UNIVERSITE EVRY VAL D'ESSONNE

Système de fichiers chiffrés sous Linux

GETTLIFFE Joffrey

10/04/2008

Sommaire

Pourquoi, comment et avec quoi crypter ses fichiers 3
Les algorithmes de cryptage 4
AES – Advanced Encryption Standart 4
Serpent 4
Twofish 4
Comment procéder : exemple de TrueCrypt 5
Liens 7

Pourquoi, comment et avec quoi crypter ses fichiers

Pourquoi :

Le chiffrage de fichier est une méthode utilisée afin de sécuriser l'accès aux données d'une machine. Seul l'utilisateur possède la clé nécessaire au décryptage et donc en cas de perte ou de vol des données, personne ne sera capable de s'en servir.

Comment :

Il existe deux méthodes pour protéger ses fichiers :

- Crypter chaque fichier

  Tout les fichiers d'un volume sont chiffrés et éventuellement possèdent une clé différente. Cette méthode implique d'entrer la clé à chaque utilisation du fichier.

- Crypter directement le volume

  Le chiffrage se fait au niveau du volume ou de la partition contenant les fichiers. Ces derniers sont utilisables par toute personne ayant accès à la partition. L'avantage par rapport au cryptage au niveau des fichiers est que l'utilisateur n'entre la clé qu'au moment d'accéder à la partition.

Avec quoi :

De nombreux logiciels gratuits sont disponibles sur internet :

- TrueCrypt
- Loop – AES
- FreeOTFE

Les algorithmes de cryptage

AES – Advanced Encryption Standart

Créer en 1998 par Joan Daemen et Vincent Rijmen, l'algorithme récupère des blocks de 128 bits qu'il permute et stocke dans une matrice qui, après rotation de ses lignes, subit diverse modifications par multiplications binaires, polynomiales et matriciel définissant ainsi un tour. Pour des clés de 256 bits avec 128 bits de block, l'algorithme AES crypte les données sur 14 tours.

Cette méthode est utilisée par le gouvernement américain dans le chiffrement de leurs données de plus haute importance.

Serpent

Mis au point par Ross Anderson, Eli Biham, and Lars Knudsen en 1998, il s'applique sur des clés de 256 bits par bloc de 128 bits sur 32 tours. Malgré son niveau de sécurité, il fut l'algorithme finaliste pour le processus de standardisation AES de cryptage lancé en 1997.

Twofish

Créer par Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall et Niels Ferguson en 1998, il fut un des 5 finalistes pour le processus AES. Il utilise également des clés de 256 bits par bloc de 128.

A noter la possibilité de combiner les différents algorithmes entre eux et ainsi donner forme à 4 nouvelles variantes : AES – Serpent, AES – Twofish, AES – Serpent – Twofish, Serpent – AES – Twofish

Comment procéder : exemple de TrueCrypt

Un exemple de logiciel gratuit proposant un chiffrage de fichier à l'aide des algorithmes vu précédemment : TrueCrypt.

Ce programme simple et facile d'utilisation, propose la création d'un volume de taille paramétrable qu'il cryptera ensuite en fonction de l'algorithme choisi par l'utilisateur et du mot de passe que ce dernier entrera pour le protéger.

