# Loopback Encrypted Filesystem HOWTO

Copyright by Ryan T. Rhea, rhear@cs.winthrop.edu
Vertaler: *Reggy Ekkebus*, *reggy@zeelandnet.nl* v1.1, 29 November 1999

Dit document verteld hoe je een filesysteem moet instellen dat, als het gemount is door een gebruiker, drastisch en transparant zijn inhoud versleuteld. Het filesysteem wordt bewaart in een reguliere file, welke verborgen of on opvallend genoemd kan zijn zodat de meeste mensen er over kijken. Dit staat een hoog niveau aan veilige data opslag toe.

## Inhoudsopgave



## 1 Voordat je begint

Dit proces vereist de kernel bron code, kennis van over hoe je deze code moet compileren, en veel geduld. Ik raad je aan om een bootdisk klaar te hebben liggen. Wees ook zeker dat je een backup hebt voordat je permanent je belangrijke data bewaard in het versleutelde filesysteem - het kan aangestast worden als elk ander filesysteem.

Als een minimum, moet je de laatste versie 2.2.9 van de linux kernel patchen voordat je door kan gaan. Er is een verdere instructie over het patchen in de 4 () sectie later in dit document.

De source code van de kernel kan gevonden worden op:

`<ftp://ftp.kerneli.org/>`

Er is een HOWTO over het proces van een kernel hercompileren op:

`<http://metalab.unc.edu/LDP/HOWTO/>`

Dit document mag worden gereproduceerd en gedistributeerd in zijn geheel of in delen, zonder betaling, overgegeven aan de volgende voorwaarden:

- De copyright notitie en de permissie notitie moet geheel bewaard blijven op alle komplete of gedeeltelijke kopieën.
- Elke vertaling of afgeleide werk moet toegstaan zijn door de auteur van het document voor distributie.
- Als je dit werk in een deel distributeerd, moet er een instructie aanwezig zijn over hoe je de hele howto kunt verkrijgen.

- Alle source code in dit document is geplaatst onder de GNU General Public License, verkrijgbaar via anonieme FTP van:

  <ftp://prep.ai.mit.edu/pub/gnu/COPYING/>

# 2 Introductie

Het proces gebruikt het device '/dev/loop*' (waar * 0-7 kan zijn bij de meeste installaties) om een loopback filesysteem te mounten. Het zelfde proces kan worden gebruikt om een linux filesysteem te bewaren op een niet-linux partitie. Er is een HOWTO over dit op de LDP site eerder aangegeven.

Er kunnen verschillende types van encryptie gebruikt worden, zoals XOR, DES, twofish, blowfish, cast128, serpent, MARS, RC6, DFC en IDEA. Het programma 'losetup' (loopback setup) is wat je versleutelde file systeem associeert met een filesysteem en zijn versleutel type. Overeenkomstig met Alexander Kjeldaas, die de kerneli.org site onderhoud en de internationale crypto patches, DES en losetup zijn momenteel niet samengaand. Dit is door het verschil van het hanteren van parity bits. Er zijn geen plannen om DES te ondersteunen omdat het veel minder veilig is dan de andere methoden.

Twofish, blowfish, cast128 en serpent zijn vrij te gebruiken. De anderen hebben of hebben geen licentie beperkingen. Vele van deze zijn kandidaten voor de AES standaard. De finalisten zullen vrij gebruik van hun versleutelaars wereldwijd verstrekken.

Dit document gebruik het serpent algoritme omdat het erg sterk is en ongelooflijk snel, en het is vrij distributeerbaar onder de GPL. Overeenkomstig aan de documentatie gebruik serpent 128-bit blok versleuteling gemaakt door Ross Anderson, Eli Biham en Lars Knudsen. Het geeft gebruikers het hoogste practische niveau van beveiliging dat er geen korte aanvallen worden gevonden. De documentatie over serpent en ook de source code kan gevonden worden op:

<http://www.cl.cam.ac.uk/~rja14/serpent.html>

Dit document neemt ook aan dat de algoritmes direct in de kernel zijn gecompileerd. Je mag ze installeren als een module, maar de techniek wordt niet besproken in dit document. Je moet de file '/etc/conf.module' editten; het proces wordt in detail beschreven in de Kernel compilatie HOWTO erdeer angegeven.

