Loopback Encrypted Filesystem HOWTO

Copyright di Ryan T. Rhea, rhear@cs.winthrop.edu v1.1, 29 novembre 1999

Questo documento spiega come impostare e quindi usare un file system che, quando montato da un utente, cifra in maniera dinamica e trasparente i suoi contenuti. Il file system viene conservato in un file regolare, che può essere nascosto o nominato in modo non-evocativo così che probabilmente passerebbe inosservato. Questo permette di conservare dati ad un alto livello di sicurezza. Traduzione a cura di *Isabella Ruocco* e di *Diego Buffa* . Ultima revisione 3 aprile 2000.

Indice

1 Prima di iniziare

Questo procedimento richiede il codice sorgente del kernel, saper come compilare questo codice e un sacco di pazienza. Raccomando caldamente di tenere pronto un disco di avvio. Inoltre, siate sicuri di avere una copia prima di memorizzare permanentemente i vostri dati importanti sul file system cifrato - potrebbe danneggiarsi come qualsiasi altro file system.

Dovrete applicare le patch come minimo fino alla versione 2.2.9 del kernel di linux prima di continuare. Ulteriori istruzioni su come applicare le patch si trovano nella sezione 4 (Dettagli) più avanti in questo documento.

Il codice sorgente del kernel si può trovare in:

```
ftp://ftp.kerneli.org/
```

C'è un HOWTO sul procedimento della ricompilazione del kernel in:

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

2 Introduzione

Il procedimento usa il dispositivo '/dev/loop*' (dove * può essere 0-7 sulla maggior parte delle installazioni) per montare un file system di loopback. Lo stesso procedimento può essere usato senza cifratura per tenere un file system linux su una partizione non-linux. C'è un HOWTO su questo nel sito LDP citato precedentemente.

Si possono usare diversi tipi di cifratura, compresi XOR, DES, twofish, blowfish, cast128, serpent, MARS, RC6, DFC e IDEA. Il programma 'losetup' (loopback setup ovvero impostazione del loopback) è ciò che associa il vostro file cifrato ad un file system e al suo tipo di cifratura. Secondo Alexander Kjeldaas, che mantiene kerneli.org e le patch internazionali sulla cifratura, DES e losetup sono attualmente incompatibili. Questo è dovuto alle differenze nel modo in cui i due gestiscono i bit di parità. Non ci sono progetti per supportare il DES poiché è molto più insicuro degli altri cifrari.

Twofish, blowfish, cast128 e serpent hanno tutti una licenza libera per qualunque uso. Gli altri potrebbero o meno avere restrizioni di licenza. Molti di essi sono candidati per lo standard AES. I finalisti forniranno in tutto il mondo l'uso senza royalty dei loro cifrari.

Questo documento usa l'algoritmo serpent perché è forte e anche notevolmente veloce ed è liberamente distribuibile sotto la GPL. In base alla sua documentazione, serpent usa un cifrario a blocchi di 128 bit progettato da Ross Anderson, Eli Biham e Lars Knudsen. Esso fornisce agli utenti il più alto livello pratico di assicurazione che non verrà trovato nessun attacco a scorciatoia. La documentazione su serpent, così come il codice sorgente, si possono trovare in:

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

Inoltre, questo documento presuppone che i cifrari siano compilati direttamente nel kernel. Potreste installarli come moduli, ma la tecnica non viene discussa in questo documento. Dovrete editare il file '/etc/conf.module'; il procedimento è discusso in dettaglio nell'HOWTO sulla compilazione del kernel citato in precedenza.

3 Sommario

Ci sono molti passi coinvolti nel procedimento. Fornirò 4 (Dettagli) per questi passi nel prossimo paragrafo. Ho pensato che sarebbe stato carino fornire prima un sommario di riferimento (se voi avete esperienza con unix/linux probabilmente non avete bisogno comunque dei dettagli). Sono riassunti come segue:

1. Scaricate la più recente patch internazionale sulla cifratura (io ho usato 'patch-int-2.2.10.4' quando questo documento è stato scritto) da:

   `http://ftp.kerneli.org/pub/kerneli/`

2. Applicate la patch al kernel

3. Eseguite 'config' (o 'menuconfig' o 'xconfig') per configurare il vostro 'MakeFile' per il nuovo kernel. Le opzioni per abilitare la cifratura sono sparpagliate. Prima di tutto, prima che vediate qualche altra opzione, dovete abilitare 'Prompt for development and/or incomplete code/drivers' sotto 'Code Maturity level options'. Sotto 'Crypto options' abilitate 'crypto ciphers' e 'serpent'. Ancora una volta, questo documento presume che stiate usando serpent, ma provate quello che volete. Ricordate che DES è notoriamente incompatibile con 2.2.10.4 - potrebbe non essere mai supportato del tutto. Ci sono molte opzioni importanti da selezionare sotto 'Block Devices'. Queste includono 'Loopback device support', 'Use relative block numbers as basis for transfer functions (RECOMMENDED)', e 'General encryption support'. NON selezionate la cifratura 'cast 128' o 'twofish' qui. Notate anche che non avete bisogno di nessuna delle opzioni sulla cifratura sotto le varie categorie di rete. Non andrò oltre nella configurazione del kernel, è fuori dagli intenti di questo documento e si può trovare sul sito LDP.

