

Café Vie Privée Alternative pour Android

Café Vie Privée

Présentation d'outils libres pour se protéger sur Android



Déroulé

- 1 Pourquoi se protéger ?
- 2 Comment se protéger ?
- 3 Les Applications
- 4 OS Alternatif

Pourquoi se protéger ?

Wikipedia

Android est un système d'exploitation mobile fondé sur le noyau Linux et développé actuellement par Google.

Android à été lancé en 2007.

Le code est sous *licence apache (ASL)*. Il peut donc être intégré dans des applications propriétaires.

Quelques infos

On peut le trouver sur

- Téléphone
- Tablette
- Télévision
- Livre électronique (ex : chomebook)
- Montre
- Voiture
- ...

Il possède plus de 80% de part de marché des smartphone (en 2015).

Économie de la surveillance

Les Publicitaires

Les applications dépendent d'un model économique, qui souvent est dépendant des publicitaires.

Pour cela ils utilisent des pisteurs.

Exodus Privacy

Exodus Privacy

Est une plate-forme d'analyse des applications Android qui liste les traqueurs et les autorisations de celles-ci.

Créer en 2017.

(ClassyShark3xodus le fait pour les apk de F-droid)

Programme de surveillance

Les enjeux

Il existe de nombreux programmes de surveillance plus ou moins connus.

Jérémy Zimmermann

Ne pas confondre entre : j'ai rien à me reprocher et j'ai rien à cacher.

Cf. Le documentaire Notiong To Hide

Refuser les programmes de surveillance des données comme PRISM, XKeyscore et Tempora.

PRISM

Programme de surveillance américain créé par la NSA. Collecte les données sur internet. Edward Snowden a dénoncé ce programme en juin 2013.

XKeyscore

Programme de surveillance créé par la NSA. Collecte quasi systématique des activités de tout utilisateur sur Internet. Révélé en juillet 2013.

Tempora

Programme britannique permettant d'intercepter les données transitant par les câbles en fibre optique entre l'Europe et les États-Unis.

Contre attaque

Il existe des projet pour se défendre contre ça :

<https://prism-break.org/fr/categories/android/>

On y reviendra :)

La surveillance de masse

Les puissants - la centralisation

Nos environnements informatiques utilisent des **logiciels propriétaires**, et pour la plupart détenue par quelques uns qui ont un **poids important** dans notre société.

D'où la création du terme **GAFAM** : Google Apple Facebook Amazon Microsoft

Les besoins

Accéder au code source permet d'**auditer** le code et vérifier que le logiciel correspond à ce pourquoi il est fait.

Le logiciel libre permet de **modifier** le code pour nos besoins personnels.

Ainsi que la **décentralisation**.

Comment se protéger ?

En utilisant du logiciel Libre.
On se permet d'auditer le code source,
de l'adapter pour soi même.
Donc il ne **dépend pas** d'un **modèle économique** particulier.

On va voir quelques exemples :

- Magasin d'applications
- Navigation
- Réseaux sociaux
- Cartes
- Multimédia
- Recherches
- Divers

Les Applications

Playstore → F-Droid

Playstore → Aurora Droid

Playstore → Yalp store

Playstore → Aurora Store

Chrome → Firefox

Google → Duckduckgo

Tor Browser (anciennement Orfox)

Orobot (Proxy pour le réseau Tor)

Facebook → slim social (ou Frost for facebook)

Diaspora

Mastodon

Whatsapp → Signal
SMS → Silence
Conversation (XMPP)

OsmAnd (Openstreetmaps)

Youtube → NewPipe
Peertube → Thoruim

Google → Duckduckgo

Clavier Google → AnySoftKey

Météo Votre météo locale (F-droid)

Caméra Open Caméra

Transport Transportr

Bloqueur Blokada

Liseure Book Reader

Luminosité Red Moon

Battery Drowser

OS Alternatif

Il n'existe pas beaucoup d'alternatives complètes, car la difficulté est le support matériel du téléphone.

Exemple :

- Replicant
- PureOS
- LineageOS

Replicant est un système d'exploitation entièrement libre pour les smartphones et les tablettes, en remplaçant les composants propriétaires d'Android par leurs équivalents libres.

Fait pour Librem5.

<https://puri.sm/products/librem-5/pureos-mobile/>

- Théorie avec microG

- Avantage du contrôle accès applications - Démo