

Tabla de contenidos

El autor	- 7 -
Prólogo	- 9 -
Recordatorio sobre el espacio de trabajo	- 11 -
Para quién es este libro	- 13 -
¿Cómo leer este libro?	- 15 -
Introducción	- 19 -
Saca el máximo partido de leer este libro.....	- 20 -
Convenciones en el libro.....	- 20 -
Detalles sobre las fuentes	- 22 -
Repositorio en Github	- 22 -
Alcance de este libro.....	- 22 -
Contactar.....	- 23 -
¡Deja una revisión!	- 23 -
Capítulo 1. Introducción a UEFI.....	- 25 -
CSM y UEFI clases de 0 a 3	- 26 -
¿Qué es Secure Boot?	- 27 -
Arranque con UEFI.....	- 31 -
Capítulo 2. Un bootloader simple UEFI	- 32 -
QEMU y BIOS UEFI	- 33 -
El disco: <code>disk.img</code>	- 34 -
Una prueba con GRUB	- 39 -
Una prueba con nuestro <code>initrd</code> personalizado	- 44 -
Disco maestro: <code>disk_master.img</code>	- 49 -
Bootloader simple con EFI.....	- 52 -
Capítulo 3. Mejorando nuestra aplicación EFI	- 70 -
Eliminar (algunos) de los mensajes en arranque.....	- 72 -

Bootloader en C/C++.....	- 80 -
GNU-efi	- 80 -
Usando MingW	- 94 -
EDK II	- 98 -
Primera aplicación con EDK II.....	- 114 -
Parámetros para la aplicación EFI	- 135 -
Capítulo 4. bootloader mejorado (gnu-efi).....	- 138 -
Qué son los GUID.....	- 138 -
uefi_call_wrapper.....	- 143 -
¿Qué es BS (Boot Services)?.....	- 145 -
¿Qué es RT (Runtime Services)?.....	- 148 -
¿Qué es ST (SystemTable)?.....	- 151 -
Leer ficheros	- 152 -
Capítulo 5. bootloader mejorado (EDK II)	- 178 -
Reutilizar edk2 del Capítulo 3	- 179 -
Actualizando Makefile para edk2	- 179 -
bootloader.c para EDK II	- 182 -
Capítulo 6. Cargar el kernel de Linux e initrd	- 194 -
Modificar el Makefile	- 195 -
Bootloader.c: cargando kernel e initrd.....	- 197 -
Cargar el kernel.....	- 201 -
Cargar initrd	- 201 -
Capítulo 7. UEFI y la red con edk2.....	- 204 -
QEMU y los interfaces de red	- 204 -
QEMU “-netdev”	- 205 -
QEMU “-device”	- 207 -
Servidor TFTP integrado	- 207 -

Configurando un tap	- 208 -
Interfaces de red disponibles	- 209 -
IPv4 válida	- 220 -
Implementando un Ping básico	- 223 -
Bloque 1: el paquete ICMP	- 236 -
Bloque 2: el token de transmisión	- 238 -
Bloque 3: el evento de envío (transmisión)	- 239 -
Bloque 4: el envío (la transmisión real)	- 240 -
Bloque 5: la recepción (echo-reply)	- 242 -
Conexión TCP válida	- 248 -
Una conexión HTTP	- 263 -
Capítulo 8. UEFI y la red con gnu-efi	- 278 -
ip.efi	- 279 -
Reflexiones finales	- 284 -
Capítulo 9. EFI STUB para el kernel de Linux	- 287 -
Kernel como aplicación EFI	- 287 -
startup.nsh	- 292 -
Nuestro STUB EFI que carga el kernel	- 293 -
Analicemos un poco el binario de STUB	- 310 -
Capítulo 10. Herramientas diversas	- 321 -
Esperar la pulsación de una tecla	- 321 -
Borrar la pantalla	- 323 -
Función Sleep	- 324 -
Datos de fecha y hora	- 325 -
Detalles del sistema - firmware	- 332 -
Detalles del binario del kernel	- 333 -
Capítulo 11. Breve contacto con Secure Boot	- 337 -

Conceptos importantes iniciales	- 337 -
Herramientas necesarias	- 338 -
Generando claves para UEFI.....	- 339 -
Platform Key (PK).....	- 339 -
Key Exchange Key (KEK)	- 340 -
Certificado de firma (para la db)	- 341 -
Cadena de confianza	- 342 -
Firmando la primera aplicación UEFI.....	- 343 -
Llevar las claves al mundo UEFI.....	- 344 -
Creamos un disco rápido de pruebas	- 347 -
Arrancamos QEMU	- 348 -
Copiar los ficheros OVMF localmente.....	- 348 -
Enrolar la clave PK	- 349 -
Enrolar claves desde el EFI shell.....	- 361 -
Enrolar claves desde una aplicación EFI	- 364 -
Claves MOK.....	- 366 -
Capítulo 12. Algunas conclusiones	- 391 -
Finalmente, ¿gnu-efi o edk2?	- 391 -
Conectividad de red	- 393 -
El infame goto.....	- 394 -
La especificación	- 394 -
Capítulo <EOT>: nuevos libros y trabajo futuro.....	- 402 -
Anexo I. Comandos del shell EFI	- 406 -
map - muestra discos y particiones.....	- 406 -
smbiosview - información de SMBIOS	- 407 -
devicetree - árbol de dispositivos	- 413 -
pci - examina el bus PCI.....	- 413 -

dh - mostrar handles	- 414 -
comp - comparar ficheros	- 416 -
ifconfig - configuración de red	- 417 -
tftp - descargar desde un servidor tftp	- 418 -
vol - información sobre volúmenes de disco.....	- 421 -
bcfg - opciones de arranque	- 421 -
memmap - mapa de memoria disponible.....	- 423 -
dmem - vuelca memoria.....	- 424 -
dmpstore - volcar variables UEFI.....	- 425 -
Anexo II. TPM	- 428 -
PCRs	- 429 -
Measured Boot (Arranque Medido).....	- 430 -
Sealed Storage (Almacenamiento Sellado).....	- 431 -
Attestation (Atestación)	- 431 -
El emulador de TPM	- 434 -
Anexo III. Vulnerabilidades e incidentes UEFI	- 439 -
Anexo IV. Multihilo (falso).....	- 445 -
El primer enfoque obvio: polling	- 446 -
Usar eventos	- 447 -
Jugando con múltiples procesadores.....	- 447 -
Referencias.....	- 451 -