OPEN SOURCE FIRMWARE

LinuxBoot

- Variedad de dispositivos
- Depende del modelo
- Poca comunidad interesada
- Falta de desarrollo

Desafíos

Intel's Boot Guard

Verifica el firmware

Root of Trust

PRIVADO de Intel

Verificar el SW, en cada elemento

Componentes del sistema

Sistema operativo

Acceso

Kernel

Firmware

Privilegiado
poca visibilidad

Producido por el fabricante

Vulnerabilidad / ¡Poca Seguridad!

Open Source Firmware

Objetivo

Transparencia de Firmware
Seguridad
Control de daños

Tipos de Firmware

Esta presente en diversos aparatos, algunos ejemplos son;

- EC,
- TPM.
- GPU
- NIC
- SSD/HDD
- BMC
- eMMC
- CPLDs
- Ventiladores
- Fuente de alimentación

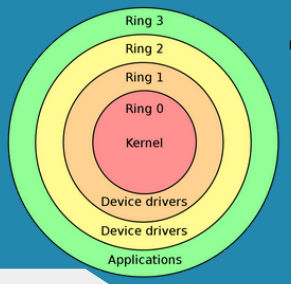
Proyectos

Firmware de código abierto

u-boot coreboot

LinuxBoot

Niveles de privilegio



Extrema Precaución

Anillo -3

Motor de gestión
SO Minix

Anillo -2

SMM

Recursos del CPU
Invisible al resto de la pila
Manejo de energía
Control de HW
Eventos del sistema

UEFI

Interfaz entre SO y BIOS firmware

Funciones

- Limitaciones de Direcciones
- Criptografia
- Redes
- Autenticación
- Servicios de booteo
- Servicios corriendo

APLICACIONES
UEFI shell, GRUB, Gummiboot,Windows Boot Manager

Vive en el firmware del Microprocesador

Causar daños = peligro

Morales Ortega Carlos