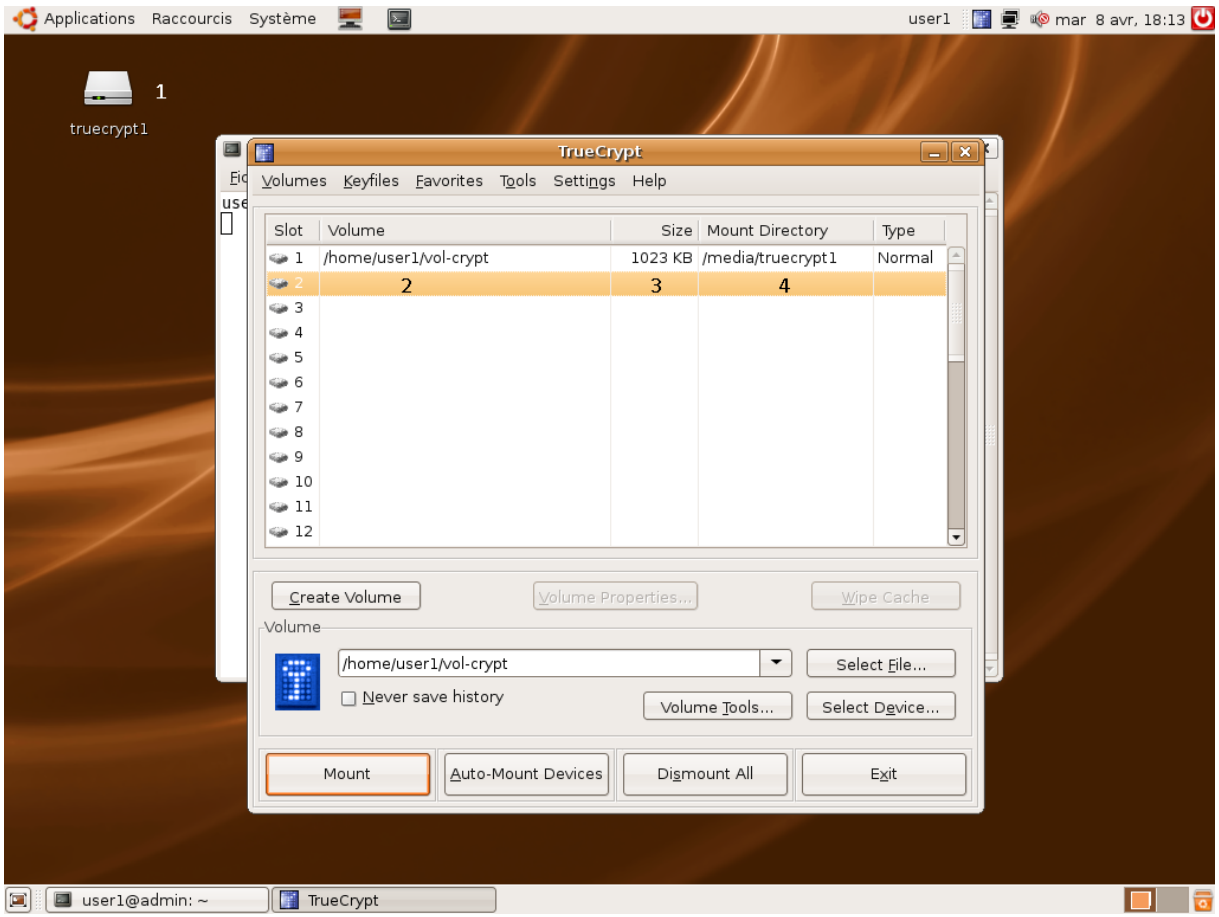
Un assistant accompagne la progression et préviendra l'utilisateur en cas de mauvais paramétrage ou encore pour informer si le passe choisi est compliqué ou non.

La procédure se déroule en plusieurs étapes à travers lesquelles l'utilisateur peut choisir si le volume est caché ou non, l'emplacement du fichier crypté à monter et la taille qu'il souhaite lui dédier en fonction de l'espace disponible sur le disque.

Ces informations concernent principalement le fichier de sortie que retournera le programme. Il sera stocké à l'emplacement définit par l'utilisateur et sera nécessaire pour accéder au volume une fois la procédure terminée.

Vient ensuite le choix de l'algorithme parmi les variantes proposées précédemment puis le mot de passe qui protégera l'accès au volume. Ce dernier sera nécessaire pour monter le volume une fois créé et ainsi accéder à son contenu.

Le formatage suit avec le choix du type de système de fichier (en FAT ou non) et les clés (header et master keys) qui vont encrypter le volume.



1 – Volume monté par le logiciel
2 – Fichier crypté du volume
3 – Taille du volume crypté
4 – Volume monté par le logiciel

Une fois le volume créé, l'utilisateur devra le monter sur l'un des emplacements disponible proposé par le programme et lui sera demandé le mot de passe qu'il à précédemment défini. Dés que le fichier est monté, l'icône du volume apparait et l'utilisateur peut y accéder librement sans avoir à entrer de nouveau le mot de passe tant que le fichier reste monté (même en quittant le logiciel).

Liens

TrueCrypt (2.1 Mo) : http://www.truecrypt.org/downloads.php

Documentation : http://www.truecrypt.org/docs/

Algorithmes de cryptage : http://www.wikipedia.org