TrueCrypt

Truecrypt je program pro bezpečné šifrování dat. Nabízí veliké množství šifrovacích algoritmů, mezi nimi i velmi známý AES-256. TrueCrypt je multiplatformní, můžete tedy jeho jednotky používat na více operačních systémech - zatímco v OS Windows se truecrypt jednotky připojí jako nový disk, v Ubuntu se připojí jako klasický disk skrze adresářovou reprezentaci.

 Od verze 5.0 můžete TrueCrypt používat přes grafické rozhraní a od této verze také odpadly problémy s verzí jádra (truecrypt využívá FUSE) a s použitím souborového systému NTFS. V tomto návodu jsou uvedeny převážně textové příkazy, ale vše můžete naklikat v grafickém rozhraní. Pro nováčky je to doporučená metoda.

Pokud chcete aby se vám truecrypt spouštěl v textovém módu, použijte první paramater -t nebo –text, tedy příkaz: *truecrypt -t*.

Instalace

Nejsnažší instalace je přes .tar.gz balíčky pro Linux, které se dají stáhnout na domovské stránce programu: http://www.truecrypt.org/downloads.php (Linux Standard - x86 / x64 podle verze vašeho operačního systému). Po stáhnutí balíčku jej rozbalte a vytvořený soubor nainstalujte dvojitým poklepáním. Grafické rozhraní programu je stejné jako v ostatních operačních systémech.

Spuštění TrueCrypt po přihlášení

Pokud často používáte zašifrované jednotky, je výhodné spouštět TrueCrypt již po přihlášení. Spusťte si nástroj **Aplikace spouštěné při přihlášení** a vyberte **Přidat**. Vyplňte:

```
Název: Truecrypt
Příkaz: truecrypt
```

 Pokud před vypnutím systému správně neodpojíte TrueCrypt jednotku, může se stát, že zůstane zamčená. Standardně se zámek odstraní, ale někdy se to nepovede. Truecrypt se potom odmítá spustit s dialogem, že již běží. Nejsnažším řešením je se znovu odhlásit a přihlásit.

Vytvoření Truecrypt jednotky se souborovým systémem NTFS

 Před použitím návodu se ujistěte, že máte nainstalovaný balík *ntfs-3g*.

Vytvoření NTFS truecrypt jednotky je výhodné tehdy, pokud plánujete používat tuto jednotku v Ubuntu i v OS Windows. Další možností je použít EXT3/4 - a v OS Windows doinstalovat ovladače, které nejsou příliš stabilní.

Klasickým způsobem vytvořte truecrypt jednotku, ale vyberte jako souborový systém *none*. Pro vytvoření existují dva způsoby - skrze grafické rozhraní, nebo textovým průvodcem:

```
sudo truecrypt -t -c
```

Zde jako volume type doporučuji pro začátečníky použít typ normal. Následně zadejte cestu, kde chcete jednotku vytvořit. Můžete vybrat buď soubor, nebo celý oddíl disku. Zde zadáváte k cestu k souborové reprezentaci vašeho oddílu (například /dev/sda3. Pokud prázdný oddíl nemáte, můžete jej vytvořit přes gparted.

 Při vybírání oddílu buďte velmi opatrní. Jakmile vyberete nesprávný oddíl, všechna data na něm budou nenávratně ztracena. Pokud například vyberete kořenový oddíl, na kterém běží váš operační systém, formátování proběhne a vymaže veškeré zaváděcí záznamy. Daleko bezpečnější je pro vytváření truecrypt jednotky použít soubory, které lze následně lehce spravovat.

Nyní musíte zjistit, jaké hardwarové zařízení trucrypt po namountování vytvoří. To zjistíte připojením diskového oddílu s těmito parametry:

```
sudo truecrypt -t /dev/sda3 --filesystem=none
```

A s největší pravděpodobností vznikne v adresáři */dev/mapper/* nové zařízení truecrypt1 (to zjistíme přes příkaz ls /dev/mapper). Pokud se tak nestane, můžete tuto informaci vyčíst po zadání příkazu *mount*.

Pokud jste si jistí, že souborová reprezentace truecrypt zařízení je např. */dev/mapper/truecrypt1*, můžete začít vytvářet souborový systém. K tomu slouží příkaz *mkntfs*. Použijeme jej takto:

```
sudo mkntfs -f /dev/mapper/truecrypt1
```

Pokud vám po proběhnutí popřeje konzole příjemný den, máte úspěšně vytvořenou NTFS truecrypt jednotku. Nyní ji stačí je odpojit přes *sudo truecrypt -d* a znovu připojit pomocí klasického postupu, např. *truecrypt /dev/sda3 /media/truecrypt*.

Připojení TrueCrypt jednotky

V okně programu vyberte pomocí **Select file** nebo **Select device** svůj zašifrovaný soubor/oddíl. Klepnutím na tlačítko **Mount** vyvoláte výzvu pro zadání hesla. Zde můžete také nastavit v podnabídce *Options* adresář, do kterého se chcete připojit (pokud jej nevyberete, truecrypt si jej vytvoří sám). Po zadání hesla a potvrzení se vás může program zeptat na vaše administrátorské heslo, kvůli přístupu do adresáře */media/*. Po úspěšném připojení by se vám měl objevit v Nautilu nový

disk, který by měl být standardně přístupný i pro zápis.

 Velice výhodné je také přidat nejčastěji používané jednotky do oblíbených (favorites). To můžete provést přes pravé tlačítko v hlavním okně programu na připojené jednotce. Poté stačí jen přes menu programu vybrat **Mount All Favorite Volumes**.

