

Linux CryptoFS

Petr Novický
<P.Novicky@sh.cvut.cz>

Osnova přednášky

- Loop-AES
 - Úvod
 - Příprava, kompilace, instalace
 - Použití
 - Diskový oddíl
 - Soubor
 - Diskový oddíl s použitím „semínka“
- Závěr

Loop-AES (úvod)

- šifrovaný filesystem založený na loopback zařízení (jako CryptoAPI)
- pro práci s loopback zařízením používáme program losetup
- balíček Loop-AES obsahuje modul (loop.o) pro podporu loopback zařízení
- pro kernely řady 2.0, 2.2, 2.4 (2.4.7 a pozdější), nejnovější řada 2.6 by měla být podporována rovněž (neověřeno!)
- ověření heslem (minimálně 20 znaků), bezpečnost může být zvýšena použitím „semínka“ (viz. dále)

Loop-AES (úvod)

Typ šifrování	Hashovací funkce	Použitá šifra
AES128	SHA-256	128b AES
AES192	SHA-384	192b AES
AES256	SHA-512	256b AES

- použití žurnálovacího filesystemu v případě filesystemu v souboru je doporučeno pouze v případě, že i filesystem, kde je soubor uložen má v sobě žurnál
- Klíč uchováván v RAM počítače (okamžitě vymazán, když už není potřeba)
- Nepoužívat suspend-to-disk v případě aktivního šifrovaného filesystemu (velké bezpečnostní riziko)!!

Instalace Loop-AES (příprava)

Zdroje:

URL: `http://loop-aes.sourceforge.net/`

Soubor: `loop-AES-latest.tar.bz2`

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

Soubor: `util-linux-2.12pre.tar.bz2`

Instalace Loop-AES (kernel)

Nutné volby kernelu:

Podpora modulů: `CONFIG_MODULES=y`

(Loadable module support->Enable loadable module support)

Podpora loopback zařízení: `CONFIG_BLK_DEV_LOOP=n`

(Block devices->Loopback device support)

! Tato volba musí být vypnutá, jinak Loop-AES nebude fungovat !

Nepovinné volby kernelu:

Automatické náhrávání modulů: `CONFIG_KMOD=y` (nepovinné)

(Loadable module support->Kernel module loader)

Instalace Loop-AES (kernel)

Důvody proč kompilovat nové jádro:

- 1) Deaktivovat podporu loopback zařízení v kernelu.
- 2) Kvůli přizpůsobení zdrojových souborů kernelu použitému kernelu.
- 3) Kvůli přizpůsobení souboru **.config** použitému kernelu.
- 4) Kvůli přizpůsobení linků generovaných při konfiguraci kernelu.
- 5) Kvůli přizpůsobení hlavičkových souborů generovaných při kompilaci kernelu.

Instalace Loop-AES (cesty)

Vyhledávání zdrojových souborů kernelu, probíhá postupně v adresářích:

```
/lib/modules/`uname -r`/build
```

```
/usr/src/linux
```

```
/usr/src/linux-`uname -r`
```

```
/usr/src/kernel-source-`uname -r`
```

Nastavení cesty pomocí proměnné prostředí LINUX_SOURCE

```
LINUX_SOURCE=/moje/podivna/cesta/ke/zdrojakum
```

Vždy je nejlepší tuto cestu explicitně zadat!

Instalace Loop-AES (cesty)

Nastavení kořenového adresáře použitého při instalaci. Pomocí proměnné prostředí `INSTALL_MOD_PATH`

```
INSTALL_MOD_PATH=/cesta/k/cilovemu/root/adresari
```

Makefile zjistuje při instalaci typ procesoru. V případě, že se jedná o Pentium nebo lepší x86 procesor se použije optimalizovaná implementace v assembleru.

Pokud se jedná o x86 procesor starší než Pentium nebo je jedná o jinou architekturu, použije se defaultní implementace v programovacím jazyce C.

V případě potřeby můžeme použití optimalizované implementace v assembleru potlačit nastavením proměnné prostředí `PENTIUM_ASM`:

```
PENTIUM_ASM=n
```

Instalace Loop-AES (kompilace)

Pokud máme vše správně nastavené Loop-AES zkompilujeme a nainstalujeme příkazy (pod uživatelem root):

```
# make clean  
# make
```

Posledním příkazem vytvoříme modul loop.o, který je obvykle nainstalován do adresáře /lib/modules/`uname -r`/block

Pro použití Loop-AES nepotřebujeme žádné další moduly, protože loop.o má již v sobě obsaženou podporu šifry AES

Instalace Loop-AES (util-linux)

Pro vytvoření a používání šifrovaného diskového oddílu ještě potřebujeme upravené verze programů: mount, umount, losetup, swapon and swapoff

Pro naše potřeby stačí nainstalovat pouze tyto příkazy. Instalace celého balíčku util-linux se nedoporučuje. Instalaci provedeme pomocí následujících kroků:

```
$ bzip2 -d -c util-linux-2.12pre.tar.bz2 | tar xvf -  
$ cd util-linux-2.12pre  
$ patch -p1 < /cesta/k/loop-AES/util-linux-2.12pre.diff  
$ CFLAGS=-O2 ./configure  
$ make SUBDIRS="lib mount"  
$ cd mount
```

Následující sadu příkazů již musíme provést pod uživatelem root.

