May 2014 WMLUG Meeting

TrueCrypt

Patrick TenHoopen

TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

http://www.truecrypt.org/

TrueCrypt

TrueCrypt is software for establishing and maintaining an on-the-fly-encrypted volume (data storage device).

On-the-fly encryption means that data is automatically encrypted right before it is saved and decrypted right after it is loaded, without any user intervention.

No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys.

The entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).

Main Features

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed (pre-boot authentication).
- Encryption is automatic, real-time (on-the-fly) and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- Provides plausible deniability in case an adversary forces you to reveal the password.

Downloads

http://www.truecrypt.org/downloads

Installing TrueCrypt

From download directory, run as root:

```
./truecrypt-7.1a-setup-x86
```

Files installed:

/usr/bin/truecrypt

/usr/bin/truecrypt-uninstall.sh

/usr/share/applications/truecrypt.desktop

/usr/share/pixmaps/truecrypt.xpm

/usr/share/truecrypt/doc/License.txt

/usr/share/truecrypt/doc/TrueCrypt User Guide.pdf

Uninstalling TrueCrypt

Run as root:

```
/usr/bin/truecrypt-uninstall.sh
```

Plausible Deniability

In case an adversary forces you to reveal your password, TrueCrypt provides and supports two kinds of plausible deniability:

1. Hidden volumes and hidden operating systems.
2. Until decrypted, a TrueCrypt partition/device appears to consist of nothing more than random data (it does not contain any kind of "signature").

Keyfiles

A TrueCrypt keyfile is a file whose content is combined with a password. The user can use any kind of file as a TrueCrypt keyfile. The user can also generate a keyfile using the built-in keyfile generator.

Demos

Setting up an Encrypted File Container

Demos

Creating a Volume within a Partition or Drive

Demos

Setting up a Hidden Partition

Potential Issues

Error:

```
Failed to set up a loop device:
/home/pat/Documents/Test1
```

Solution:

Make sure loop module is running via modprobe loop.