Truecrypt

Położenie: (nie dotyczy)

Wstęp

Na licencji *freeware* (nie *GPL*). Umożliwia szyfrowanie za pomocą klucza (może nim być dowolny plik na dysku) oraz / lub hasła. Najlepiej stosować obie metody jednocześnie. Plik konfiguracyjny programu to *~/.TrueCrypt/Configuration.xml*. Aby program działał prawidłowo, muszą być załadowane następujące moduły z jądra:

Device Drivers →
[*] Block devices
  <> Loopback device support* (moduł *loop*; u mnie jest na stałe w jądrze)
[*] Multiple devices driver support (RAID and LVM):
  <M> Device mapper support (moduł *dm_mod*)
    <M> Crypt target support (moduł *dm_crypt*)
File systems →
  <M> FUSE (Filesystem in Userspace) support (moduł *fuse*; oprócz tego należy zainstalować pakiet „*sys-fs/fuse*”)
Cryptographic API →
  <M> XTS support (moduł *xts*)
  oraz inne metody szyfrowania, które chcemy używać (jako moduły)

W moim przypadku *udev* nie ładował automatycznie *fuse*, więc dałem wpis w pliku */etc/conf.d/modules* → *fuse* (moduł *dm_crypt* ładowany jest automatycznie, gdy jest potrzebny). Należy upewnić się także, że usługa jest ładowana podczas startu systemu. Jeśli nie jest, należy wykonać:
rc-update add truecrypt boot

Tryb tekstowy

Z trybu tekstowego należy korzystać w *tty terminalu* poza środowiskiem graficznym. Jeśli chcemy z tego trybu korzystać uruchamiając terminal w środowisku graficznym, musimy w poleceniach stosować parametr *--text*.
1. Tworzymy klucz:
truecrypt --text --create-keyfile mojKlucz.txt (klucz jest tworzony w oparciu o losowy szum poruszanej myszki lub losowo wpisywane znaki; co ciekawe, kluczem może być dowolny zwykły nieszyfrowany plik na naszym dysku twardym - ważne, aby nie zmieniał zawartości).

2. Tworzymy wirtualny kontener (normalny lub ukryty):
truecrypt --text --create /mnt/usb/mojTajnyKontener.txt

a) rodzaj kontenera: *normal* (kontener ukryty można zrobić tylko wewnątrz wcześniej utworzonego normalnego kontenera, musi mieć inne hasło i klucz choć będzie mieć tą samą nazwę kontenera; podając to hasło, program automatycznie przekieruje do kontenera ukrytego);
b) encryption algorithm: *AES*;
c) hash algorithm: *SHA-512*;
d) filesystem: *none*;
e) password: *...publiczne*
f) wpisać co najmniej 320 losowych znaków;

3. Mapujemy kontener do postaci wirtualnego dysku i tworzymy na nim system plików:
truecrypt --text /mnt/usb/mojTajnyKontener.txt --keyfiles=/root/mojKlucz.txt --filesystem=none (montujemy folder bez montowania systemu plików)
a) podajemy utworzone wcześniej hasło do tajnego kontenera (normalnego lub ukrytego);
b) program pyta czy chcemy zabezpieczyć ukryty kontener (wybrane sektory w kontenerze normalnym) przed nadpisaniem; jeśli mamy taki, to odpowiadamy „tak” (sektory kontenera ukrytego są wtedy *read-only*), inaczej odpowiadamy „nie”.

Jeśli wszystko powiedzie się, tworzone jest urządzenie */dev/mapper/truecrypt1* (wirtualny abstrakcyjny dysk).
truecrypt --text --verbose --list (czy wirtualny dysk na pewno powstał?)
mkreiserfs /dev/mapper/truecrypt1 (zakładamy system plików na wirtualnym dysku)
truecrypt --text --dismount /mnt/usb/mojTajnyKontener.txt (odmontowanie)

4. Montowanie utworzonego konteneru:
truecrypt --text /mnt/usb/mojTajnyKontener.txt --keyfiles=/root/mojKlucz.txt --fs-options=noauto,notail,rw,user /mnt/szyfrowane (wymagane prawa administratora; można równocześnie zamontować normalny i ukryty kontener, z tym że ukryty jako pierwszy, a normalny jako drugi z opcją ochrony kontenera ukrytego)

5. Kopiowanie plików przez zwykłego użytkownika:
groupadd truecrypt (tworzymy grupę *truecrypt*)
usermod -a -G truecrypt (dodajemy użytkownika do grupy *truecrypt*)
Niestety, prawa do tego udziału są resetowane za każdym razem, gdy system jest uruchamiany od nowa. Należy więc za każdym razem powtórzyć na koncie roota jeszcze to:
chown -R root.truecrypt /mnt/szyfrowane (zmieniamy grupę dostępu do zamontowanego udziału; polecenie to należy wydać po zamontowaniu udziału)
 # chmod -R 775 /mnt/szyfrowane (zmieniamy prawa dostępu dla grupy *truecrypt*)
Na koniec pracy z szyfrowanym kontenerem:
truecrypt --text --dismount /mnt/usb/mojTajnyKontener.txt (odmontowanie)
history -c; echo > /root/.bash_history (czyścimy historię poleceń)

Tryb graficzny

1. Generowanie klucza: menu *Tools / Keyfile generator*.
2. Tworzenie kontenera: *Volumes / Create New Volume...*
3. Tworzenie systemu plików *Reiser*: w trybie tekstowym.
4. Montowanie:
a) zamontować pendrive pod */mnt/usb*;
b) Select file: */mnt/usb/kontener.txt* / *Mount: Password, Use keyfiles, Mount at directory(/mnt/szyfrowane), Mount options*; (na pierwszym slocie pojawia się zamontowany kontener);

Informacje:
Od roku 2014, program nie jest rozwijany. Jego następcą jest *VeraCrypt*.

Ostatnia aktualizacja: 6 września 2016.