Protéger ses données avec 5 outils de chiffrement sur Linux

Si vous pensez que vos données sont très précieuses, vous devriez certainement considérer leurs sécurités comme une priorité.
Dans de plus en plus d'entreprises travaillant avec de multiples plates-formes, vous devez être prêt à travailler avec le chiffrement sur à peu près tous les systèmes d'exploitation disponibles, y compris Linux.

Mais quels sont les outils que vous devriez peut-être regarder?
Sur Ubuntu, vous trouverez la majorité des outils disponibles (dans les résultats de la recherche “chiffrement ou cryptage”) dans La logithèque Ubuntu (Ubuntu Software Center).
Je vais vous montrer 5 outils de chiffrement pour Linux.

1. GnuPG

GnuPG est le logiciel de base pour chiffré un fichier sous Linux.
Vous pouvez facilement chiffrer un fichier avec GnuPG en ligne de commande.
Pour l'installer :

```
aptitude install gnupg
```

La commande pour chiffrer un fichier est:

```
gpg -c <FICHIER>
```

Le fichier chiffré aura une extension `.gpg`. Pour déchiffrer un fichier, la commande est:

```
gpg <FICHIER.gpg>
```

C'est le moyen le plus rapide et facile pour chiffrer des fichiers (même si vous devez toucher la ligne de commande).

2. Veracrypt

Veracrypt est un fork amélioré de TrueCrypt, donc beaucoup plus sûr, car, selon ces développeurs, ils auraient tenu compte des remarques soulevées par l'audit du code de Truecrypt.
Comment beaucoup plus sécurisé?\\Eh bien, TrueCrypt utilise 1000 itérations de l'algorithme PBKDF2-RIPEMD160 pour les partitionnements du système, VeraCrypt en utilise 327 661.
VeraCrypt utilise 655331 itérations de l'algorithme RIPEMD160 et 500.000 itérations de SHA-2 et Whirlpool.
Même si cela rend VeraCrypt légèrement plus lent à ouvrir, il rend le logiciel 10 a 300 fois plus sûr contre les attaques de force brute.
“En effet, quelque chose qui pourrait prendre un mois à se crack avec TrueCrypt pourrait prendre une année avec VeraCrypt”. Wikipédia

Le GUI de VeraCrypt est simple à utiliser et vous guide à travers l'ensemble du processus de création

des conteneurs chiffrés, pour ceux qui auraient utilisé le GUI de Truecrypt et bien c'est le même. Pour l'installation sous debian on récupère la tarball ici

```
tar -xvjf veracrypt-1.0f-2-setup.tar.bz2
```

Puis l'installation, simple :

```
./veracrypt-1.0f-2-setup-gui-x64 #ou x86
```

Après, cette étape n'est pas obligatoire, mais j'ai la flemme de lancer l'application en `root`, j'ai donc installé `sudo` et fait quelques manipulations dans gnome pour que cela fonctionne.

```
aptitude install sudo
visudo
```

Ajouté ce qui suit à la fin, en prenant soin de changer `<LOGIN>` par votre `login`.

```
<LOGIN> ALL=NOPASSWD: /usr/bin/veracrypt
```

Dans gnome utilisé l'application `menu principal` allé dans `Accessoires` sélectionné Veracrypt, cliqué sur propriété entrer dans le champ `command` ce qui suit:

```
sudo /usr/bin/veracrypt
```

Après, cela la flemme est en vous et vous pouvez lancer Veracrypt depuis le menu de gnome.

3. GNOME Files

c'est le gestionnaire de fichier par défaut pour les ordinateurs de bureau GNOME.
Dans cette outil convivial se trouve la capacité de protéger facilement vos fichiers et dossiers avec un chiffrement du mot de passe de bas niveau.
Il suffit de sélectionner le fichier pour la compression, sélectionnez un format de compression qui travaille avec chiffrement (comme zip), ajouter un mot de passe et de compresser.

4. KGpg (KDE) ou Seahorse (gnome)

KGpg et Seahorse sont des interfaces conviviales pour l'utilisation de GnuPG.
Bien que vous ne soyez pas en train de chiffre/déchiffrer des répertoires avec KGpg et seahorse, vous gérez les clés de chiffrement qui fonctionnent avec un certain nombre d'outils. (engmail sur thunderbird, etc)
Sans les clés de chiffrement, beaucoup de ces outils ne fonctionneront tout simplement pas, certaines personnes évite de travailler avec le chiffrement sur Linux en raison de la complexité perçue de la ligne de commande GnuPG.

Note: ils devraient être déjà installé sinon :

```
aptitude install seahorse #pareille pour kGgpg
```

5. Gnome Encfs Manager

Gnome Encfs Manager est un outil graphique pour le système de chiffrement de fichier de encfs.
Il convient de noter qu'il existe une vulnérabilité avec encfs, si votre système(s) est sujets aux attaques, encfs n'est pas l'outil idéal pour vos données sensibles.
Toutefois, si votre système hôte (ou réseau) ne sont pas sujet aux attaques, cela devrait être bon.
Gnome encfs Manager facilite la création de “caches” (aka conteneurs) facilement.
Avec seulement quelques clics, vous pouvez créer et configurer un dossier caché sur votre répertoire Linux. Les options incluent le montage au démarrage, délai d'inactivité et le changement de mot de passe.
Gnome encfs Manager peut fonctionner uniquement avec encfs de sorte que vous ne saurez pas déchiffrer les conteneurs provenant d'autres systèmes.

Pour finir, certains de ces outils peuvent aussi aller bien au-delà des simples explications données. Mais si, vous cherchez une application qui offre la sécurité de chiffrement et le fait en un clin d’œil, ces cinq applications vous aideront à démarrer.

Avez-vous un outil de chiffrement Linux préféré, qui ne fait partie de cette liste?
Partagez vos recommandations.