# 3 Samenvatting

Er zijn veel stappen betrokken in het proces. Ik geef 4 () voor deze stappen in de volgende sectie. Ik dacht dat het wel leuk zou zijn om eerst een referentie te geven (als je ervaren bent met unix/linux heb je de details niet nodig). Hier zijn ze beknopt:

1. Download de nieuwste internationale crypto patch (Ik gebruikte 'patch-int-2.2.10.4' toen ik document schreef) van:

   <http://ftp.kerneli.org/pub/kerneli/>

2. Patch de kernel
3. Draai 'config' (of 'menuconfig' of 'xconfig') om je MakeFile voor de nieuwe kernel te configureren. De opties om versleuteling aan te zetten zijn verspreid. Eerst, voordat je andere opties ziet moet je eerst 'Prompt for development and/or incomplete code/drivers' aanzetten in het 'Code Maturity level options' menu. Onder 'Crypto opties' 'crypto ciphers' en 'serpent' aanzetten. Nog een keer, dit

document neemt aan dat je serpent gebruikt, maar probeer wat je wilt. Onthoud dat DES bekent is als onsamengaand met 2.2.10.4 - het wordt misschien wel nooit ondersteund. Er zijn verschillende belangrijke opties die je moet selecteren onder 'Block Devices'. Deze zijn 'Loopback device support', 'Use relative block numbers as basis for transfer functions (RECOMMENDED)' en 'General encryption support'. Selecteer NIET 'cast 128' of 'twofish' versleuteling hiet. Weet ook dat je de verschillende crypto opties onder de verschillende netwerk catagorieen niet nodig hebt. Ik ga niet verder in het configureren van de kernel, dat is buiten beschouwing van dit document en kan gevonden worden op de LDP site.

4. Compileer de nieuwe kernel.

5. Verander '/etc/lilo.conf' om het nieuwe kernel image toe te voegen. Draai 'lilo -v' om de kernel toe te voegen aan de boot lader.

6. Download de source van de nieuwste 'util-linux' (Ik gebruikte 'util-linux-2.9v') van:

   `<ftp://ftp.kernel.org/pub/linux/utils/util-linux/>`

7. Pak de 'util-linux' source uit.

8. Pas de daarbij behorende patch in je '/usr/src/linux/Documentation/crypto/' directory toe.

9. lees de 'INSTALL' file ZORGVULDIG! Dit pakket houdt de source code van veel systeem afhankelijke files in (belangrijke tools zoals 'login', 'passwd' en 'init'). Als je de MCONFIG file niet zorgvuldig veranderd, voordat je deze bron code gaat compileren zorg dan dat je een boot diskette en/of een shotgun bij de hand hebt, omdat je systeem erg in de war zal zijn. Fundementeel zul je de meeste van de 'HAVE_*' velden op 'yes' zetten zodat de belangrijkste authenticatie tools niet worden gecompileerd en dus ook niet overschreven. De tools die je moet hercompileren zijn 'mount' en 'losetup' om de nieuwe encryptie schema's onder te brengen. Ik raad je aan om naar de 4 () sectie hieronder te gaan voor deze stap.

10. Compileer en installeer de 'util-linux' source

11. Reboot de machine met de nieuwe kernel.

12. Verander '/etc/fstab', een regel toevoegen voor je mount punt gaat als volgt:

```
/dev/loop0  /mnt/crypt  ext2  user,noauto,rw,loop 0 0
```

13. Maak de directory aan die het filesysteem gaat inhouden, zoals in '/mnt/crypt' hierboven.

14. Als de gebruiker, maak je versleutelde file als volgt:

    ```
    dd if=/dev/urandom of=/etc/cryptfile bs=1M count=10
    ```

15. Draai losetup als volgt:

    ```
    losetup -e serpent /dev/loop0 /etc/cryptfile
    ```

    Je hebt maar een kans om het paswoord in te vullen, dus wees voorzichtig. als je je paswoord twee keer wilt laten controleren, kun je het volgende commando gebruiken:

    ```
    losetup -d /dev/loop0
    ```

    Dit deactiveert je loop device. Daarna draai je losetup opnieuw om je paswoord te testen, als volgt:

    ```
    losetup -e serpent /dev/loop0 /etc/cryptfile
    ```

16. Maak je ext2 filesysteem als volgt:

```
mkfs -t ext2 /dev/loop0
```

17. Nu kun je je versleutelde filesysteem mounten met:

```
mount -t ext2 /dev/loop0 /mnt/crypt
```

18. Als je klaar bent, kun je je filesysteem unmounten en beschermen als volgt:

```
umount /dev/loop0
losetup -d /dev/loop0
```

# 4 Details

**Kernel Patches:**

Je kan upgraden van '2.2.x' uitgaven met een patch. Elke patch die voor '2.2.x' is uitgebracht bevat bug verbetering. Nieuwe kenmerken worden toegevoegd aan de Linux '2.3.x' ontwikkelings kernel. Om te installeren door een patch, haal de nieuwste patch files en doe het volgende:

```
cd /usr/src
gzip -cd patchXX.gz | patch -p0
```

verander de xx voor alle versies groter dan de versie van je momentele bron boom, IN VOLGORDE.

De standaard directory voor de kernel source is '/usr/src/linux'. Als je source ergens anders staat raad ik een symbolische link aan van '/usr/src/linux'.

**De 'MCONFIG' file vervanderen voor de 'util-linux' package compilatie:**

De volgende zijn uittreksels van de 'MCONFIG' file die ik heb gebruik om het 'util-linux' pakket te compileren. Dit is bijna identiek aan mijn setup, welke losjes is gebaseerd op RedHat 5.2. Het punt is dat je geen belangrijke systeem tools gaat overschrijven zoals 'login', 'getty', of 'passwd'. Hoe dan ook, hier zijn de belangrijke regels als volgt:

---

```
CPU=$(shell uname -m | sed s/I.86/intel/)

LOCALEDIR=/usr/share/locale

HAVE_PAM=no

HAVE_SHADOW=yes

HAVE_PASSWD=yes

REQUIRE_PASSWORD=yes

ONLY_LISTED_SHELLS=yes

HAVE_SYSVINIT=yes

HAVE_SYSVINIT_UTILS=yes

HAVE_GETTY=yes

USE_TTY_GROUP=yes
```

```
HAVE_RESET=yes

HAVE_SLN=yes

CC=gcc
```

**Suggesties:**

Onthoud dat je elke van de acht loopback devices kunt gebruiken, van '/dev/loop0' tot '/dev/loop7'. Gebruik een onopvallende directory voor het mount punt. Ik raad aan een directory te maken met 700 permissies in je home directory. Het zelfde geld voor de file waar de data in staat. Ik gebruik een filenaam als 'sysfile' of 'config.data' in de '/etc/' directory. Deze worden meestal over het hoofd gezien.

Ik heb erg simpele Perl scripts gemaakt om het filesysteem te mounten en weer te unmounten met een commando. Schrijf deze, maak ze uitvoorbaar (chmod u+x), en zet ze in je path.

```
#!/usr/bin/perl -w
#
#minimaal programma om een loopback encrypted filesysteem in te stellen.
#Copyright 1999 door Ryan T. Rhea
`losetup -e serpent /dev/loop0 /etc/cryptfile`;
`mount /mnt/crypt`;
```

Noem het bovenstaande script 'loop' en dan kun je starten met een commando ('loop') en een paswoord.

```
#!/usr/bin/perl -w
#
#minimaal utility om een loopback encrypted filesysteem te deactiveren.
#Copyright 1999 door Ryan T. Rhea
`umount /mount/crypt`;
`losetup -d /dev/loop0`;
```

Noem de tweede 'unloop' en als je dan 'unloop' typt wordt je filesysteem snel gedeactiveerd.