Bootloader

Bootloader je program, který se nachází v pevné paměti zařízení a jehož jediným úkolem je načíst operační systém do operační paměti (RAM) a následně mu předat řízení.

V okamžiku, kdy zapnete počítač, procesor neví, kde se nachází Windows, Linux nebo macOS. Ví pouze to, jak spustit instrukce z firmwaru (BIOS nebo UEFI). Právě tento firmware najde a spustí bootloader.

Jak Bootloader funguje?

Proces zavádění probíhá v několika fázích (tzv. Chain Loading):

```
1. **Inicializace (POST):** Hardware provede vlastní testy.
2. **Lokalizace:** Firmware prohledá připojená média (disky, USB) a hledá zaváděcí sektor nebo EFI soubor.
3. **Stage 1:** Načte se velmi malý kód (např. z MBR), který má pouze dostatek informací k tomu, aby našel zbytek bootloaderu.
4. **Stage 2:** Načte se hlavní část bootloaderu, která již umí číst souborové systémy. V této fázi se často zobrazuje menu pro výběr operačního systému.
5. **Zavedení jádra:** Bootloader najde na disku jádro ([[kernel]]) operačního systému, nahraje ho do RAM a spustí.
```

Nejčastější Bootloadery

Různé platformy používají různé zaváděcí programy:

- **GRUB (Grand Unified Bootloader):** Standard pro většinu distribucí Linuxu. Je velmi flexibilní a umožňuje multiboot (výběr mezi více systémy).
- **Windows Boot Manager (BOOTMGR):** Standardní zavaděč pro moderní systémy Windows.
- **LILO (LInux LOader):** Starší, dnes již méně používaný zavaděč pro Linux.
- **U-Boot:** Často používaný v embedded systémech a chytrých zařízeních (např. routery, Android telefony).

Bootloader v mobilních zařízeních

U chytrých telefonů (zejména s Androidem) je stav bootloaderu klíčový pro bezpečnost a modifikace:

- **Zamknutý (Locked):** Výrobce dovoluje spustit pouze autorizovaný operační systém. To chrání uživatele před instalací škodlivého softwaru na úrovni systému.
- **Odemknutý (Unlocked):** Umožňuje instalaci alternativních systémů (Custom ROM) nebo získání práv root. Odemknutí obvykle znamená ztrátu záruky a vymazání dat z důvodu bezpečnosti.

Rizika: Bootkity a zranitelnosti

Jelikož bootloader běží dříve než antivirus, je ideálním cílem pro pokročilý malware.

- **Bootkit:** Škodlivý kód, který se zapíše do bootloaderu. Dokáže skrýt svou přítomnost tak dokonale, že o něm operační systém vůbec neví.
- **Obrana:** Moderní systémy používají **Secure Boot**, který pomocí digitálních podpisů ověřuje, zda nebyl bootloader změněn útočníkem.

Rozdíl mezi Bootloaderem a BIOSem

Prvek	Umístění	Úkol
BIOS/UEFI	Čip na základní desce (Firmware)	Testování hardwaru, nalezení bootloaderu.
Bootloader	Pevný disk (MBR/GPT)	Načtení a spuštění operačního systému.

Související pojmy: BIOS, UEFI, Kernel, RAM, MBR, GPT, Secure Boot, Bootkit.