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

Diese Seite wurde zuletzt am 9. Juli 2014 um 10:29 Uhr geändert.

Allgemeines

Dm-crypt ist ein Kryptographie-Modul des Device Mappers, welches seit Version 2.6.4 (2.6.5 wird jedoch empfohlen) im Linux-Kernel enthalten ist.

Eine gängige Erweiterung ist LUKS („Linux Unified Key Setup“), welche die verschlüsselten Daten um einen zusätzlichen Header erweitert, in dem Metadaten, sowie bis zu acht Schlüssel gespeichert werden. Vorteile gegenüber „reinem“ dm-crypt sind: ein standardisiertes Format, Informationen über die Art der Verschlüsselung im Header, Vergabe von bis zu acht Schlüsseln sowie die Änderung von Schlüsseln. Dm-crypt kann jedoch auch ohne LUKS benutzt werden!

Hinweis:

Das Passwort für eine Swap-Partition wird bei jedem Start per Zufallsgenerator neu generiert!

Installation

Debian-Pakete installieren:

```
linux:~# aptitude install cryptsetup
```

Verschlüsseltes (virtuelles) Gerät „einfachst“ erstellen:

```
linux:~# cryptsetup luksFormat /dev/sda1
```

Verschlüsseltes Gerät „entschlüsseln“:

```
linux:~# cryptsetup luksOpen /dev/sda1 decrypted_sda1
```

Dateisystem (XFS) im entschlüsselten Gerät erstellen:

```
linux:~# mkfs.xfs /dev/mapper/decrypted_sda1
```

entschlüsseltes Gerät einbinden:

```
linux:~# mkdir /mnt/geheim
linux:~# mount /dev/mapper/decrypted_sda1 /mnt/geheim
```

… Daten im Verzeichnis /mnt/geheim erstellen…

entschlüsseltes Gerät trennen:

```
linux:~# umount /mnt/geheim
```

„Entschlüsselung“ aufheben:

```
linux:~# cryptsetup luksClose decrypted_sda1
```

Identifizierung

Kernel-Modul(e)

Um es benutzen zu können, müssen folgende Kernel-Module geladen sein: linux:~# lsmod | egrep dm_crypt linux:~# lsmod | egrep aes linux:~# lsmod | egrep sha256

Geräte/Dateien

Sind verdächtige Geräte eingebunden?

```
linux:~# mount
```

oder

```
linux:~# cat /proc/mounts
linux:~# cat /etc/fstab
```

Im Verzeichnis /sys/block/dm-X/slaves/ (X steht für die Zahl, die das virtuelle „entschlüsselte“ Gerät hat) ist der „Verweis“ auf das Ursprungs-Gerät gespeichert.

```
linux:~# hexdump -C -n 512 /dev/mapper/decrypted_sda1
```

Hier sollte ein unverschlüsseltes Dateisystem zu erkennen sein...

xfs:

```
linux:~# hexdump -C -n 3 <DEVICE>
```

reiserfs:

```
linux:~# hexdump -C -s 0x00010034 -n 9 <DEVICE>
```

ext2 bzw. ext3 kann so offensichtlich nicht erkannt werden, man kann jedoch erkennen, dass es sich nicht um verschlüsselte Daten handelt!

Im Fall von cryptsetup + LUKS sind die ersten vier Zeichen „LUKS“ und der Rest ein verschlüsseltes Durcheinander:

```
linux:~# hexdump -C -n 512 <DEVICE>
```

Gibt es „größere“ Dateien (z. B. größer als 1GB) im System, welche als Container dienen könnten?

```
linux:~# ls -laS $(find / -type f -size +1000000k)
```

Diese Dateien sollten per hexdump als verschlüsselt bzw. nichtverschlüsselt identifiziert werden können!

Logdateien

Sind in Logdateien hinweise zu Ereignissen (z. B. laden/entladen von Kernel-Modulen, einbinden/trennen von Geräten,...) vorhanden?

Verschlüsselungsprogramm

Informationen über verschlüsselte Geräte können abgerufen werden:

```
linux:~# cryptsetup status <**ENT**SCHLUESSELTES_DEVICE>
```

oder

```
linux:~# cryptsetup luksDump <**VER**SCHLUESSELTES_DEVICE>
```