# FileSystem Cifrati

Ci eravamo già occupati nel numero 13 di questa rivista del problema di cifrare dati sul proprio elaboratore. In quella occasione avevamo visto come usare PGP per cifrare singoli files, ma avevamo anche evidenziato il fatto che questo approccio ha molte lacune dal punto di vista di sicurezza. Ad esempio il file deve prima essere creato in modo non cifrato, e poi solo successivamente viene cifrato. La versione non cifrata del file può sopravvivere sia nel filesystem che nello swap (anche se si *cancellano*, normalmente i dati rimangono sul disco poiché viene solo cancellato l'indirizzo dei dati sul disco e non i dati in se, ed in alcuni casi è possibile recuperare i dati con strumenti hardware anche se vengono sovrascritti). Per evitare questo, bisogna almeno cifrare sia lo swap che una partizione od un ramo di directory intero.

**Cifrare device/partizioni**

Il nostro scopo è quello di cifrare un intero disco, partizione o ramo di directory. Per fare ciò deve essere risolto il problema di come accedere ai dati all'interno del contenitore cifrato. In pratica quello che vorremmo fare è di avere una parte del filesystem che normalmente è cifrata e quindi inaccessibile a chiunque. Quando l'utente ne ha bisogno, *apre* il ramo del filesystem cifrato decifrandolo con la opportuna chiave. Da quel momento il ramo del filesystem non è più cifrato nel senso che il sistema operativo è in grado di leggere e scrivere in esso come se non fosse cifrato. In questo momento perciò il sistema operativo ha accesso diretto a tutti i dati che sono contenuti nel filesystem e deve pertanto fare in modo che solo il legittimo proprietario possa accedervi utilizzando le usuali protezioni. Una volta che l'utente ha terminato di usare i dati contenuti nel filesystem cifrato, l'utente *rilascia* il filesystem, il sistema operativo *dimentica* la chiave di accesso ad esso, ed i dati in esso contenuti diventano inaccessibili a chiunque.

Vi sono quindi due situazioni: la prima in cui il filesystem/partizione è cifrato ed appare a chiunque come una partizione contenente dati incomprensibili; la seconda in cui previo l'utilizzo della chiave appropriata, il sistema operativo e l'utente hanno accesso ai dati contenuti nel filesystem/partizione.

Si noti come in questa seconda fase se si utilizza un comune sistema operativo, sia l'amministratore di sistema che l'utente hanno accesso ai dati.[1] Inoltre in questa seconda fase i dati sono protetti dall'accesso di altri utenti solo utilizzando le normali protezioni del sistema operativo.

**Il device/partizione virtuale**

E' importante cercare di spiegare meglio questo punto. Prima di tutto, sul disco fisico i dati sono sempre cifrati, quindi un accesso diretto al disco non è utile. Per poter accedere ai dati pur mantenendoli sempre cifrati sul disco fisico, si utilizza un device virtuale. In altre parole, i dati non vengono acceduti direttamente, ma attraverso una partizione virtuale, creata dal sistema operativo e presente solo in memoria. Lo scopo di questa partizione virtuale è quello di cifrare/decifrare i dati che la attraversano: i dati che sono inviati dall'utente verso il disco sono cifrati prima di essere scritto sul device vero, mentre i dati che sono letti dal device vero sono decifrati prima di essere inviati all'utente. Quindi il driver di questa partizione virtuale non contiene le procedure necessarie per accedere ai dischi fisici, bensì gli algoritmi crittografici che permettono di cifrare e decifrare i dati (Fig. 1).

Una volta che il filesystem virtuale è montato, e quindi attivo, si comporta come un normalissimo filesystem, con le usuali directory, file, protezioni eccetera. L'unica differenza con un filesystem normale è che i dati sul disco fisico sono sempre cifrati.

**Utilizzo dei filesystem cifrati**

Abbiamo quindi visto che le caratteristiche principali di un filesystem cifrato sono

1. i dati sul disco fisico sono sempre cifrati
2. l'accesso ai dati avviene tramite un device virtuale che cifra/decifra i dati in transito
3. il device virtuale ha le normali protezioni offerte dal sistema operativo.

Utilizzando quindi un filesystem cifrato possiamo fare in modo che

1 Sistemi Operativi con caratteristiche MAC sono in grado di impedire l'accesso ai dati all'amministratore e limitarlo solamente all'utente.

