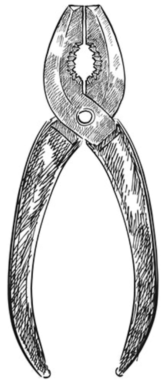
GUIDA ALL'AUTODIFESA DIGITALE

7



Quello che avete tra le mani è l'ottavo numero della traduzione a puntate della Guide d'autodéfence numerique.
L'edizione originale integrale (in francese) è leggibile online e scaricabile liberamente qui:
http://guide.boum.org
Trovate invece le puntate precedenti della traduzione in italiano qui:
http://numerique.noblogs.org

evitera di cancellarle per errore, dall'altra renderà la ricerca del nostro hard disk più facile.

Ovviamente non dobbiamo fare niente di tutto ciò se è proprio il contenuto di un disco esterno quello che vogliamo rendere inaccessibile.

APRIRE L'UTILITY DEL DISCO

Apriamo "Dischi": accediamo alla vista d'insieme delle Attività cliccando sul tasto ⊞ (⌘ su Mac), poi scrivere "disco" e cliccare su "Dischi".

CERCARE L'INDIRIZZO DI UNA PERIFERICA

La colonna di sinistra mostra l'elenco dei dischi del sistema conosciuti. Si può cliccare su uno di questi e vedremo apparire a destra più informazioni. L'icona, la grandezza e il nome stesso, dovrebbero consentirci di identificare quello che cerchiamo.

Se questo non dovesse bastare, si può dare un'occhiata all'organizzazione delle partizioni, guardando la tabella che appare nella parte di destra:

- se il disco da cancellare contiene un sistema GNU/Linux non cifrato, ci devono essere almeno due partizioni, una con un file system swap, l'altra generalmente con ext3 o ext4;
- se il disco da cancellare contiene un sistema GNU/Linux cifrato, devono esserci almeno due partizioni, una con un file system ext2 e l'altra LUKS;
- se il disco da cancellare contiene un sistema Windows, dovrebbero esserci una o piu' partizioni chiamate ntfs o fat32.

In genere, la periferica che corrisponde al disco interno è la prima della lista.

Una volta trovato e selezionato il disco, potremmo leggerne l'indirizzo nella parte in basso a destra, accanto al titolo Periferica.

L’indirizzo della periferica inizia per /dev/ seguito da tre lettere e una cifra, i primi caratteri nella maggior parte dei casi saranno sd, hd o mmcblk : per esempio /dev/sdx1. Segnatevi l’indirizzo da qualche parte, senza la cifra finale (per esempio /dev/sdx): d’ora in poi dovremo scrivere quello al posto di “LA_PERIFERICA”.

Attenzione! Questo indirizzo non è necessariamente sempre lo stesso. Sarà meglio riprovare questa piccola procedura dopo aver riavviato il computer, attaccato e
staccato una penna USB o un hard disk. Questo ci eviterà brutte sorprese… come quella di perdere il contenuto dell’hard disk sbagliato.

LANCIARE IL COMANDO SHRED

Apriamo un Terminale: apriamo la vista d’insieme delle attività cliccando sul tasto (⌘

sistema operativo che usiamo abitualmente, bisogna quindi mettere l’hard disk dentro un altro computer oppure utilizzare un sistema live. Shred è uno strumento base standard, indipendentemente da quale live utilizzeremo.

Il comando è molto semplice. Ha bisogno soltanto di sapere la locazione della periferica (il suo percorso) che vogliamo eliminare, e poi di un po’ di pazienza, perché il processo prenderà diverse ore.

TROVARE IL PERCORSO DI UNA PERIFERICA

Prima di tutto bisogna saper individuare, senza errori, il percorso utilizzato dal sistema operativo per localizzare la periferica che vogliamo cancellare.
Se dobbiamo cancellare un disco interno, cominciamo smontando tutti gli hard disk esterni, chiavi USB, lettori di schede o altre periferiche attaccate al computer. Da una parte questo ci

SOMMARIO

Autoproduzione spinta & No-copyright: stampate, riproducete, diffondete.

CANCELLARE DEI DATI "PER DAVVERO"

Negli scorsi capitoli abbiamo visto che quando cancelliamo un file, il suo contenuto non viene davvero eliminato. Nonostante ciò, esistono dei programmi che permettono di cancellare dei file e il loro contenuto, o almeno che ci provano, con tutti i limiti che spiegheremo più avanti.

