



# einleitung

- ich bin **kein** crypto experte
- dieser vortrag konzentriert sich daher auf die **anwendung** von verschlüsselten filesysteme unter linux

bei der frage nach zu verwendenden ciphern kann ich nur wiedergeben was ich selber gelesen habe

- **blowfish**
- plainIV gilt als zu voraussagbar, dh. cipher block chaining verwenden (wie wird erläutert)

## verschiedene ansätze

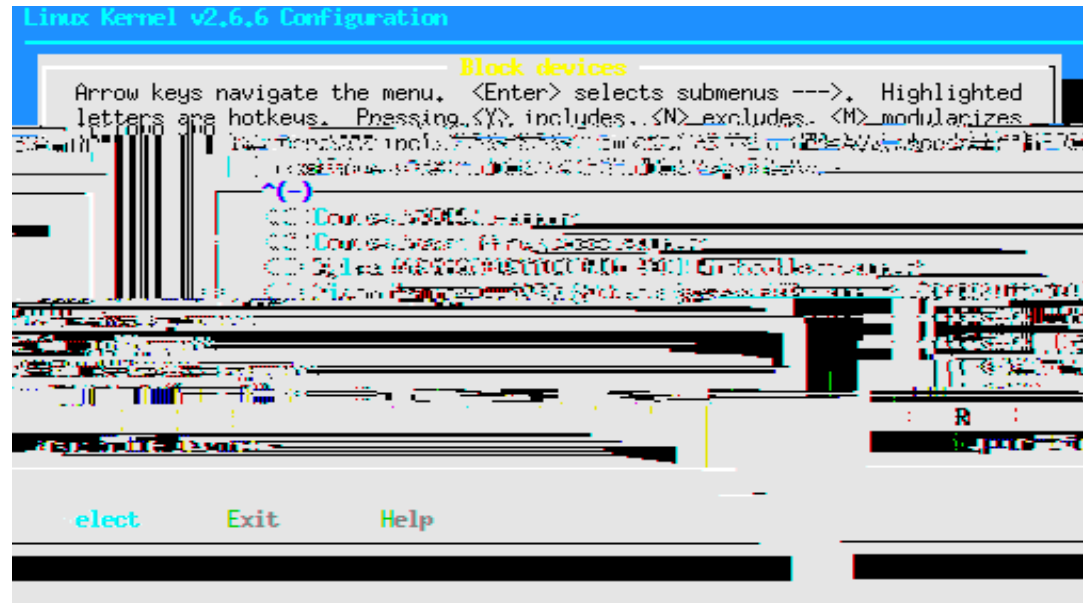
**crypto loop** ehemaliger kernel patch, seit version 2.4.22 sind ciphli in den kernel integriert, mit kernel 2.6 auch crypto loop.

**dm-crypt**



verschl

# cryptoloop - kernel config





## cryptoloop - losetup patchen

util-linux 2.12 sollte die crypto funktionen eigentlich unterstützen, ist aber broken.

<http://www.paranoiacs.org/sluskyb/hacks/util-linux/losetup-combined.patch>

<http://www.ece.cmu.edu/rholzer/cryptoloop/util-linux-2.12-kernel-2.6.patch>

- gentoo inclut diese patches in der distribution
- util-linux muss nicht komplett neu übersetzt und install20kt werden
- `make lib losetup` und `kop20ken deslosetup binaries nach /sbin reicht`







# cryptoloop - passwörter ändern

- loop device `/dev/loop0` mit altem passwort aktivieren
- 2. loop device `/dev/loop1` mit neuem passwort aktivieren
- `dd if=/dev/loop0 of=/dev/loop1`







# dm-crypt - benutzung



einrichten:

verschl

# cryptoloop und dm-crypt

-

# encrypted swap und tmp

-

# swap und tmp mit cryptoloop

```
#!/bin/sh

# loop device fuer /tmp
# in der fstab wie folgt eintragen:
# /dev/loop0 /tmp ext2 defaults,nodev,nosuid,noexec 0 0
/bin/dd if=/dev/urandom bs=1c count=32 |\
/sbin/losetup -p0 -aes-256-cbc /dev/loop0 /dev/hda2
/sbin/mkfs.ext2 /dev/loop0

# loop device fuer swap
# in der fstab wie folgt eintragen:
# /dev/loop1 none swap sw 0 0
/bin/dd if=/dev/urandom bs=1c count=32 |\
/sbin/losetup -p0 -aes-256-cbc /dev/loop1 /dev/hda3
/sbin/mkswap /dev/loop1
```





**pam**

# pam\_mount - beispiel

- `/etc/security/pam_mount.conf` snippet  
(note: eine zeile)

```
volume rupi local - /dev/hda6 /home/rupi  
loop,user,exec,encryption=blowfish-cbc-256 aes-256-ecb /home/.rupi.key
```





# bash\_profile - beispiel

- fstab sniplet

```
/dev/hda6 /home/rupi ext2 user,loop,encryption=aes-cbc-256,noauto 0 0
```

- bash\_profile unencrypted

```
openssl enc -d -aes-256-ecb -in /home/rupi/.key | \
```

# bash\_profile - beispiel


## tmp und ehd

- encrypted /tmp ist nur tw. eine lösung - multiuser rechner, login server die nicht rebooted werden
- ausweg: anlegen eines eigenen tmp dirs innerhalb des ehd
- env var \$TMPDIR
- alle programme die auf `tempnam` funktion setzen respektieren das
- nachteil: es gibt programme die `/tmp` hardcoded verwenden
- manchmal braucht mensch temp space ausserhalb des ehd (performance, platz)

verschl



# backup und ehd

- cleartext backups sind contraproduktiv
- das verschlüsselte device / file backupen unter umständen nicht adequat (incremental backup)
- 

## resources

- linux-crypto mailingliste  
<http://mail.nl.linux.org/linux-crypto/>
- cryptoloop howto  
<http://gd.tuwien.ac.at/opsys/linux/LDP/HOWTO/Cryptoloop-HOWTO/index.h>
- cryptoloop migration guide  
[http://clemens.endorphin.org/Cryptoloop\\_Migration\\_Guide](http://clemens.endorphin.org/Cryptoloop_Migration_Guide)

**auf wiedertschüss,**