!!! ACHTUNG - evtl. veraltet - ACHTUNG !!!

Diese Seite wurde zuletzt am 9. Juli 2014 um 08:58 Uhr geändert.

Allgemeines

TrueCrypt ist ein freies, quelloffenes und kostenlos verfügbares Programm zur Verschlüsselung von Festplatten, Teilen davon oder Wechseldatenträgern. Es läuft unter Windows ab Windows 2000, Linux (32 bzw. 64bit) und Mac OS X 10.4 und 10.5.

Installation

Unter Linux und Mac OS X setzt es das Kernel-Modul „fuse“ voraus. Jeder Benutzer im System, welcher TrueCrypt benutzen möchte, benötigt entsprechende Rechte, „fuse“ zu benutzen!

Es reicht die Binärdatei „truecrypt“ aus den entsprechenden unter http://www.truecrypt.org verfügbaren Paketen. Das Paket muss nicht installiert werden.

Fuse-Bibliothek installieren:

```
linux:~# aptitude install libfuse2
```

Benutzer der Gruppe „fuse“ hinzufügen:

```
linux:~# usermod -a -G fuse <LOGIN>
```

Entsprechendes Paket von http://www.truecrypt.org herunterladen, entpacken und ausführen (nur deb.-Archiv extrahieren).

```
linux:~# tar xvzf truecrypt-6.1a-ubuntu-x86.tar.gz
linux:~# ./truecrypt-6.1a-setup-ubuntu-x86
linux:~# dpkg -x /tmp/truecrypt_6.1a-0_i386.deb ~/truecrypt.i386
```

Sollte das nicht von Erfolg gekrönt sein, so steht unter http://www.debianforum.de/forum/viewtopic.php?f=29&t=102767&start=15#p658334 beschrieben, wie ein eigenes Archiv erstellt (kompiliert) werden kann.

Die grafische Oberfläche (identisch zu der unter Windows und Mac OS X) kann dann wie folgt aufgerufen werden:

```
linux:~# ~/truecrypt.i386/usr/bin/truecrypt
```

Verschlüsseltes Gerät ohne Verwendung von Keyfiles und ohne Formatierung mit einem Dateisystem als normaler Benutzer (hier wird davon ausgegangen, dass truecrypt im bin-Verzeichnis des Benutzers verfügbar ist) erstellen:

```
 user@linux:~$ ~/bin/truecrypt --text --create --keyfiles="" --volume-
type=Normal --encryption=AES --hash=RIPEMD-160 --filesystem=None /dev/sda1
```

Das verschlüsselte Gerät als Superuser „entschlüsseln“ (da noch kein Dateisystem enthalten ist, wird es nicht eingebunden):

```
 linux:~# ~/truecrypt.i386/usr/bin/truecrypt --text --keyfiles="" --protect-
hidden=no --filesystem=None /dev/sda1
```

Das entschlüsselte, virtuelle Gerät identifizieren:

```
 linux:~# ~/truecrypt.i386/usr/bin/truecrypt --text --list --verbose
```

Ein Dateisystem nach Wahl im entschlüsselten, virtuellen Gerät erstellen:

```
 linux:~# mkfs.xfs /dev/loop0
```

Die Entschlüsselung des Gerätes als Superuser wieder aufheben:

```
 linux:~# ~/truecrypt.i386/usr/bin/truecrypt --text --dismount /dev/sda1
```

Die Entschlüsselung als normaler Benutzer durchführen:

```
 user@linux:~$ mkdir geheim
 user@linux:~$ ~/bin/truecrypt --text --keyfiles="" --protect-hidden=no --
mount-options=nokernelcrypto /dev/sda1 ~/geheim
```

... Daten im Verzeichnis ~/geheim erstellen...

Die Entschlüsselung des Gerätes wieder aufheben:

```
 user@linux:~$ ~/bin/truecrypt --text --dismount /dev/sda1
```

Identifizierung

Kernel-Module

Um es benutzen zu können, müssen folgende Kernel-Module geladen sein:

```
 linux:~# lsmod | egrep fuse
```

Prozesse

Gibt es einen TrueCrypt-Prozess?

```
 linux:~# ps -A | egrep truecrypt
```

Welcher Dateien hat der Prozess „truecrypt“ offen:

```
linux:~# lsof | egrep truecrypt | egrep /dev/ | egrep -v
"/dev/[[null|fuse]]"
```

Geräte/Dateien

Bezüglich der Erkennung, welche Geräte eingebunden sind, ob verschlüsselt oder nicht und ob es große, „auffällige“ Dateien gibt, die als Container dienen könnten, wird auf die o. a. Ausführungen zu dm-crypt inkl. LUKS verwiesen.

Einen per TrueCrypt verschlüsselten Container kann man jedoch nicht als solchen (Verschlüsselung per TrueCrypt) selbst identifizieren!

Existiert in dem Verzeichnis /tmp eine versteckte Datei „.truecrypt_aux_mnt*X*“ (sind mehrere verschlüsselte Geräte eingebunden, so existieren mehrere solcher Dateien. *X* entspricht einer fortlaufenden Zahl)?

```
linux:~# ls -la /tmp/.truecrypt_aus_mnt*
```

Existiert ein verstecktes Verzeichnis „.TrueCrypt“ im Heimatverzeichnis eines Benutzers?

Logdateien

Analog zu den Ausführungen zu dm-crypt inkl. LUKS.

Verschlüsselungsprogramm

Die binäre Datei „truecrypt“ kann umbenannt werden. Sie funktioniert weiterhin wie gehabt. Neben dem Namen ändert sich auch der Prozess-Name zum Zeitpunkt der Ausführung!

Informationen über aktuell eingebundene, verschlüsselte Geräte können wie folgt abgerufen werden:

```
linux:~# truecrypt --text --list
```

Sind keine Geräte eingebunden, erfolgt eine leere Ausgabe!