UN PO` DI TEORIA

IL METODO GUTMANN
La documentazione (1) del pacchetto secure-delete che utilizzeremo nella ricetta seguente, ispirata da una pubblicazione di Peter Gutmann pubblicata nel 1996 (2), dice:

Il processo di cancellazione funziona in questo modo:
- la procedura di distruzione (in modo sicuro) rimpiazza il contenuto di un file 38 volte. Dopo

CANCELLARE L'INTERO CONTENUTO DI UN DISCO

Aggiornamento: i software evolvono, per questo motivo è vivamente consigliato di utilizzare la versione più recente di questa ricetta, che è disponibile sul sito https://guide.boum.org/.

Durata: 5 minuti di preparazione, poi alcune ore di attesa a seconda della grandezza del disco.

Per cancellare un intero volume (disco o partizione), utilizzeremo il comando shred in modo da fargli sovrascrivere per tre volte con dei contenuti aleatori la totalità dei dati. Questo comando permette quindi, oltre alla cancellazione dei file, di sovrascrivere lo spazio cancellato in modo che diventi quasi impossibile ritrovare cosa contenesse in precedenza.
Per sovrascrivere il contenuto di un disco, non dobbiamo starlo utilizzando… se contiene il

su Mac), poi scrivere “term” e cliccare su “Terminale”.
Scrivere il comando seguente sostituendo LA_PERIFERICA con l’indirizzo della periferica che abbiamo trovato prima:

pkexec shred -n 3 -v LA_PERIFERICA

Se preferiamo utilizzare il metodo originale di Gutmann (più lungo, e forse più sicuro), dobbiamo sostituire -n 3 con -25.

Una volta scritto e controllato il comando, premere Invio. Ci verrà chiesta una password, perché questo comando necessita dei privilegi di amministrazione. A questo punto il comando shred scriverà sul terminale quello che sta facendo (perchè gliel’abbiamo chiesto noi, aggiungendo al comando shred l’opzione -v che in questo caso significa che il computer dovrà essere “verboso” – cioè “chiacchierone”):

shred: /dev/sdb: pass 1/3 (random)…
shred: /dev/sdb: pass 2/3 (random)…
shred: /dev/sdb: pass 3/3 (random)…

Alla fine di questa procedura, il terminale restituirà di nuovo il segno $, che indica il prompt. A questo punto possiamo chiudere il terminale.

RIUTILIZZARE IL DISCO

Attenzione, questo metodo non soltanto cancella i dati di un intero volume ma, alla fine dell'operazione, il disco non avrà più una tabella di partizioni, nè un file system. Per poterlo riutilizzare, è necessario creare da capo almeno una nuova partizione e il suo file system, attraverso l'utility Dischi, per esempio.

CANCELLARE "PER DAVVERO" UN INTERO DISCO

Prima di disfarsi di un hard disk, di riciclarlo, di installare un nuovo sistema operativo, o anche solo di mandare un computer rotto all'Assistenza, può essere saggio provare a mettere dei bastoni tra le ruote di chi volesse recuperare i dati che esso conteneva. Per farlo, la migliore soluzione è sempre quella di sovrascrivere tutto con cose a caso.
Prima di utilizzare questa ricetta, bisogna pensarci bene e farsi un attento backup dei dati che vogliamo conservare. Se applicheremo bene questa ricetta, essa renderà effettivamente i file molto difficili da recuperare, anche analizzando il disco in laboratorio.

Vediamo prima di tutto come cancellare tutto il contenuto di un disco, poi come rendere rapidamente inaccessibile il contenuto di una partizione cifrata.

ciascun passaggio, la cache del disco viene ripulita;
- il file viene smembrato, in modo che un attaccante non sappia quali blocchi del disco appartengano al file;
- il file viene rinominato, in modo che un attaccante non possa trarre conclusioni sul contenuto del file soppresso a partire dal suo nome;
- alla fine di tutto ciò, il file viene cancellato. ...

IL COMPROMESSO ADOTTATO

Lo studio di Peter Gutmann si basava su delle tecnologie di hard disk che al giorno d'oggi non esistono più. Alla fine del suo articolo, un paragrafo intitolato Epilogo in sostanza diceva che per un hard disk "recente" (3), le 38 scritture successive non sono più necessarie: basta sovrascrivere più volte i dati con degli altri dati aleatori. Ma apparte la natura e il numero delle riscritture, il processo che aveva descritto in modo sicuro e ripulire lo spazio disco con Nautilus Wipe".