4. Compilate il nuovo kernel.

5. Editate '/etc/lilo.conf' per aggiungere la nuova immagine del kernel. Eseguite 'lilo -v' per aggiungere il kernel al boot loader.

6. Scaricate il sorgente per il più recente pacchetto 'util-linux' (io ho usato 'util-linux-2.9v') da:

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

7. Estraete il sorgente 'util-linux'.

8. Applicate la patch corrispondente trovata nella vostra directory '/usr/src/linux/Documentation/crypto/'.

9. Leggete ATTENTAMENTE il file 'INSTALL'! Questo pacchetto contiene i sorgenti per molti file dipendenti dal sistema (strumenti importanti come 'login', 'passwd', ed 'init'). Se non editate attentamente il file MCONFIG prima di compilare questi sorgenti tenete pronto un dischetto di avvio e/o un fucile perchè il vostro sistema sarà un po' confuso. Essenzialmente volete impostare quasi tutti i campi 'HAVE_*' uguali a 'yes' così che gli strumenti importanti di autenticazione non vengano compilati e sovrascritti. Gli strumenti che volete ricompilare sono 'mount' e 'losetup' in modo da adattarli ai nuovi schemi di cifratura. Suggerisco di fare riferimento al paragrafo 4 (Dettali) nel seguito per questo passo.

10. Compilate ed installate il sorgente 'util-linux'

11. Fate riavviare la macchina con il nuovo kernel.

12. Editate '/etc/fstab', aggiungendo una voce per il vostro mount point come segue:

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

13. Create la directory che conterrà il vostro file system, come in '/mnt/crypt' sopra.

14. Come utente, create il vostro file cifrato come segue:

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

15. Eseguite losetup come segue:

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

Avete una sola possibilità per digitare la password, state attenti. Se volete fare una doppia verifica sulla vostra password, potete usare il comando:

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

Questo disattiverà il vostro dispositivo di loop. Poi eseguirete nuovamente losetup per verificare la vostra password, come segue:

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

16. Create il vostro file system ext2 come segue:

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

17. Ora potete montare il file system cifrato con:

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

18. Quando avrete finito, vorrete smontare e proteggere il vostro file system come segue:

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

4 Dettagli

Applicare le patch al Kernel:

Potete fare l'aggiornamento dalle distribuzioni '2.2.x' applicando le patch. Ciascuna patch rilasciata per '2.2.x' contiene correzioni dei bachi. Verranno aggiunte nuove caratteristiche al kernel Linux di sviluppo '2.3.x'. Per installare applicando le patch, prendete tutte le patch più recenti e fate quanto segue:

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

Ripetete xx, IN ORDINE, per tutte le versioni più recenti rispetto a quella del vostro albero dei sorgenti corrente.

La directory predefinita per il sorgente del kernel è '/usr/src/linux'. Se il vostro sorgente è installato da qualche altra parte vi suggerirei di usare un collegamento simbolico da '/usr/src/linux'.

Editate 'MCONFIG' per la compilazione del pacchetto 'util-linux':

Quelle che seguono sono citazioni dal file 'MCONFIG' che ho usato per compilare il pacchetto 'util-linux'. Notate che questo è abbastanza specifico per la mia configurazione, che è vagamente basata su RedHat 5.2. Il punto è assicurarsi che non sovrascriviate nessun importante strumento di sistema come 'login', 'getty', o 'passwd'. Comunque, ecco di seguito le righe importanti:

```
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
```

Suggerimenti:

Notate che potreste usare uno qualunque degli otto dispositivi di loopback, da 'dev/loop0' a '/dev/loop7'. Usate una directory non evocativa per il mount point. Suggerirei di creare una cartella con permessi 700 dentro la vostra home directory. Lo stesso vale per il file che contiene i dati. Io uso un nome di file come 'sysfile' o 'config.data' nella cartella '/etc'. Questo di solito passerà inosservato.

Ho creato degli script Perl molto semplici per montare e smontare il file system con un comando. Scrivete questi, rendeteli eseguibili (chmod u+x), e metteteli da qualche parte nel vostro percorso.

```
#!/usr/bin/perl -w
#
#piccolo file di utilita per impostare un file system cifrato di loopback
#Copyright 1999 di Ryan T. Rhea
`losetup -e serpent /dev/loop0 /etc/cryptfile`;
`mount /mnt/crypt`;
```

Chiamate 'loop' lo script qui sopra, e poi potrete essere sulla strada buona con un comando ('loop') ed una password.

```
#!/usr/bin/perl -w
#
#piccolo file di utilita per disattivare un fliesystem cifrato di loopback
#Copyright 1999 di Ryan T. Rhea
`umount /mount/crypt`;
`losetup -d /dev/loop0`;
```

Chiamate 'unloop' il secondo, e poi digitando 'unloop' si disattiverà velocemente il vostro file system.