing de MAC

# L'utilisabilité, une propriété de sécurité



# LE POINT DE DÉPART

- La confidentialité et l'anonymat sont des questions collectives
- Des outils plus sécurisés mais moins utilisables = moins de sécurité collective

# HYPOTHÈSE

Souvent privilégier l'utilisabilité à la sécurité "pure".

Rendre l'anonymat et la sécurité accessibles, pour

- que Tails soit largement utilisé
- attirer davantage de contributeurs
- tous se noyer dans la masse

# EXEMPLES

- Bureau GNOME, et son accessibilité associée
- Cryptographie accessible (Seahorse, applet OpenPGP, GNOME Disks, OTR)
- OTR par défaut sur Pidgin
- Le greeter pour présenter des choix de manière simple
- Mises à jour incrémentales
- Les Blobs

# EXEMPLES (CONT.)

- L'installateur magique
- Installateur web pour vérifier l'image
- Tout plein de documentation
- Traductions
- Avertissements
- *WhisperBack*

# COMMENT ON REND LES CHOSES UTILISABLES ?

C'est loin d'être évident.

1. Donner des objectifs aux utilisateurs, et les regarder se planter
2. Identifier les points de blocage, et les corriger
3. Recommencer

# EXEMPLE: LA PERSISTENCE

- Basée sur LUKS, dm-crypt et ext4
- L'UX est **non-triviale**
- Des profils pour les logiciels/composants essentiels
- Laisser la liberté aux *power users* de persister tout et n'importe quoi

# SUPPORT ET ASSISTANCE

- WhisperBack pour remonter des bugs
- Frondesk pour répondre aux emails
- Mailing list
- XMPP

Un petit delta pour  
ne pas couler



# LEÇON D'HISTOIRE

Souvent, les petites distributions (dans ce domaine) spécialisées meurent vite: Haven, Anonym.OS, ParanoidLinux, onionOS, Phantomix et tant d'autres.

# POURQUOI ?

- Projets individuels, peu ou pas organisés pour grandir
- Sous-estimation du travail de maintenance et de support utilisateur
- Pas d'engagement sur le long terme
- Le syndrome NIH

# HYPOTHÈSES

- Privilégier la maintenabilité
- Éviter d'avoir un delta qui grandit trop, ou trop vite, avec nos upstreams

# EXEMPLES : CE QUI N'A PAS ÉTÉ FAIT EN INTERNE

... malgré les pressions :

- grsecurity
- durcissement lors de la compilation

# EXEMPLES : CE QUI A ÉTÉ FAIT EN INTERNE

... et qu'on devrait partager :

- tests complets (cucumber, sikuli, libvirt)

# EXEMPLES : CE QUI A ÉTÉ FAIT UPSTREAM

- AppArmor
- libvirt
- Seahorse
- Debian
- Debian Live
- Applet OpenPGP
- Corriger une attaque de downgrade sur OTR

# CONSÉQUENCES #1

- travail “politique” :
  - parler aux upstreams
  - sensibiliser à nos besoins
  - trouver des gens compétents pour faire le travail au bon endroit

# CONSÉQUENCES #2

- travail de glue
- peu de code spécifique à Tails
- rythme lent (attendre la prochaine version de Debian, voire la suivante), malgré les backports



# CONSÉQUENCES #3

Et surtout...

*Tails est encore là !*

# CONTACT

- [tails-dev@boum.org](mailto:tails-dev@boum.org), liste publique pour le développement
- [tails@boum.org](mailto:tails@boum.org), liste privée et chiffrée, pour les discussions à avoir en secret
- XMPP, cf. <https://tails.boum.org/contribute/>
- Venez me parler ;)

<https://tails.boum.org/>

# QUESTIONS

