Cifrare lo Swap in Linux

Come abbiamo ormai fatto spesso in questa rubrica, usiamo Linux per esemplificare la procedura di cifratura di filesystem discussa nell'articolo precedente. Utilizziamo in questo caso la linea di comando e spieghiamo passo passo la procedura per illustrare i principali concetti del funzionamento di un filesystem cifrato.

Come esempio utilizziamo il modulo *dm-crypt* [1] presente dalla versione 2.6.4 del kernel Linux. Il modulo *dm-crypt* richiede anche il modulo *dm_mod* ed entrambi possono essere sia compilati staticamente nel kernel che lasciati come moduli da caricare dinamicamente. Inoltre avremo bisogno anche degli algoritmi crittografici *aes* e *sha256*, anch'essi possono essere sia compilati staticamente nel kernel che lasciati come moduli. Assumiamo che tutti questi moduli siano dinamici e quindi dovremo caricarli esplicitamente nel kernel prima di utilizzare un filesystem cifrato (vedi Tabella 1). Tutta la procedura che illustreremo deve essere effettuata come l'amministratore (l'utente *root*) della macchina. E' facile automatizzare questa procedura realizzando ad esempio uno script che automaticamente al boot della macchina cifri le partizioni di swap come descritto in questo articolo.

Lo swap

Il nostro punto di partenza è una installazione con una singola partizione di swap sul device `/dev/hda3` di 1,5GB (vedi Tabella 3). Vogliamo trasformare questo swap in uno swap cifrato. Il primo passo è quindi fermare (*smontare*) lo swap con il comando `swapoff`. Dobbiamo poi caricare tutti i moduli di cui avremo bisogno (vedi Tabella 1): in particolare il ruolo di *dm-mod* è quello di realizzare la connessione tra il device virtuale usato da *dm-crypt* ed il device vero (*dm* sta per device-mapper) mentre *dm-crypt* implementa la cifratura/decifrazione dei dati che attraversano il device virtuale.

In pratica la gestione del device virtuale è effettuata con il tool `cryptsetup`, scaricabile da [1] e presente anche ad esempio in pacchetti *rpm* quale `cryptsetup-luks`. Nel nostro caso la creazione del device virtuale si esaurisce in un unico comando `cryptsetup` riportato in Tabella 1. Le opzioni passate a cryptsetup hanno il seguente significato:

- `-c aes` indica di utilizzare l'algoritmo AES[1]
- `-s 256` indica la lunghezza della chiave, in questo caso 256bit
- `-d /dev/urandom` indica di ottenere la passphrase dal device `/dev/urandom`
- `create swap0 /dev/hda3` indica di creare un device virtuale in `/dev/mapper/` di nome `swap0` connesso al device reale `/dev/hda3`.

In pratica ogni dato in input/output al/dal device virtuale `/dev/mapper/swap0` è de/cifrato con *aes256* ed una chiave generata (pseudo) casualmente dal device `/dev/urandom`. La chiave non è salvata da nessuna parte, viene solo passata da *cryptsetup* a *dm-crypt* (che è eseguito all'interno del kernel) che a sua volta la utilizza per de/cifrare i dati. Con il comando `cryptsetup remove` (vedi Tabella 2) viene poi rimossa l'associazione tra il device virtuale e quello reale, e *dm-crypt* cancella la chiave dalla propria memoria. A questo punto qualunque dato presente in `/dev/hda3` è inaccessibile. Questo è esattamente quello che ci interessa, in quanto lo scopo di cifrare lo swap è proprio quello di impedire che dati rimasti nell'area di swap su disco dopo lo spegnimento dell'elaboratore, possano essere recuperati.

A questo punto, creato il device virtuale cifrato, possiamo utilizzarlo come se fosse una partizione di un vero disco. Pertanto per attivare un'area di swap su di esso, è necessario per prima cosa inizializzare il device all'uso di swap con il comando `mkswap` e poi attivare lo swap con il comando `swapon` (vedi Tabella 1) sul device virtuale `/dev/mapper/swap0`. Analogamente, al termine dell'uso, prima di rimuovere il device virtuale con `cryptsetup`, dobbiamo disattivare l'area di swap su `/dev/mapper/swap0` con il comando `swapoff`.

1 Per maggiore protezione contro gli attacchi di watermarking e simili, si consiglia di usare l'algoritmo aes-cbc-essiv:sha256 che adotta una gestione più sofisticata degli IV.

In Tabella 3 abbiamo riportato lo stato dell'area di swap prima e dopo dell'attivazione della cifratura con dm-crypt.

Alcune osservazioni

Come abbiamo già accennato, il comando `cryptsetup remove` cancella sia l'associazione tra il device virtuale e quello reale, che la chiave di cifratura dalla memoria del sistema operativo. Questa operazione deve essere effettuata non appena si termina l'uso della partizione cifrata, altrimenti altri utenti o l'amministratore potrebbero accedervi *montandola* come un proprio filesystem.

Nella forma del comando `cryptsetup` che abbiamo utilizzato, la passphrase/chiave è letta dal device `/dev/urandom`, se non usassimo l'opzione `-d` la passphrase sarebbe chiesta interattivamente all'utente. Nel caso in cui venga fornita una passphrase direttamente dall'utente, questa viene trasformata nella chiave usata per cifrare tramite un hash crittografico, ad esempio SHA256 che può essere specificato con l'opzione `-h`, e poi troncata alla lunghezza indicata dall'opzione `-s`. Quando invece la passphrase è presa da un file od un device con l'opzione `-d`, questa viene utilizzata direttamente come chiave di cifratura, previa essere troncata alla lunghezza indicata dall'opzione `-s`.

Lo stesso approccio indicato in questo articolo può essere adottato per altre aree del filesystem, come ad esempio l'area temporanea che in ambienti unix di solito corrispondente alla directory `/tmp`. Ad esempio su di un portatile potremmo cifrare la directory `/tmp`, ed ogni qualvolta si effettua lo shutdown del portatile, tutti i contenuti della directory `/tmp` rimangono sul disco cifrati con una chiave non più presente nel sistema operativo, e quindi effettivamente indisponibili. Ovviamente al riavvio della macchina bisogna ricreare il filesystem cifrato temporaneo che risulta quindi disponibile solo per il tempo di un boot del sistema operativo.

Andrea Pasquinucci

pasquinucci@ucci.it

Riferimenti Bibliografici

[1] http://www.saout.de/misc/dm-crypt/, http://clemens.endorphin.org/LUKS

```
modprobe aes
modprobe sha256
modprobe dm_mod
modprobe dm_crypt
cryptsetup -c aes -s 256 -d /dev/urandom create swap0 /dev/hda3
mkswap /dev/mapper/swap0
swapon /dev/mapper/swap0
```

Tabella 1. Attivare swap cifrato

```
swapoff /dev/mapper/swap0
cryptsetup remove swap0
```

Tabella 2. Disattivare swap cifrato

```
# prima della cifratura dello swap
> cat /proc/swaps
Filename           Type         Size      Used    Priority
/dev/hda3          partition    1536184   812     -1

# dopo la cifratura dello swap
> cat /proc/swaps
Filename           Type         Size      Used    Priority
/dev/mapper/swap0  partition    1536184   0       -2

> /sbin/cryptsetup status swap0
/dev/mapper/swap0 is active:
  cipher:  aes-cbc-plain
  keysize: 256 bits
  device:  /dev/hda3
  offset:  0 sectors
  size:    3072384 sectors
  mode:    read/write
```

Tabella 3. Verifica cifratura dello swap