By Marcin
Published: 2007-07-02 19:41

TrueCrypt Tutorial: Truly Portable Data EncryptionA short presentation of the program(TM)s functions

TrueCrypt is a free software that encrypts data ***æon-the-fly•***.Right now the newest version released is version 4.3. You can create anencrypted hard drive, a separate partition or a directory withTrueCrypt. It doesn(TM)t simply encrypt the content of files, but theirnames and the names of the directories they are in as well. Moreoverthere is no way to check the size of the encrypteddirectory/HDD/partition. TrueCrypt is available for Windows and Linux.

Advantages of TrueCrypt:

- creates encrypted hard drive and mounts it,
- encrypts an entire drive, selected partition/directory and even USB flash drive,
- encryption is automatic, on-the-fly and transparent for user
- there is no way to check the size of the encrypted partition/directory,
- uses such encryption algorithms as: ***AES***-256, ***Serpent***, ***Twofish***,
- enables the creation of a hidden volume,
- in use you can(TM)t distinguish between the created volume and common data,
- it is very simple to use,
- the virtual drives created with TrueCrypt are completely independent of the operating system,
- authorization keys can be held on a USB stick.
- and much more¦

There are three ways to secure the encrypted data:

- with a password,
- with a special key,
- with both a password and a key.

What is this key? The key can be any file from your hard drive e.g.: ****.avi***, ****.mpg*** or ****.txt*** and even a whole directory containing a few files. ***Warning!Be***

careful using *.txt file as the key because if you modify it, thekey will change and you won(TM)t be able to decrypt your data.What happens when you lose your key? You will never recover your data!That(TM)s why I suggest using both, the key and the password as the bestway. In this case if you lose your key you can change it by enteringthe right password, and vice versa. Naturally, there is no idealsolution because you can forget your password and lose your key at thesame time.

A short comparison of TrueCrypt and DM-Crypt

In fact it is very difficult to say which of these programs isbetter. After a laborious review of the descriptions of their optionsand deliberations on both, I realized that the best solution would becombining the pair of them. They both enable you to create a so-calledœcontainer• which is an encrypted file that works like a directory inwhich you can store your private files (a very useful feature when youdon(TM)t want to encrypt the entire partition). The great advantage ofthese programs is that they can encrypt data while burning them on aCD/DVD. A slight disadvantage of TrueCrypt can be that after reloading the kernel you may have to install the TrueCrypt module again. On theother hand " in TrueCrypt you can simultaneously use differentencryption algorithms! It also runs under Windows so if you use bothsystems TrueCrypt will be a better choice.

How to choose the best key?

Personally I don(TM)t recommend choosing any file or directory fromyour hard drive as a key. The best way will be using a special keygenerator built-in to TrueCrypt. RNG - ***Random Number Generator*** - is the feature, it creates some random data with a maximum size of ***320 bytes*** and saves this to a previously chosen file. How is random data generated? If it is Linux, RNG uses ***/dev/random*** or ***/dev/urandom*** that represents all of the noise generated by devices plugged to your PC, such as the mouse and keyboard.

How does TrueCrypt work?

The entire encryption process is transparent to the user. Whencopying a file to the encrypted drive, its constituent fragments (if itis a big file such as a movie) are copied to RAM then encrypted andsaved to the destination file. The decryption process is the same.First the file, by fragments, is decrypted to RAM and next is passed onto a user. TrueCrypt never saves unencrypted data to the drive,encrypted data is always stored in RAM. This is a very secure methodthat prevents accidental access to your files.

TrueCrypt download

The newest version of the program you will always find on ***http://www.truecrypt.org***. TrueCrypt needs a tool called ***dmsetup*** to work correctly. ***Dmsetup*** is a tool enabling you to work with logical drives mapped with the ***device-mapper*** driver. The newest version of dmsetup is available on ***http://sources.redhat.com/dm/***. The first thing you have to do after downloading the source is to install dmsetup:

```
tar -zxvf device-mapper.
your_version_no
```

cd device-mapper.***your_version_no***
./configure
make
make install (as root or sudo)

If everything has gone well, try to install TrueCrypt:

```
tar -zxvf truecrypt-
your_version_no
```

cd truecrypt-***your_version_no***

Enter linux directory and install:

```
cd linux

./build.sh
```

```
Checking build requirements...
Building kernel module... Done.
Building truecrypt... Done.
```

First the script will check if your system fulfills all therequirements, it will prompt with information if it is not able to findthe location of a package.
Warning! To install TrueCrypt properly you have to have a kernel 2.6.5 or newer.