1. i dati sui dischi fisici siano sempre cifrati
2. l'accesso ai dati sui dischi sia possibile solo se l'utente fornisce l'opportuna chiave.

Sottolineiamo ancora il fatto che i dati in memoria, RAM o swap[2], sono non cifrati e che l'accesso al filesystem virtuale è protetto con le usuali protezioni del sistema operativo, quindi se ad esempio permettiamo a tutti gli utenti l'accesso in lettura al filesystem virtuale, quando il proprietario dei dati ha fornito l'opportuna chiave ed attivato il filesystem virtuale, tutti gli utenti possono leggere quello che vi è contenuto.

Le tipiche applicazioni dei filesystem virtuali sono quindi

1. elaboratori portatili
2. dischi rimovibili
3. dati altamente sensibili.

Nei primi due casi l'utilizzo di filesystem cifrati previene l'esposizione di dati in caso di furto o smarrimento dell'oggetto fisico, nel terzo caso invece è una ulteriore protezione per l'accesso ai dati anche da parte di utenti del sistema o da intrusioni/virus eccetera.

Dal punto di vista tecnico, quello che vogliamo ottenere è che i dati di nostro interesse non compaiano mai in chiaro, ovvero non cifrati, su qualunque supporto fisico. Per ottenere questo, in generale dobbiamo:

1. cifrare il filesystem nel quale vogliamo far risiedere i dati
2. cifrare lo swap
3. cifrare le aree utilizzate temporaneamente dai programmi (videoscrittura eccetera) che manipolano i dati.

In realtà è di solito possibile configurare le applicazioni in modo che queste utilizzino come aree temporanee lo stesso filesystem (cifrato) in cui risiedono i dati, quindi con una accurata configurazione degli applicativi non è necessario cifrare altre aree oltre al filesystem e lo swap.

## Altre applicazioni

2 Nel caso in cui lo swap non sia lui stesso cifrato.

E' ovvio che la principale applicazione dell'uso di filesystem cifrati è per gli elaboratori portatili e i dischi rimovibili, siano essi riscrivibili quali chiavette USB, zip, jazz, vecchi dischetti eccetera, che cd e dvd non riscrivibili. Un problema pratico che si pone anche con macchine normali è quello dell'invio presso l'assistenza hardware per riparazioni: se i dati principali risiedono su di un filesystem cifrato il rischio peggiore è quello della perdita dei dati, ma non della loro divulgazione.

Vi sono poi sistemi che permettono di cifrare tutta la home-directory usando come chiave la password di login. Essi sono ovviamente molto semplici da usare, l'utente non deve far altro che fare l'usuale login ed automaticamente il sistema *apre,* decifrandolo, il filesystem della home-directory dell'utente. Al logout il filesystem è automaticamente chiuso ed i dati sono presenti solo sul disco in modo cifrato. Se l'automazione del processo è molto comoda, bisogna però stare molto attenti alla sua effettiva sicurezza. Prima di tutto, usare la stessa password sia come login che come chiave di cifratura del filesystem non è conveniente: troppo spesso la password di login è usata in mille altre applicazioni, e c'è sempre il rischio di un attacco di forza bruta al file delle password. Poi bisogna sincerarsi che il sistema cifri anche lo swap e tutti i file temporanei che potrebbero contenere i dati, cosa non sempre vera. Pertanto, a nostro parere, in generale si ottiene un più alto livello di sicurezza se si cifra un filesystem particolare con una chiave utilizzata solo per questo scopo.

Un'ultima osservazione riguarda la cifratura di tutto il disco (o dischi) includendo anche il sistema operativo, con la sola eccezione delle procedure iniziali di boot modificate appropriatamente per decifrare i vari filesystem. Questo è ovviamente possibile, ma sono poche le situazioni in cui la complicazione di mantenere un intero sistema cifrato è veramente necessaria per garantire la sicurezza dei dati. Di solito infatti i sistemi operativi utilizzati sono comuni e ben noti, come pure le principali applicazioni. Cifrare tutto il disco non è indicato come misura di controllo degli accessi e nella maggior parte dei casi non è necessario per la confidenzialità dei dati; si noti che in questo caso una volta attivato il sistema, tutti i dischi appaiono in chiaro al sistema operativo e a tutti gli utenti. Ovviamente vi sono situazioni ove questa può essere la soluzione più adatta, ma deve essere valutata caso per caso. Qualora si ritenga utile una soluzione del genere, essa può essere implementata ad esempio generando una chiave pseudo-casuale che viene mantenuta cifrata su di un dispositivo ri-

movibile quale una chiavetta USB, ed è poi possibile utilizzare i dischi solo inserendo la chiavetta USB nell'elaboratore e digitando la relativa passphrase durante la fase di boot. Infine non va dimenticato che in caso di perdita della chiave di cifratura dei dischi, tutti i dati sono praticamente persi.

