Gestire filesystem cifrati usando LUKS

Per cifrare i contenuti di un intero disco viene normalmente utilizzato **LUKS**, acronimo di "Linux Unified Key Setup", che si propone come lo standard per la crittografia dei dischi in sistemi Linux (e non solo), offrendo un formato standard "on-disc", la possibilità di avere più di una coppia chiave-passphrase per l'accesso ai contenuti ed una gestione sicura di tutte le chiavi.

Benché sia possibile (ad esempio nel caso di Debian e derivate) installare direttamente il sistema cifrando il disco, nel caso che tutte le operazioni vengano gestite dal programma di installazione, si pone talvolta la necessità di effettuare la stessa operazione quando si aggiunge un disco esterno.

Spesso si ha questa esigenza quando si usano dischi di backup rimuovibili (da spostare in una diversa collocazione, come possibile realizzazione di una procedura elementare di disaster recovery) in modo da proteggere i dati in essi contenuti o più in generale tutte le volte che si vogliono proteggere i dati salvati su un supporto esterno. In tutti questi casi occorre eseguire le operazioni di gestione dei dischi cifrati manualmente, nelle modalità che esamineremo nel seguito.

Creazione di un disco cifrato

Un disco cifrato con LUKS, nel caso lo si sia formattato con una filesystem compatibile (es. vfat), è accessibile anche dai sistemi Windows usando LibreCrypt. Per utilizzarlo da Linux è necessaria una versione del programma cryptsetup(che viene usato anche per la cifratura diretta con "dm-crypt") che lo supporti, ormai disponibile su tutte le distribuzioni. Si può comunque verificare la presenza del supporto con il comando cryptsetup --help controllando in coda la presenza delle opzioni relative a LUKS. Nel caso in cui il comando non fosse presente, su Debian lo si può installare semplicemente con:

```
apt-get install cryptsetup
```

A questo punto è possibile iniziare il lavoro di preparazione del dispositivo, nel nostro esempio prenderemo il caso una chiavetta USB rilevata dal sistema come /dev/sdd.

La prima cosa da fare è verificare l'affidabilità del dispositivo e, al tempo stesso, riempire tutto lo spazio disponibile con dei dati casuali rendendo di fatto molto più difficoltosi eventuali tentativi di attacco e compromissione del filesystem cifrato che verrà creato in seguito. Prima di iniziare, va tenuto presente il fatto che a seconda della dimensione del disco, questo processo può richiedere molte ore, quindi se dovete lanciarlo su di un disco molto grande, vi conviene farlo prima di andare a dormire.

```
badblocks -c 10240 -s -w -t random -v /dev/sdc
```

Se siete particolarmente paranoici potete utilizzare /dev/urandom come sorgente di dati casuali e riempirci il disco. La casualità dei dati sarà migliore rispetto a quella del metodo precedente, ma l'operazione farà un uso intensivo della CPU e richiederà ancora più tempo. Il comando da eseguire è:

```
dd if=/dev/urandom of=/dev/sdc
```

Successivamente va partizionato il disco. In questo caso l'obiettivo è creare un'unica partizione che occupi tutto lo spazio disponibile e per farlo ci sono diverse alternative, sia da linea di comando come fdisk o cfdisk che grafiche comegparted e qtparted. Si supponga comunque di avere creato una sola partizione, riconosciuta dal sistema come /dev/sdd1.

A questo punto è possibile cifrare la partizione con LUKS e poi "agganciarla" al device mapper, in modo che possa essere presentata in maniera "trasparente" al sistema. E' molto importante la scelta di una passphrase abbastanza lunga e complessa poiché l'utilizzo di una frase corta e/o facilmente indovinabile vanificherebbe l'utilizzo della crittografia.

