Chiffrement de dossiers (conteneurs) : Linux

Matthieu Herrb

10 mai 2019

Introduction

Protéger des documents sensibles *en ligne*.

- lorsqu'ils ne sont pas utilisés,
- pendant le transport (mail, sauvegardes,...)

Sur Linux, 2 outils possibles Zed ! ou veracrypt

Veracrypt

- Successeur de *TrueCrypt*
- Reprend la même technologie
- A fait l'objet d'un audit de sécurité indépendant en 2016

Fonctionnalités :

- Multi-plateformes (Windows, Linux, macOS).
- Chiffrement de partitions ou de conteneurs.
- Bootable sous Windows.
- Mode portable sous Windows.
- Possibilité de créer des volumes cachés (« Déni Plausible »).

`https://www.veracrypt.fr/`

Principe

- Un conteneur $\rightarrow$ un fichier contenant un système de fichiers
- « Montage » du conteneur comme un disque avec un mot de passe
- Permet de travailler sur le contenu avec tous les outils habituels
- Pendant l'accès au conteneur monté, jamais de copie en clair du contenu vers le disque
- Une fois le conteneur démonté, le contenu en mémoire en clair est effacé

Limitations

- Conteneurs de taille fixe, pré-allouée à la création.
- Attention à certaines applications qui créent des fichiers de sauvegarde en clair hors du conteneur (par ex l'éditeur de textes `vi`)
- Utiliser un système de fichiers FAT32 (MSDOS) pour avoir des conteneurs portables aux autres systèmes
- Intégration au bureau Linux améliorable...