Jak umožnit běžným uživatelům připojení Truecrypt jednotek

Toto je výhodné, pokud je váš počítač používán jako multiuživatelský systém a každý uživatel nemá přístup k heslu roota. Nejprve je třeba vytvořit novou uživatelskou skupinu truecrypt, to provedete například takto:

```
sudo groupadd truecrypt
```

Poté je třeba upravit chování příkazu sudo, aby všichni členové skupiny truecrypt přistupovali k programu s oprávněním administrátora. Přes program *visudo* přidejte tyto řádky:

```
# Users in the truecrypt group are allowed to run truecrypt as root.
%truecrypt ALL=(root) NOPASSWD:/usr/bin/truecrypt
```

A následně přidejte do skupiny truecrypt požadované uživatele:

```
sudo gpasswd -a USER_1 truecrypt
```

Pokud stále uživatel nemůže do jednotky zapisovat, je třeba změnit oprávnění přípojného bodu, např.:

```
sudo chgrp truecrypt /media/truecrypt/
```

Šifrování diskového oddílu

Přístup k datům je chráněn heslem. Kvalitu hesla si volí uživatel sám. Obecně se doporučuje heslo délky 12 až 15 znaků, které je kombinací malých a velkých písmen, číslic a speciálních znaku. Další možností přístupu k datům je přes šifrovací klíč, a nebo přes kombinaci hesla a klíče. Speciální klíč je generován přímo programem Truecrypt, jeho velikost je 320 bajtů a ukládá se do uživatelem zvoleného souboru.

```
truecrypt --create-keyfile key.txt
```

Vytvoření šifrovaného oddílu

Šifrovaný adresář nebo oddíl můžete vytvořit dvěma způsoby. Nejjednodušší cestou je příkaz v konzoli:

```
truecrypt -c
```

Tento příkaz interaktivně umožní uživateli nakonfigurovat požadované vlastnosti šifrovaného adresáře – typ oddílu a souborového systému, hašovací a šifrovací algoritmus, velikost oddílu a nakonec přístupové heslo. V závěru konfigurace se používá zařízení /dev/input/mice pro sběr náhodných dat. Pokud tedy vytváříte šifrovaný oddíl v uživatelském režimu, je vhodné nastavit přístupová práva k zařízení /dev/input/mice do read módu pro ostatní uživatele příkazem:

```
chmod o+r /dev/input/mice
```

Výstup programu je následující:

```
[user@localhost ~]# truecrypt -c cryptovolume.tc
Volume type:
 1) Normal
 2) Hidden
Select [1]: 1

Filesystem:
 1) FAT
 2) None
 Select [1]: 2

Enter volume size (bytes - size/sizeK/sizeM/sizeG): 100M

Hash algorithm:
 1) RIPEMD-160
 2) SHA-1
 3) Whirlpool
 Select [1]: 1

Encryption algorithm:
 1 ) AES
 2 ) Blowfish
 3 ) CAST5
 4 ) Serpent
 5 ) Triple DES
 6 ) Twofish
 7 ) AES-Twofish
 8 ) AES-Twofish-Serpent
 9 ) Serpent-AES
10 ) Serpent-Twofish-AES
11 ) Twofish-Serpent Select [1]:  1
```

```
Enter password for new volume ‘cryptovolume.tc’:
Re-enter password:

Enter keyfile path [none]:
Enter keyfile path [finish]:

TrueCrypt will now collect random data.

Is your mouse connected directly to the computer where TrueCrypt is running?
y
Please type at least 320 randomly chosen characters and then press Enter:
```

Druhou možností je zapsat všechny důležité vlastnosti nově vytvářeného šifrovaného oddílu přímo do příkazové řádky. Například vytvoření normálního oddílu o velikosti 500 MB, šifrovaného kryptografickým algoritmem AES s hašovací funkcí SHA-1 do souboru cryptovolume.tc:

```
truecrypt –type normal –size 500M –encryption AES –hash SHA-1 -c
cryptovolume.tc
```

Nakonec budete vyzváni k zadání přístupového hesla k nově vytvořenému oddílu, nebo k zadání cesty k souboru, který obsahuje vygenerovaný klíč.

Připojení a odpojení virtuálního oddílu

Opět existují dvě možnosti připojení virtuálního oddílu. Nejjednodušším způsobem je spuštění interaktivního příkazu

```
truecrypt -i
```

Nebo specifikace oddílu a místa připojení přímo v příkazové řádce:

```
truecrypt cryptovolume.tc /media/data
```

Po zadání hesla můžete s adresářem /media/data pracovat jako s ostatními adresáři v systému, tj. kopírovat, upravovat a mazat soubory. Po ukončení práce s citlivými daty nezapomeňte virtuální oddíl odpojit.

```
truecrypt -d cryptovolume.tc
```

Přístupové heslo k oddílu lze změnit pomocí příkazu:

```
truecrypt -C cryptovolume.tc
```

Informace o připojených oddílech a jejich vlastnostech zjistíte příkazem:

```
truecrypt -vl
```

Odkazy

- http://www.truecrypt.org
- http://www.linuxexpres.cz/praxe/zasifrujte-si-diskovy-oddil
- http://ubuntuforums.org/showthread.php?t=149561
- http://www.root.cz/clanky/novy-truecrypt-5-0-s-grafickym-rozhranim-pro-linux/
- http://gentoo-wiki.com/HOWTO_Truecrypt

Grafická úprava: Tento návod potřebuje důležité grafické a stylistické úpravy. Více...