Il primo passo è inizializzare il disco per la cifratura con LUKS, per questo si usa il comando:

```
# cryptsetup --verbose --verify-passphrase luksFormat /dev/sdd1

WARNING!
========
Questo sovrascriverà i dati in /dev/sdd1 in modo irreversibile.

Are you sure? (Type uppercase yes): YES
Inserire la passphrase:
Verifica passphrase:
Comando eseguito con successo.
```

occorrerà confermare la formattazione del disco e poi inserire la passphrase, ripetendola due volte per verifica.
A questo punto si potrà attivare il disco cifrato con:

```
# cryptsetup luksOpen /dev/sdd1 cifrato
Inserire la passphrase per /dev/sdd1:
```

dove si dovrà inserire, per poter accedere in chiaro ai dati del disco, la passphrase fornita con il comando precedente.

Se tutto è andato a buon fine, l'output del comando ls /dev/mapper/ dovrebbe restituire anche cifrato fra i file presenti, confermando l'avvenuto "aggancio" della partizione criptata al device mapper, il quale fornirà su/dev/mapper/cifrato il dispositivo su cui operare in chiaro. A questo punto si potrà creare un filesystem sulla partizione criptata con:

```
mkfs.ext4 /dev/mapper/cifrato
```

e sarà possibile montarlo con:

```
mount /dev/mapper/cifrato /mnt
```

Infine i comandi per smontare il filesystem e disabilitare l'accesso alla partizione criptata sono:

```
umount /mnt
cryptsetup luksClose /dev/mapper/cifrato
```


Truelite Srl
Via Monferrato, 6
50142 Firenze
055.7879597
www.truelite.it - info@truelite.it

dove il secondo comando distacca il disco dal device mapper (si potrà verificare che /dev/mapper/cifrato non è più disponibile), rendendo impossibile l'accesso ai dati del disco.

Si tenga presente che una volta formattato un disco con luksFormat questo potrà essere identificato, oltre che con il nome di dispositivo classico, anche tramite l'UUID ad esso associato rendendo il riconoscimento dello stesso indipendente dall'eventuale presenza di altri dischi e dall'ordine con cui il kernel assegna i vari nomi /dev/sdX.

In particolare nel nostro caso potremo individuare eventuali dischi cifrati con:

```
# blkid -t TYPE="crypto_LUKS"
/dev/sdd1: UUID="695fb63b-bb47-45d5-9561-15f6664c0296"
TYPE="crypto_LUKS" PARTUUID="05548b2f-01"
```

ed in tutti i comandi riguardanti LUKS si potrà usare, al posto dell'indicazione del dispositivo specifico (nel caso /dev/sdd1) l'indicazione dell'UUID (nella forma UUID=695fb63b-bb47-45d5-9561-15f6664c0296).

Utilizzo dei dischi cifrati

Le distribuzioni sufficientemente moderne usano hal, d-bus e gnome-volume-manager (o l'equivalente per altri desktop) per la gestione dei volumi disponibili nel sistema. Quando viene collegata al sistema una chiavetta USB (o altro disco rimuovibile) contenente la partizione crittografata con LUKS, questa viene riconosciuta e compare una finestra che chiede di inserire la passphrase. Se la passphrase inserita è corretta, la partizione viene montata e sarà possibile utilizzarla normalmente da tutte le applicazioni.

Qualora invece si intenda cifrare un disco di sistema (ad esempio un disco per i backup) da montare all'avvio, si deve ricorrere all'uso del file /etc/crypttab che contiene l'elenco dei dischi cifrati che devono essere sbloccati, in modo tale da poterli poi usare normalmente dentro /etc/fstab. Si tenga conto che in questo caso la passphrase sarà chiesta all'avvio e che se non verrà fornita l'avvio si bloccherà sulla richiesta di montaggio del dispositivo.

Il formato di /etc/crypttab prevede quattro campi separati da spazi. Il primo campo indica il nome che si darà al dispositivo cifrato sotto /dev/mapper (nel caso dell'esempio precedente, cifrato), il secondo campo indica il dispositivo fisico e si può indicare con il nome dello stesso (nel nostro esempio /dev/sdd1), o con l'UUID come detto in precedenza. Oltre che con blkid l'UUID si può ottenere anche con il comando:

```
# cryptsetup luksUUID /dev/sdd1
695fb63b-bb47-45d5-9561-15f6664c0296
```

Il terzo campo indica le modalità con cui si sblocca il dispositivo ed il default di none indica la necessità di fornire la passphrase sulla console. Si può comunque anche indicare un nome di un file (ad esempio da fornire su un dispositivo esterno) da cui questo verrà letto (in tal caso viene usato tutto il file e la passphrase in esso contenuta non deve terminare con un a capo). L'ultimo campo, che indica le opzioni con cui viene creato il dispositivo cifrato, nel nostro caso dovrà essere luks.