IN UNA DEBIAN CIFRATA

Per cancellare dei file e il loro contenuto a partire dal file manager, risaliamo al file, clicchiamoci sopra con il destro e selezioniamo "Elimina". Si aprirà una finestra che ci chiederà di confermare l'eliminazione, proponendoci anche alcune opzioni.
Possiamo scegliere il numero di passaggi da effettuare per sovrascrivere i dati della nostra periferica e anche alcune opzioni di comportamento circa l'eliminazione dei dati. Le opzioni di default sono più che sufficienti per gli attuali hard disk.

Clicchiamo ora su Cancella. Una volta che la cancellazione è terminata, si aprirà una finestra "Cancellazione riuscita" per dare conferma che gli elementi siano stati eliminati con successo.

RENDERE IRRECUPERABILI DEI DATI GIÀ CANCELLATI

Aggiornamento: i software evolvono, per questo motivo è vivamente consigliato di utilizzare la versione più recente di questa ricetta, che è disponibile sul sito https://guide.boum.org/.

Durata: 5 minuti di preparazione, più da qualche minuto a qualche ora d'attesa, a seconda della dimensione del disco da ripulire e a seconda del metodo usato.

Se i file sono già stati cancellati senza precauzioni particolari, i dati che contenevano si trovano ancora sul disco. L'obiettivo di questa ricetta è quello di sovrascrivere quei dati superstiti, ripulendo lo spazio libero di un hard disk. Questo metodo quindi non cancella nessun file visibile nel gestore dei file.

Attenzione! Come gli altri metodi di cancellazione

Gutmann resta perfettamente attuale anche per gli hard disk odierni. Questo metodo non è però adatto per i dischi SSD. E dal momento che i dischi SSD attualmente stanno tendendo a rimpiazzare gli hard disk.....

Inoltre, il NIST (National Institute of Standards and Techonology, organismo governativo degli Stati Uniti che definisce i protocolli di sicurezza utilizzati, tra gli altri, dalle amministrazioni di quel paese) ha pubblicato di recente uno studio (4) della NSA, che sembra concludere che sugli hard disk moderni, i dati sono talmente appiccicati l'uno con l'altro che diventa praticamente impossibile affidarsi a delle analisi magnetiche per recuperare le tracce dei dati cancellati; in effetti, la densità dei dati degli hard disk è in continua crescita, per permettere di aumentare la capacità di stoccaggio.

Di conseguenza, nelle ricette seguenti ci accontenteremo di qualche passaggio aleatorio, rifacendoci alla messa in pratica del metodo originale di Gutmann.

Si tratta ancora una volta di trovare caso per caso un compromesso tra rapidità e livello di protezione desiderato, a seconda della grandezza dei dati da cancellare, dell'età dell'hard disk e di quanto ci fidiamo del NIST.

PENNE USB, DISCHI SSD E ALTRE MEMORIE FLASH

Riguardo alle penne USB o altre memorie flash – come le schede SD, o i dischi SSH – uno studio del 2011 (5) ha mostrato che la situazione è davvero problematica.

Questo studio dimostra che è impossibile, a prescindere dal numero di riscritture, avere la garanzia che tutto il contenuto di un file sia stato completamente sovrascritto. Anche se rendessimo inaccessibili i dati semplicemente

disco SSD) ci sono buone possibilità che il file risulti ancora leggibile in una zona inaccessibile della periferica!

INSTALLARE I PROGRAMMI NECESSARI

Se non l'abbiamo già fatto, bisogna installare nautilus-wipe e poi riavviare il computer.
Questo pacchetto è presente di default in Tails.

ELIMINARE DEI FILE E IL LORO CONTENUTO A PARTIRE DAL FILE MANAGER

IN TAILS

Per eliminare dei file e il loro contenuto utilizzando Tails, consultiamo la documentazione cliccando sull'icona Documentazione di Tails che si trova sul Desktop.
Cliccare su Documentazione, nel menù a destra. Dentro l'indice, cercare la sezione Cifratura e vita privata e cliccare sulla pagina "Cancellare dei file

di un file "per davvero", questo metodo non funziona con alcuni tipi di file system "intelligenti" che, per essere più efficaci, non mostrano al programma incaricato di coprire le tracce tutto lo spazio libero. Come abbiamo detto all'inizio del capitolo, non si deve fare affidamento su questo metodo per una penna USB, schede SD o dischi SSD ed è invece preferibile sovrascrivere più volte l'intero disco.

IN TAILS

Il pacchetto nautilus-wipe è già installato di default dentro Tails. Ci basta quindi consultare la documentazione cliccando sull'icona "Documentazione di Tails" che si trova sul desktop. Nel menù a destra, clicchiamo su Documentazione. Poi, all'interno dell'indice che si aprirà, cerchiamo la sezione "Cifratura e vita privata" e clicchiamo sulla pagina "Cancellare dei file in modo sicuro e ripulire lo spazio disco con Nautilus Wipe".

