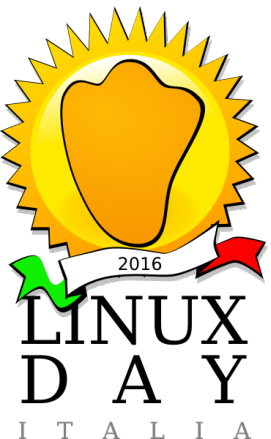
Installazione su disco criptato

Sossi Andrej – andrej.fil@gmail.com



Urban center - Fablab
Sabato 26 ottobre 2024

Informazioni sulla distribuzione

- Slackware nasce nel 1992 (pubblica nel 17 Luglio 1993)
- Nasce come una serie di bugfix della SLS
- È la distribuzione più longeva in ancora attiva e una delle più prolifere.
- Realizzata e gestita da Patrick Volkerding.
- Tranne in alcuni periodi nei quali si sono affiancati uno o due collaboratori (pagati) Patrick era e rimane l'unico a mantenere ed aggiornare la distribuzione.
- Comunità composta da tecnici molto esperti (grande comunità Brasiliana)
- Distribuzione molto “grezza” e “pura”
- Ottima per studiare e imparare Linux (imparare seriamente)

Informazioni sulla distribuzione

- Il motto

Chi impara RedHat conosce RedHat,

Chi impara Slackware conosce Linux!

- Oggi un po’ meno vero di una volta…

Slackware e sicurezza

- Il livello di sicurezza intrinseco della distribuzione è uguale al livello di sicurezza dei software sviluppati dai sviluppatori originali (cioè delle versioni “vanilla”)
- Le problematiche di sicurezza sono identiche alle problematiche di ogni distribuzione Linux
- Le soluzioni che funzionano in Slackware sono portabili
- I pochi fronzoli di Slackware non aiutano nel lavoro ma principalmente non lo ostacolano

Slackware e sicurezza

- Argomento molto complesso
- Dipende dalle possibili (probabili) minacce
- Ognuno di noi deve proteggere dei segreti (PIN del bancomat, svariate password di accesso, documenti aziendali, segreti aziendali, etc.)
- La protezione dei dati in un PC dipende da come gli utilizziamo e dai software che li trattano

Slackware e sicurezza

- Un portatile potrebbe essere dimenticato ed estratto il disco con i dati
- Criptare i singoli file è troppo oneroso (quanti, quali, quando e quante password???)
- Soluzione scelta è drastica e “logicamente” semplice:

  Criptare l'intero disco!

Come si può cifrare tutto? (1)

- TPM – **Trusted Platform Module**
- **è il nome con cui vengono indicate sia le specifiche per la costruzione di un microchip deputato alla sicurezza informatica, pubblicate dal Trusted Computer Group sia il chip stesso. Tale microchip viene generalmente implementato come modulo aggiuntivo per la scheda madre di un computer, ma si può trovare anche in palmari e in altri dispositivi elettronici.**

(fonte: https://it.wikipedia.org/wiki/Trusted_Platform_Modulehttps://it.wikipedia.org/wiki/Trusted_Platform_Module)

Come si può cifrare tutto? (1)

- **Tale chip era noto in precedenza come Chip Fritz, nome che deriva dal senatore statunitense Ernest "Fritz" Hollings, forte sostenitore di questo progetto. Lo scopo del TPM è l'aumento della sicurezza informatica: ogni chip è dotato di una coppia di chiavi crittografiche uniche, che lo rendono univocamente identificabile, e di un motore per la crittografia asimmetrica per la criptazione dei dati.**

(fonte: https://it.wikipedia.org/wiki/Trusted_Platform_Modulehttps://it.wikipedia.org/wiki/Trusted_Platform_Module)

Come si può cifrare tutto? (1)

- **Il TPM cripta tutto il traffico interno dell'elettronica (disco, scheda video, scheda audio,…)**
- **Presenti in tutti i PC moderni (disattivabile)**
- **Le chiavi di cifratura sono scritte (solamente) nel chip**
- **Se il PC non si accende il disco rimane indecifrabile**

Come si può cifrare tutto? (2)

- I vecchi PC si avviavano con il BIOS (Basic Input Output System)
- (Oggi con EFI si può emulare l'avvio con il CSM (Compatibility Support Module))

- Il boot del sistema lo fa il BIOS che non sa né decriptare né leggere i file
- Almeno qualcosa deve essere in chiaro (/boot)
- LILO deve essere installato in MBR (o nella root sector della partizione di boot)

Come si può cifrare tutto? (3)

- **I nuovi PC si avviano con EFI (UEFI Unified Extensible Firmware Interface)**
- **Il boot del sistema lo fa il UEFI che sa leggere solamente FAT32 e non sa decriptare**

- **Almeno qualcosa deve essere in chiaro (la partizione FAT32 – tipicamente la /boot/efi)**
- **Nella cartella /boot/efi/EFI/Slackware/ c'è il kernel, la ramdisk e il loader (elilo o grub)**

Come si può cifrare tutto? (2 e 3)

- Dopo il caricamento del kernel (sia via BIOS che UEFI) il resto procede nella maniera identica

- Il resto viene criptato e decriptato direttamente dal kernel e la(e) chiave(i) viene gestito da LUKS (Linux Unified Key Setup)
- I FileSystem viene gestito da LVM (Logical Volume Manager)
- Risultato finale: nessun programma deve fare operazioni particolari. La lettura e la scrittura dei dati cifrati vengono gestiti in maniera trasparente dal kernel.
  Carico maggiore per la CPU (non sensibile)
  Anche la SWAP è cifrata (anche ibernazioni sicure)

Comandi

```
# cfdisk /dev/sda                          # e creare 2 partizioni
# dd if=/dev/urandom of=/dev/sda2
# cryptsetup -s 256 luksFormat /dev/sda2
# cryptsetup luksOpen /dev/sda2 slackluks
# pvcreate /dev/mappers/slackluks
# vgcreate cryptvg /dev/mapper/slackluks
# lvcreate -L 1G -n swap cryptvg
# lvcreate -l 100%FREE -n root cryptvg
# vgscan --mknodes
# vgchange -ay
# mkswap -f /dev/cryptvg/swap
# setup                                    # eseguire l'installazione
```

Da non dimenticare

IMPORTANTE! Dopo un aggiornamento del kernel bisogna prima modificare il RAMDisk.

 # chroot /mnt
 # mkinitrd -c -k 5.15.19 -m ext4 -f ext4 -r /dev/cryptvg/root -C /dev/sda2 -L -l it

E modificare il link del kernel in caso di BIOS
#rm /boot/vmlinuz
#ln -s /boot/vmlinuz-generic-5.15.19 /boot/vmlinuz

O copiare i file nel caso di UEFI
#cp /boot/vmlinuz-generic-5.15.19 /boot/efi/EFI/Slackware/vmlinuz
#cp /boot/initrd.gz /bot/efi/EFI/Slackware/

Licenza d'uso di questo documento

CopyLeft 2024 – Sossi Andrej
andrej.fil@gmail.com