# Verschlüsselung unter *NIX

Eine kleine Einführung


lutz.willek@belug.de

# Verschlüsselung unter *NIX

## Agenda

- Über mich
- Warum verschlüsseln
- Überblick der Methoden, Vorteile, Nachteile
- Etwas graue Theorie
- Beispiel Linux: Cryptsetup, /home verschlüsseln
- Anleitung: Verschlüsseln eines USB-Sticks


lutz.willek@belug.de

# Über mich

Lutz Willek <lutz.willek@belug.de> https://belug.de/~lutz/pub/vortrag/20090418/

- 1984-1994: Realschule
- 1994-1998: Berufsausbildung Gas-Wasser Installateur (Heizung, Spengler)
- 1998-2004: Arbeiten im Ausbildungsberuf, als Lagerverwalter, Bundeswehr
- 2004-2006: Studium zum Techniker: Heizung- und Klimatechnik
- Ab 2006: Netzwerk- und Anwendungsadministrator
- Angestellt bei s+c http://www.science-computing.de/ im IT-Service Berlin

- 1986: Arbeitsgruppe „Elektronikfreunde“
- 1987: meine erstes selbst gebautes Radio, Arbeiten mit KC 85-2
- 1989: mein erster selbst gebauter Fernseher
- 1990: weg von Elektronik, hin zu Computertechnik
- 1991: mein erster eigener PC (PC 286-XT, langsam und teuer..)
- 1991-1999: DOS, Windows 3.x, 95, 98, 2000, der übliche Weg
- 1997: erster Kontakt mit Linux durch CD- Beilage einer Computerzeitschrift
- Ab 2000: Linux als Hauptsystem
- 2005: Berufliche Umorientierung, arbeiten als „Techieh“ http://Xtops.de/

# Warum Verschlüsseln

Vorteile
- Schutz bei Verlust oder Diebstahl
- Schutz der vertraulichen oder privaten Daten
- Einfache Vernichtung von Daten
- Weil man es kann :-)

Nachteile
- Aufwand
- Portierbarkeit
- Schnelligkeit


lutz.willek@belug.de

# Methoden

Dateien: PGP, GPG, Crypto-FS, Enc-FS,...

Geräte: Loop-AES, DM-Crypt, Truecrypt, Cryptsetup-Luks, CGD, …

Zum Nachlesen:

http://www.linux-magazin.de/heft_abo/ausgaben/2006/10/loechriger_kaese
http://net-tex.dnsalias.org/~stefan/nt/netbsd/advocacy/guug-uptimes-cgd_cfs.pdf
http://www.linux-magazin.de/layout/set/print/content/view/full/2702
http://www.saout.de/misc/dm-crypt/

# Theorie

Cryptsetup

- Verschlüsselungssoftware, setzt auf Device-Mapper des Kernels auf
- Schlüsselgenerierung und Verschlüsselungsverfahren beeinflussbar
  - dh. beliebig lange Passwörter wählbar
  - die Daten werden mit 256Bit Schlüssel verschlüsselt

Nachteil:

- Trennt Informationen wie die Daten verschlüsselt sind von den Informationen selbst, dh. die Parameter stehen unverschlüsselt in Skripten und Konfigurationsdateien.
  - **Sind diese Informationen weg sind auch die Daten verloren**

# Theorie

CryptsetupLuks

Linux Unified Key Setup Managementtool

- setzt Masterkey ein
  - der Hash und damit das Passwort kann beliebig geändert werden
  - mehrere Passwörter möglich
- Wird erreicht durch  Passwortmanagement- Schicht, die die Daten schützt

- Spart viel Zeit und Nerven bei Änderung des Passwortes
- Auch für andere Betriebssysteme einsetzbar

# Theorie

CryptsetupLuks

Linux Unified Key Setup Managementtool

Definiert Header für DMCrypt Partitionen, in dem alle Informationen für die Schlüsselableitung, sowie Algorithmus und Modus enthalten sind. Der Header ist Teil der verschlüsselten Partition, somit sind diese Informationen immer vorhanden.

# Theorie

CryptsetupLuks

Linux Unified Key Setup Managementtool

Setzt statt „Ripemd160“ „PBKDF2“ zur Hashbildung ein
(Password Based Key Derive Function, Version 2)

Antiforensische Informationsspeicherung, ermöglicht salting und stretching

**AFSplitter stretching**: absichtlich rechenintensive Funktion zur Berechnung eines Hashwertes (Wörterbuchangriffe)
**Salting**: zufällige Zeichenkette hinter jedem Passwort, diese Zeichenkette wird Klartext im Partitionsheader gespeichert

# Theorie

Watermarkingangriffe

• gleicher Klartext führt zu gleichem Schlüssel

ECB: Electronic Code Book

Na und?

LRWAES: Liskov, Rivest, Wagner Advanced Encryption Standard
CBC: Cipher Block Chaining
ESSIV: Encryptet SaltSector Initial Vector

# Theorie

Watermarkingangriffe

• gleicher Klartext führt zu gleichem Schlüssel

ECB: Electronic Code Book

Na und?

LRWAES: Liskov, Rivest, Wagner Advanced Encryption Standard
CBC: Cipher Block Chaining
ESSIV: Encryptet SaltSector Initial Vector

```
cryptsetup -c aes-cbc-essiv:sha256 ...
```


lutz.willek@belug.de

# Verschlüsseln von /home

```
cryptsetup -c aes-cbc-essiv:sha256 -y -s 256 luksFormat /dev/sdb5
cryptsetup luksOpen /dev/sdb5 crypt
mkfs.ext3 /dev/mapper/crypt

mount /dev/mapper/crypt /home2
rsync -aH /home/* /home2
umount /home2 ; umount /home
mount /dev/mapper/crypt /home    #Zeile in /etc/fstab ändern
cryptsetup luksClose crypt

cryptsetup luksAddKey /dev/sdb5
cryptsetup luksDelKey /dev/sdb5 0
```


lutz.willek@belug.de