Nei prossimi articoli illustreremo degli esempi pratici di cifratura di filesystem.

Andrea Pasquinucci

pasquinucci@ucci.it

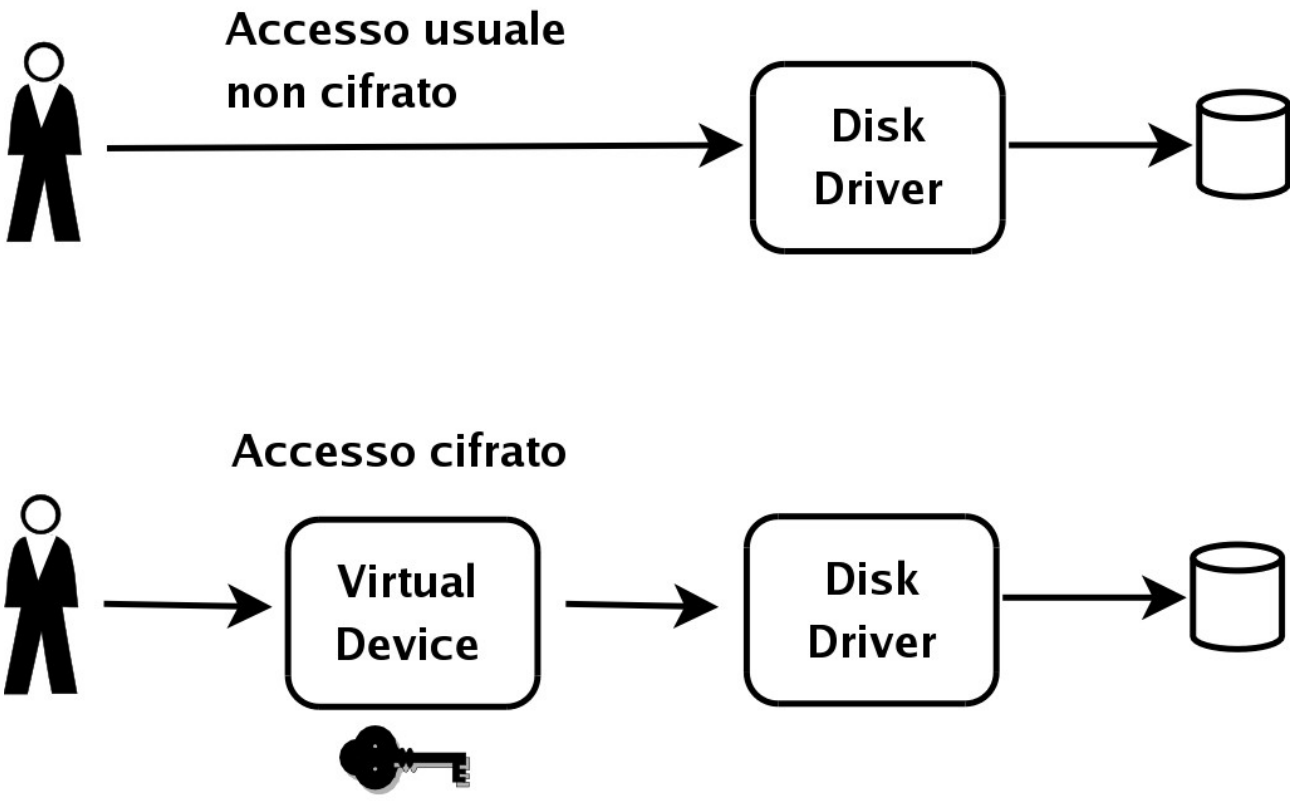


Fig. 1 Accesso diretto e tramite il device virtuale di cifratura