Instalace Loop-AES (util-linux)

```
# install -m 4755 -o root mount umount /bin
# install -m 755 losetup swapon /sbin
# rm -f /sbin/swapoff && \
    ( cd /sbin && ln -s swapon swapoff )
# rm -f /usr/share/man/man8/{mount,umount,losetup,
    swapon,swapoff}.8.gz
# install -m 644 mount.8 umount.8 losetup.8
    /usr/share/man/man8
# install -m 644 swapon.8 swapoff.8 /usr/share/man/man8
# rm -f /usr/share/man/man5/fstab.5.gz
# install -m 644 fstab.5 /usr/share/man/man5
# mandb
```

Otestování funkčnosti Loop-AES

Po kompilaci ovladače loop.o a programu losetup můžete provést test, zda všechno funguje tak jak má.

Toto provedeme pomocí příkazu spuštěného v adresáři se zdrojovými soubory Loop-AES pod uživatelem root:

```
# make tests
```

Pokud na konci výpisu najdeme zprávu:

```
*** Test results ok ***
```

je vše v pořádku. Pokud se test selže, pak Loop-AES nepoužívejte, je totiž nějakým způsobem poškozený!

Použití Loop-AES (diskový oddíl)

1. příklad ukazuje jak použít šifrovaný diskový oddíl. Diskový oddíl použití v našem případě je /dev/hda3, který chceme připojit jako adresář /cryptohd.

Loopback zařízení /dev/loop0 s 128-bitovou šifrou připojené na /dev/hda3 nastavíme pomocí příkazu:

```
# losetup -e AES128 -T /dev/loop0 /dev/hda3
```

Program losetup se Vás zeptá na heslo (minimálně 20 znaků!), které si samozřejmě musíte zapamatovat.

Dále je vhodné vytvořit na tomto novém diskovém oddílu nějaký souborovém systém, v našem případě vytvoříme třeba ext3.

```
# mkfs.ext3 /dev/loop0
```

Použití Loop-AES (diskový oddíl)

Nyní již můžeme `/dev/loop0` odpojit:

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

Nejllepší způsob použití tohoto oddílu je vložení nového řádku do souboru `/etc/fstab`:

```
/dev/hda3 /cryptohd ext3 defaults,noauto,  
loop=/dev/loop0,encryption=AES128 0 0
```

Oddíl můžeme poté připojit (resp. odpojit) pomocí příkazu:

```
# mount /cryptohd, resp.
```

```
# umount /cryptohd
```

Šifrovaný diskový oddíl můžeme případně připojit rovnou příkazem:

```
# mount -t ext3 /dev/hda3 /cryptohd -o loop=/dev/loop0,  
encryption=AES128
```

Použití Loop-AES (soubor)

2. příklad ukazuje vytvoření souborového systému uvnitř zašifrovaného souboru. Postup je víceméně obdobný předchozímu: Nejdříve si připravíme soubor, ve kterém si náš souborový systém vytvoříme:

```
# dd if=/dev/urandom of=/cryptofile bs=1M count=500
```

Další kroky jsou již známe:

```
# losetup -e AES128 -T /dev/loop1 /cryptofile
```

```
# mkfs.ext3 /dev/loop1
```

```
# losetup -d /dev/loop1
```

Do souboru `/etc/fstab` přidáme řádek:

```
/cryptofile /cryptohd ext3 defaults,noauto,loop=/dev/loop1,  
encryption=AES128 0 0
```

Práce s takto vytvořeným souborovým systémem se od předchozího příkladu jinak vůbec neliší.

Použití Loop-AES (seed)

Poslední příklad ukazuje vytvoření souborového systému chráněného nejen heslem, ale také „semínkem“. Nejprve si vygenerujeme semínko:

```
$ head -c 15 /dev/urandom | uuencode -m - | head -n 2 \  
| tail -n 1
```

Semínko může vypadat následovně: hh7EVafLbir9yo3+SsyV

Dále zaplníme diskový oddíl náhodnými daty:

```
$ head -c 15 /dev/urandom | uuencode -m - | head -n 2 | \  
tail -n 1 | losetup -p 0 -e AES128 /dev/loop2 /dev/hda3
```

```
$ dd if=/dev/zero of=/dev/loop2 bs=4k conv=notrunc \  
2>/dev/null
```

```
$ losetup -d /dev/loop2
```

Použití Loop-AES (seed)

Nyní už můžeme nastavit loopback zařízení pro použití se „semínkem“.
Semínko zadáme programu pomocí parametru `-S`:

```
$ losetup -e AES128 -T -S hh7EVafLbir9yo3+SsyV \  
-C 100 /dev/loop2 /dev/hda3  
$ mkfs.ext3 /dev/loop2  
$ losetup -d /dev/loop2
```

Nový záznam v souboru `/etc/fstab` musí v tomto případě obsahovat navíc „semínko“ za parametrem `pseed=` a počet iterací hesla za `itercountk=`:

```
/dev/hda3 /cryptohd ext3 defaults,noauto,loop=/dev/loop2,  
encryption=AES128,itercountk=100,  
pseed=hh7EVafLbir9yo3+SsyV 0 0
```

Děkuji vám za
pozornost!

Případné otázky zodpoví můj tiskový
mluvčí Fanda Kocourek...

