# Sicurezza del GRUB

## GRand Unified Bootloader

di Alessio Petracca

POuL
have a lot of fun...

# ...vedremo

- L'avvio
- Grub
- Ottenere una shell di root
- Protezione del Grub
- Protezione della fase di avvio

# L'avvio

- All'accensione del computer il processore resta inizialmente sospeso nello stato di RESET dall'hardware, finchè le tensioni di alimentazione non sono stabili.
- Appena il segnale di RESET viene disattivato il processore carica la sua prima istruzione, quasi sempre un JMP (salto incondizionato) che porta l'esecuzione al vero inizio del programma di firmware: il BIOS.

# L'avvio

All'accensione del computer, il controllo della prima fase è affidato al BIOS (Basic Input/Output System), che compie principalmente 2 fasi:

- Eseguire il POST (Power On Self Test)
  una serie di test diagnostici per verificare il corretto funzionamento dell'hardware

- Caricare in Ram il Master Boot Record
  (cilindro 0, testina 0, settore 1) i primi 512 byte del disco

# Boot loader

Nell'MBR troviamo un boot loader!

Un **boot loade**r è un programma, la cui funzione principale è quella di caricare in memoria il kernel di un sistema operativo e consegnare a lui il controllo dell'esecuzione.

# Alcuni boot loader famosi:

**LILO (LInux LOader)**- usato storicamente da Linux
**GRUB (GRand Unified Bootloader)** - usato nei sistemi Linux moderni
**SYSLINUX** - usato per l'avvio da CD (CD di installazione e live CD)
**BootX** - usato da Mac OS X
**NTLDR (NT loader)** - usato da windows NT e successivi

# Boot loader – LiLo

Nell' MBR può esserci un boot loader intero: LiLo

...il quale già conosce l'indirizzo fisico del kernel che poi provvederà ad eseguire...

# Boot Loader - Grub

Nell'MBR può esserci una parte di bootloader: Grub

Il Grub è più complesso ed è diviso in 2 stage:

- **Stage1**: è nell'MBR e si occupa di caricare il secondo stage
- **Stage2**: è sul filesystem, si occupa di mostrare a schermo il menù di avvio, individua l'indirizzo fisico del kernel da caricare, lo carica in Ram e gli passa il controllo

# Grub

Per funzionare correttamente, il Grub basa le sue regole principalmente su un file chiamato: /boot/grub/menu.lst

É proprio grazie a questo semplice file di testo che possiamo gestire l'avvio dei sistemi operativi elencati nella schermata di Grub al boot.

...diamo un'occhiata a questo file “dal vivo”...

# Ottenere una shell di root

Cosa può fare un malintenzionato di fronte al nostro computer spento?

...qualcuno di noi penserà: niente, non sa le password di root e di nessun utente sudoer...

SBAGLIATO!

...vediamo perchè...

# Protezione del Grub

Tra le tante opzioni mese a disposizione dal Grub, c'è anche la possibilità di proteggere il sistema attraverso l'impiego di una parola chiave.

# Protezione del Grub

La parola chiave viene definita inserendo nella sezione globale di configurazione
la direttiva **password**
*Es: password grubpassword*

In questo modo le prossime volte che vorrò editare i parametri del kernel dovrò inserirla.

# Protezione del Grub

Domanda: ad ogni avvio prima di scegliere il sistema operativo da avviare devo inserire questa password??

No, ovviamente no, a meno che non decido di bloccarlo.

# Protezione del Grub

É anche possibile proteggere l'avvio di un singolo OS, inserendo nella entry di quel sistema operativo la direttiva **lock**

*Es:*

```
title ArchLinux
lock
root (hd0,1)
kernel /vmlinuz26 root=/dev/sda2 ro
initrd /kernel26.img
```

# Protezione del Grub

Utilizzare delle password in chiaro non è mai una buona idea!

Il Grub ci viene incontro mettendoci a disposizione la possibilità di hashare la parola chiave con l'algoritmo MD5.

# Protezione del Grub

Per prima cosa si deve creare l'hash digitando:
# grub-md5-crypt

Dopo aver inserito 2 volte la password scelta, l'utility restituirà un hash, che basterà copiare nel file di configurazione, usando la direttiva **password**

Es: password --md5 $7909a3f00957937ad5d51e102bcgGHhp

# Protezione della fase d'avvio

Una password hashata md5 riuscirà a fermare il malintenzionato davanti al vostro pc?

No.

Abbiamo bisogno di una password anche al BIOS, per vietare il setup, in modo da non permettere a nessuno di modificare l'ordine dei dispositivi di boot.

# Protezione della fase d'avvio

Una password al BIOS riuscirà a fermare il malintenzionato (armato di giravite) davanti al nostro computer?

No.

Questa volta abbiamo bisogno di lucchetti!
Perchè basta rimuovere per qualche secondo la batteria tampone che è sulla scheda madre per resettare la password al BIOS.


Grazie per l'attenzione!!!