[FORT] Tema 2: Securizando el Arranque

Es una de las partes que más dependen del hardware. En intel coexisten 2 métodos de arranque: BIOS o Legacy y UEFI:

- BIOS:
- UEFI:

ARM utilizaun sistema de Arranque similar a UEFI, mientras que SBCs como raspberry usan BIOS.

Proceso de arranque

1. Se ejecuta el código de la BIOS (Firmware) guardado en una ROM.
    - Se realiza un POST (Power On Self Test)
    - Se hace una prueba de la memoria
2. Tras eso viene el cargador, un programa lo suficientemente simple para ser ejecutado por el firmware y lo suficientemente sofisticado como para cargar el Sistema Operativo. En linux se usa GRUB (Grand Unified Boot Loader).
    - El cargador debe saber donde está el kernel para cargar el sistema operativo.
    - El cargador debe esta en el primer bloque de memoria
    - Es un archivo en un formato especial llamado .EFI en el caso de UEFI (localizados en /boot/efi/EFI).
    - Linux es un sistema operativo modular, por lo que se carga lo que es necesario en el arranque, haciendo que sea muy rápido.
    - En el caso de Linux el cargador debe saber donde están los diferentes módulos del sistema (Directorio /boot para kernel y /lib/modules para los módulos).
    - Los módulos se almacenan en el initrd agrupados (Initial Ram Disk).
    - Con “efibootmgr” se puede modificar el orden de arranque UEFI.
    - Con “efibootmgr -v” se pueden ver los archivos de arranque UEFI.
    - El cargador tiene un archivo de configuración que le dice que sistema operativo tiene que cargar.
3. Arranca el sistema operativo

Configurar Consola del Grub

```
ls #Para ver las particiones
set root=hd0,msdos3 #Seleccionamos partición
ls / #Vemos que hay en la partición en cuestión
linux /boot/vmlinux-amd64 #Le decimos donde está el kernel a GRUB
initrd /boot/initrd-nombre root=/dev/sda1 #Le decimos donde está Initrd y donde están los ficheros al GRUB
boot
```

Vulnerabilidades en el proceso de arranque

Se le debe poner una contraseña al Firmware para cambiar la configuración (También se puede hacer

para cada vez que se arranca, pero esto hace que sea tedioso arrancarlo.) Introduciendo parámetros en GRUB es posible acceder al Root del equipo, lo que es una vulnerabilidad muy grave.

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:fortificacion:tm2

Last update: **2025/02/24 14:43**