ELIMINARE DEI FILE E IL LORO CONTENUTO

Aggiornamento: i software evolvono, per questo motivo è vivamente consigliato di utilizzare la versione più recente di questa ricetta, che è disponibile sul sito https://guide.boum.org/.

Durata: 5 minuti di preparazione, più da qualche secondo a qualche ora d'attesa in base alla grandezza dei file da cancellare e del metodo usato.

Ecco quindi il metodo da seguire per sbarazzarsi dei file in modo tale da rendere illeggibile il loro contenuto.

Attenzione! Questo metodo funziona unicamente con gli hard disk meccanici. Se sovrascrivete il contenuto di un file all'interno di una penna USB (o su un altro supporto che utilizza la memoria flash come ad esempio una scheda SD o un

CON UNA DEBIAN CIFRATA

Se non l'abbiamo ancora fatto, installiamo il pacchetto nautilus-wipe e poi riavviamo il computer.

A questo punto apriamo il gestore dei file e risaliamo al disco che vogliamo ripulire. Clicchiamo col destro nella parte destra del gestore dei file e selezioniamo "Cancellare lo spazio disco disponibile". Si aprirà una finestra che ci chiederà di confermare la cancellazione dell spazio disco disponibile e ci proporrà anche qualche Opzione.
Possiamo scegliere il numero di passaggi effettuati per sovrascrivere i dati della nostra periferica e anche qualche opzione che riguarda il comportamento durante la cancellazione. Le opzioni di default sono sufficienti per gli hard disk attuali.
Adesso clicchiamo su "Cancellare lo spazio disco disponibile". La cancellazione può impiegare

togliendo la penna, essi sarebbero lo stesso visibili da chiunque guardasse direttamente dentro i chip della memoria flash.

Il solo metodo che ha funzionato in modo sistematico, è stato quello di riscrivere più volte completamente la penna USB. Nella maggior parte dei casi, due passaggi sono sufficienti, ma per alcuni modelli sono state necessarie venti riscritture prima che i dati scomparissero per davvero.

Dati questi presupposti, la soluzione preventiva pare essere quella di cifrare sistematicamente le penne USB, operazione che rende ben più difficile l'estrazione delle informazioni direttamente dai chip della memoria flash. E per ripulirle a posteriori, la formattazione per intero malgrado i suoi limiti, protegge almeno dagli attacchi via software.

diverso tempo. In alcuni casi ci verrà chiesta la password di amministrazione.

Vedremo che e' stata creata una cartella chiamata tmp.XXXXXXXXXXXX all'interno della cartella. Nautilus Wipe ci crea un file all'interno, aumentandone la grandezza fin che e' possibile, in modo da utilizzare tutto lo spazio libero disponibile e poi lo cancellerà in modo sicuro. Una volta finita la cancellazione, spunterà una finestra “La cancellazione è riuscita”, precisando che "Lo spazio disco disponibile sulla partizione o sulla periferica “…..” è stato ripulito con successo".

Nel prossimo numero:
Le ricette: partizionare e cifrare un hard disk, fare il bakup dei dati...

INIZIAMO

Quel che è possibile cancellare sono:

- i file singoli;
- un'intera periferica;
- dei file già cancellati.

NOTE:

1) Il file README.gz dentro /usr/share/doc/secure-delete all'interno di una distribuzione Debian.
2) http://gebeve.vado.li/ (in inglese)
3) Che utilizza la tecnologia PRML (http://matiga.vado.li/) , comparsa nel 1990 (http://gavide.vado.li/) (in inglese).
4) http://fetego.vado.li/ (in inglese).
5) http://dozesa.vado.li/ (in inglese)

ALTRI LIMITI DELLA CANCELLAZIONE “SICURA”

Sopratutto se se si utilizza un file system journaled come ext3, ext4, ReiserFS, XFS, JFS, NTFS oppure un sistema di scrittura, di compressione o di backup, sull'hard disk (per esempio il RAID) o via rete, possono ancora rimanere delle informazioni sui file che permettono di recuperarli. Ne abbiamo parlato nei capitoli precedenti.

RIGUARDO AGLI ALTRI SISTEMI

Abbiamo visto che se utilizziamo un sistema operativo proprietario, è un'illusione pensare di poter raggiungere una vera intimità. Anche se esistono dei programmi che dovrebbero eliminare i file e il loro contenuto sotto Windows e Mac OS X, è difficile pensare di poterci fare affidamento.