Next you run:

```
./install.sh
(as root or sudo)
```

```
Checking installation requirements...
Testing truecrypt... Done.

Install binaries to [/usr/bin]:     press [Enter]
Install man page to [/usr/share/man]: press [Enter]
Install user guide and kernel module to [/usr/share/truecrypt]: [Enter]
```

```
Allow non-admin users to run TrueCrypt [y/N]: to allow non-root users to use TrueCrypt press [y] else [N]
Installing kernel module¦ Done.
Installing truecrypt to /usr/bin¦ Done.
Installing man page to /usr/share/man/man1¦ Done.
Installing user guide to /usr/share/truecrypt/doc¦ Done.
installing backup kernel module to /usr/share/truecrypt/kernel¦ Done.
```

If everything proceeded as above you can continue.

The key generation

To generate a key type:

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

Of course you can choose another keyname, and the extension.

```
Is your mouse connected directly to the computer where TrueCrypt is running? Press œY•, then you will be prompted to move your mouse.
```

If everything was OK, the following text will be displayed: `Keyfile created.`

The virtual volume creation

To create a new volume you have to consider its name and type. There are only two types of such volume: ***normal*** and ***hidden***. What is the difference between them? The ***hidden*** is just that, hidden (the placement is different - more info on ***TrueCrypt homepage***).

In a terminal type:

```
truecrypt -c home.txt
```

You create a volume named `home.txt`. The extension is at the user(TM)s discretion, I(TM)ve chosen `*.txt`, because it is more difficult for a potential hacker to discover that it is a volume.

```
Volume type:
 1) Normal
```

```
 2) Hidden
  Select [1]: select 1

  Filesystem:
  1) FAT
  2) None
  Select [1]: select 2, because you will create other filesystem than FAT
 on your volume, default is FAT

  Enter volume size (bytes - size/sizeK/sizeM/sizeG): 10M -
  now you state a size for your volume, I have chosen 10 MB

  Hash algorithm:
  1) RIPEMD-160
  2) SHA-1
  3) Whirlpool
  Select [1]: choose hash, I suggest SHA-1, default is RIPEMD-160

  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]: choose the algorithm, default is AES

  Enter password for new volume ~home.txt(TM): press [Enter] if you don(TM)t want any password
```

Re-enter password: press [Enter] again

Enter keyfile path [none]: here enter a full path to the key or leave empty if you don(TM)t have any key

Enter keyfile path [finish]: you will be prompted again to enter the path. In case you have more than one key type another path, and if you have entered all the keypaths, leave empty and press [Enter]

TrueCrypt will now collect random data.

Is your mouse connected directly to the computer where TrueCrypt is running? Press œY• if your mouse is directly connected to your PC, but try pressing œn• and see what happens

Please type at least 320 randomly chosen characters and then press Enter: if you enter fewer than required the program will show you how many are missing

Now the program will start to create your volume. The time neededfor this operation depends on your CPU and the size of the volume. Thescript will let you know when it is complete (*Volume created*). Inroot(TM)s home directory there should be a file *home.txt*. You can try toopen it in a text processor, my congratulations if you manage to readanything from it.

Volume mapping and creation of the filesystem.

As you remember you didn(TM)t choose the filesystem for your volumeduring the creation process. That(TM)s why you have to do it now. This isrequired because TrueCrypt uses the Linux tool ***mount*** to mount a volume which needs to be passed a filesystem as an option.

Enter:

```
truecrypt /root/home.txt -k /root/key
```

Enter password for '/root/home.txt': if there is no password to this volume just press [Enter]

OK. To check if mapping has gone well type:

```
truecrypt -vl
```

(shows info about mapped devices)

If there is no info, it means that something has gone wrong.