Pertanto con un contenuto di /etc/crypttab del tipo:

```
# <target name>    <source device>         <key file>    <options>
cifrato        UUID=695fb63b-bb47-45d5-9561-15f6664c0296    none
luks
```

potremo montare il disco cifrato sotto /cifrato inserendo in /etc/fstab la riga:

```
/dev/mapper/cifrato   /cifrato      ext4    defaults        0       2
```

Qualora invece si abbia la necessità di montare e smontare il disco in uno script (ad esempio in uno script per la gestione dei backup su un disco rimuovibile) si pone il problema di come inserire la passphrase, che il comando normalmente richiede sia fornita su un terminale. In tal caso si potrà fargliela leggere da un file separato, ma è in genere preferibile inserire tutte le informazioni direttamente all'interno dello script, utilizzando una attivazione del disco cifrato nella forma:

```
echo -n passphraselungaecomplicata|cryptsetup luksOpen /dev/sdd1
cifrato --key-file=-
```

(dove il -n è importante, perché l'a capo inserito da echo nella invocazione normale verrebbe letto come carattere della passphrase).

Ovviamente in questo caso la password sarà leggibile da chi ha accesso amministrativo alla macchina, ma la protezione è pensata per proteggere il disco quando viene rimosso e spostato altrove.

Gestione delle passphrase

Una delle funzionalità più interessanti di LUKS, che lo rende preferibile rispetto all'uso diretto del "dm-crypt" elementare, è che il sistema consente l'uso di più password (fino ad un massimo di 8) che possono essere aggiunte o rimosse (posto che almeno una resti presente per poter accedere al dispositivo). Il caso più comune è quello in cui si vuole aggiungere una nuova password o cambiare quella esistente (che si realizza comunque per con una aggiunta seguita da una rimozione).

Il comando che consente di aggiungere una passphrase è il seguente:

```
cryptsetup luksAddKey /dev/sdd1
```

verrà chiesta una qualunque delle passphrase presenti per sbloccare l'accesso (all'inizio ce ne è una sola, quella impostata in fase di creazione, cui viene sempre assegnato l'indice 0) e poi l'immissione due volte della nuova passphrase. La passphrase sarà inserita nel primo degli slot disponibili (nel caso dell'esempio, se aggiunta dopo la creazione, questo sarà quello con indice 1) e potrà essere utilizzata in maniera equivalente a tutte le altre. Se lo scopo non era quello di aggiungere una nuova passhprase, ma solo quello di cambiarne una esistente, si potrà a questo punto passare alla rimozione di quella non voluta, cancellando il relativo slot.

Truelite Srl
Via Monferrato, 6
50142 Firenze
055.7879597
www.truelite.it - info@truelite.it

Per individuare lo slot si può usare il comando cryptsetup luksDump, ottenendo un risultato del tipo:

```
cryptsetup luksDump /dev/sdd1
LUKS header information for /dev/sdd1

...

Key Slot 0: ENABLED
        Iterations:             182965
        Salt:                   50 6d 67 70 63 33 19 c6 41 e7 c1 55 b6
02 49 89
                                54 79 7b 56 4e b6 78 92 c8 f8 66 e8 bb
e6 a8 f1
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: ENABLED
        Iterations:             144406
        Salt:                   56 35 b1 33 8d c9 0e b8 ba 10 a0 1c 4f
16 2b 8c
                                d3 ec fe c8 5f 7f 23 74 79 ab 5d 96 ec
4c 4c 4a
        Key material offset:    264
        AF stripes:             4000
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

e a questo punto la rimozione della passhprase indesiderata (nello specifico quella dello slot 0) sarà effettuata con:

```
cryptsetup luksKillSlot /dev/sdd1 0
```