FIRMWARE DE CÓDIGO ABIERTO

FIRMWARE PROJECTS

- U-BOOT: LAS CHROMEBOOKS DE GOOGLE USAN COREBOOT EN X86 Y U-BOOT PARA EL RESTO, EL ARRANQUE VERIFICADO REDUCE EL RIESGO DE MALWARE, PERMITE ACTUALIZACIONES DE SOFTWARE SEGURAS Y ASEGURA LA INTEGRIDAD DEL SOFTWARE EN EL DISPOSITIVO
- LINUX BOOT: MANEJA LOS CONTROLADORES DE DISPOSITIVOS, ADMINISTRA LA PILA DE RED Y PROPORCIONA UN ESPACIO MULTIUSUARIO Y MULTITAREA

ROOT FOR TRUST

LA META DE LA RAÍZ DE CONFIANZA DEBERÍA SER VERIFICAR QUE EL SOFTWARE ISTALADO EN CADA COMPONENTE DE HARDWARE ES EL QUE ESTABA DESTINADO.
DE ESTE MODO SE PUEDE SABER SIN ALGUNA DUDA Y VERIFICAR SI EL HARDWARE HA SIDO HACKEADO

KERNEL

EL KERNEL CONTROLA EL ACCESO A LOS RECURSOS DEL SISTEMA. CONTIENE LA LÓGICA PARA PERMITIR MULTIPLES PROCESOS PARA COMPARTIR MECANISMOS DE HARDWARE COMO LA MEMORIA, EL CPU Y LA ENTRADA/SALIDA.

ENTRE LOS ANILLOS -2 Y -3

AQUÍ HAY AL MENOS 2 Y MEDIO KERNELS QUE TIENEN VARIAS CAPACIDADES, CADA UNO DE ELLOS TIENE SU PROPIA PILA DE REDES Y SERVIDORES WEB, LO CUAL ES POTENCIALMENTE PELIGROSO, SOBRE TODO SI NO QUIERES QUE SE CONECTEN A LA RED PARA ACTUALIZARSE POR SÍ SOLOS. SU CÓDIGO TAMBIÉN SE PUEDE MODIFICAR POR SÍ SOLO Y PERSISTIR POR CICLOS DE ENERGÍA Y REINSTALACIONES.

FIRMWARE

EL FIRMWARE INICIALIZA EL SISTEMA OPERATIVO CON UN GESTOR DE ARRANQUE. EL FIRMWARE VIVE EN LA MEMORIA SSD, MOUSE, TECLADO, CPU, ETC.

ANILLO -2

EL SSM ES INVISIBLE PARA LA PILA QUE ESTÁ ENCIMA, ERA USADO ORIGINALMENTE PARA LA GESTIÓN DE PODER Y EL CONTROL DEL HARDWARE DEL SISTEMA. MANEJA LOS EVENTOS DEL SISTEMA COMO LA MEMORIA O LOS ERRORES DE CHIP.
UEFI ES LA INTERFAZ ENTRE EL SISTEMA OPERATIVO Y EL FIRMWARE DEL BIOS, Y SU KERNEL ES UN VECTOR COMÚN DE VULNERABILIDADES DESDE QUE TIENE ALGO DEL CÓDIGO PROPIETARIO USADO EN VARIAS PLATAFORMAS

PROBLEMAS DEL FIRMWARE

LOS "EXPLOITS" EN EL FIRMWARE PUEDEN CAUSAR MUCHOS DAÑOS DEBIDO A LAS VARIAS OPERACIONES PRIVILEGIADAS DE LAS QUE EL FIRMWARE ES RESPONSABLE. TAMBIÉN, EL CÓDIGO QUE CORRE EL MAYOR PRIVILEGIO TIENE LA MENOR VISIBILIDAD, ESTO CONDUCE A INCIDENTES QUE PUEDEN AFECTAR A LOS SUSUARIOS EN MÚLTIPLES PLATAFORMAS SIMULTÁNEAMENTE.

NIVELES DE PRIVILEGIO 2

- ANILLO -2: "MODO DE ADMINISTRACIÓN DEL SISTEMA (SMM), INTERFAZ EXTENCIBLE UNIFICADA DEL FIRMWARE". ES PREOPIETARIO DEL CÓDIGO QUE CONTROLA TODOS LOS RECURSOS DE LA CPU.
- ANILLO -3: "MOTOR DE GESTIÓN". ES PROPIETARIO DEL CÓDIGO QUE CORRE EL TIEMPO QUE LA TARJETA MADRE RECIBE ENERGÍA.

NIVELES DE PRIVILEGIO

- ANILLO 3: "USERSPACE". EN ESTE ESPACIO CORREN LOS PROGRAMAS DEL USUARIO Y ES EL ANILLO CON MENOS PRIVILEGIOS
- ANILO 0: "KERNEL". ESTE ES EL KERNEL DEL SISTEMA OPERATIVO; ALGUNOS SO DE CÓDIGO ABIERTO PERMITEN LA VISIBILIDAD DETRÁS DEL KERNEL
- ANILLO -1: "HYPERVISOR". ESTE MONITOR DE MÁQUINA VIRTUAL CREA Y CORRE MÁQUINAS VIRTUALES.