Now you create a filesystem:

```
mkfs.ext3 /dev/mapper/truecrypt0
```

You can choose any filesystem

The filesystem has been created.

Mounting created volumes

Now when you have created a filesystem on your volume and mapped it, you can mount it to any directory.

To do this type:

```
truecrypt -d /dev/mapper/truecrypt0
```

unmaps the volume

```
mkdir encrypted -
```

creates a directory named œencrypted•, this is the directory where you are going to mount the volume

```
truecrypt /root/home.txt -k /root/key /root/encrypted
```

mounts volume to encrypted directories

Done! From now on all data saved in œencrypted• directory will be encrypted.

But what should you do to encrypt an already existing directory?This is very simple. Just move data from this directory then mountvolume to this directory and move the data back to this directory.Remember to make the volume suitably large when stating its size,because otherwise it won(TM)t accomodate all the data. The size of volumeshould be a little bit larger than the size of the directory.

Automatic mounting after the reboot.

As you will discover, after a reboot you will have to mount thevolume again. There is a simple way to do it. Browsing a forum onTrueCrypt homepage I picked up on two different solutions:

- adding a script to `/etc/init.d` or `/etc/rc.d`,
- create in the home directory a configuration file named ***.profile*** and edit it properly.

I suggest you to use the second way which I describe below. Why?There is one simple reason. Let(TM)s say you secured the volume with a keyand a password or even only with a password. In this case running bootscripts placed in ***init.d*** or ***rc.d*** directories you will have to init TrueCrypt with parameter ***-p*** and the password would be explicitly written there, which isn(TM)t thesmartest solution. This way anyone could read your password.

Maybe there is already a file ***.profile*** in your home directory, but if not:

```
touch .profile - creates a new file .profile
```

Open `.profile` in an editor and add the following line:

```
truecrypt /root/home.txt -k /root/key /root/encrypted
```

Savechanges and leave the editor. Now, for each time you log in to thesystem, TrueCrypt will prompt for your password (which you don(TM)t have because in this example you are identified only by the key, so just press [Enter]) and the virtual volume will be mounted.

Can I hold the key on a pendrive/USB stick?

Yes, there is such an option, and you can believe me it(TM)s not thatdifficult. The first thing you have to do is to automatically mount theUSB drive at startup. To do this you have to edit ***/etc/fstab***. Then create a new directory for the pendrive in ***/mnt***:

```
mkdir /mnt/pendrive
```

At first you have to see where the pendrive is in the system. Stickthe pendrive into the USB port and run the following command:

```
dmesg > output.txt
```

At the end of the file there should be a line like this:

```
usb 1-1: configuration #1 chosen from 1 choice
  uba: uba1
```

As you can see in my PC the USB drive is at */dev/uba1*. You may have it at */dev/sda**. Now you have to modify */etc/fstab*. Add this line:

```
/dev/uba1  /mnt/pendrive  auto  defaults  0  0
```

Then type:

```
mount /mnt/pendrive
```

Next step is to move the key to the USB drive and change the line in your *.profile* file containing the path to the key ***/mnt/pendrive***. Done!

Nowthe system mounts the virtual volume after the reboot automatically.What are the disadvantages of the automatic mounting? Let(TM)s say youhave a very curious sibling and you don(TM)t want them to have access tosome parts of your system (regardless of working on Windows or Linux).If you authorize with only the key, and it is placed somewhere on theHDD, then after boot the data is decrypted. œBut I hold my key on theUSB drive•. What if you forget to take it out of the PC after work?

The future

In the near future the developers of TrueCrypt are planning to extend its features:

- the MAC OS version,
- adding an exterior authorization (so there will be the possibility of decryption over the network/Internet),
- building an official GUI for TrueCrypt,
- and much more¦

Are there any unofficial GUI layers for TrueCrypt? Of course there are. I suggest you have a look at the following web page: ***TruecryptGUI at GoogleCode*** . For more information visit the ***TrueCrypt forum***.