

Tuesday, August 11. 2015

Wie man Katastrophen abwendet, heute: LÄŸschen von LUKS-SchlÄŸsseln

Ich bin deutlich zu experimentierfreudig.

Ich habe vor einiger Zeit meinem Laptop beigebracht, die verschlÄŸsselte LUKS-Partition nicht nur ÄŸber eine Passphrase, sondern auch ÄŸber eine (andere) Passphrase, gepaart mit meinem Yubikey zu entschlÄŸsseln.

Das hat sich heute gerÄŸcht, weil ich den Yubikey fÄŸr andere Zwecke umkonfiguriert hatte. Ich dachte dann, diesen Slot in LUKS iÄŸschst Du mal.

DafÄŸr muss man immer noch ein funktionierendes Passwort angeben.

Dumm nur: Es wurde das Passwort gelÄŸscht welches ich eingegeben hatte. Ganz dumme Geschichte - damit wÄŸre beim nÄŸchsten hochfahren das System nicht mehr hochgekommen, weil kein EntschlÄŸsselungs-SchlÄŸssel mehr bereit gewesen wÄŸre; den initialen hatte ich gerade gelÄŸscht und der Yubikey hatte andere Werte.

Was tun fragte ich mich, besonders weil eine Suchmaschinen-Suche auf diese Fragestellung keine eindeutige Antwort gab. Ich sah mich schon alles Backuppen, formatieren und restoren (oder - wenn ich gut drauf gewesen wÄŸre - neues Device mit luks anlegen, dd if.. of ... von A nach B schieben).

Mein GlÄŸck ist, dass das Laufwerk ja noch online und damit geÄŸffnet ist. Auch der Master-Key ist (fÄŸr root) auslesbar.

Zugschluss ist gerade auf der DebConf und hat Margarita ManterolagegenÄŸber sitzen. Und sie kennt luks sehr gut. Ich weiss nicht ob sie aus Erfahrung spricht, aber sie hat den richtigen Tip gehabt:

```
# cryptsetup luksAddKey $device_name --master-key-file
```

Posted by rince at 17:34

Zum VerstÄŸndnis:

Luks hat den master key unencrypted und auslesbar im Speicher und ein tool um ihn auszulesen. Als Angreifer der irgendwie temporÄŸr root bekommt reicht also ein kommando um offline die platte zu decrypten, wenn der Rechner ausgeschaltet wurde.
Anonymous on Aug 11 2015, 18:38

Brauchst Du Dir nicht merken, wirst Du nie wieder brauchen.

Anonymous on Aug 12 2015, 10:09

Das wird wohl nicht anders gehen wÄŸhrend das Device aufgeschlossen ist.

Anonymous on Aug 12 2015, 10:10