UEFI – Security Boot

“Reparacion y Mantenimiento de PC con Herramientas Libres – Laboratorio Gugler”

Autores:

- Alvarez Joel
- Zapata Luciano

Año:

- 2015

Bibliografía:

- Experiencias personales e Investigación propia (Papers).
- Pagina web: “www.howtogeek.com”

  “www.taringa.net”

  “www.hp.com”

INDICE:

Sistema de arranque UEFI

Introducción:

Cuando se enciende una computadora se realiza una serie de pasos antes de que arranque el sistema operativo.

Cuando eso ocurre se lanza un software de bajo nivel que se halla en la motherboard conocido como BIOS y se ejecuta una rutina llamada POST (Power On Self Test) que incluye un conjunto de instrucciones de comprobación de hardware.

Luego se lee el primer sector del disco duro o sector de inicio del mismo, (en caso de seleccionar un HDD como dispositivo primario de booteo) llamado MBR (Master Boot Record), donde se encuentra un pequeño programa denominado gestor de arranque. Este permite al usuario seleccionar el sistema operativo que quiere utilizar si es que en la computadora existe mas de uno o distintas versiones del/los mismos .

El BIOS se utiliza en computadoras desde la década de los 80's, con pocas modificaciones desde entonces, manteniendo siempre retro-compatibilidad, esto provoca limitaciones de direcciones de memoria de 20 bits y limita el tamaño del gestor de arranque a 440 bytes. Estas limitaciones no son aceptables en la actualidad considerando que los gestores de arranque modernos leen múltiples sistemas de archivo, muchas veces tienen interfaces gráficas con imágenes de fondo, teniendo que cargar en memoria múltiples kernels de distintos formatos, los cuales ocupan mucho más que 440 bytes . Esto hace que en la actualidad los gestores funcionen en múltiples etapas haciendo que el proceso de arranque sea mas complejo que lo que debería ser, estos problemas son solucionados con UEFI.

UEFI nace a partir de UEFI Forum que es una alianza entre varias compañías líderes en tecnología, entre ellas Intel y Microsoft, con el objetivo de modernizar el proceso de arranque.

UEFI es la evolución de EFI (Extensible Firmware Interface) que es una especificación desarrollada por Intel, un anexo entre el SO y el firmware, lo cual puede verse como una alternativa de reemplazo de la BIOS presentando mejoras tales como la cantidad de particiones y capacidad máxima del dispositivo particionado utilizando el sistema GPT. UEFI aporta criptografía, autenticación por red, seguridad a nivel hardware e interfaz gráfica entre otras cosas.

Algunas diferencias que podemos destacar entre UEFI, EFI y una BIOS es que entre las primeras es que EFI es una especificación de Intel como alternativa a la BIOS, que no posee interfaz gráfica, y utiliza el sistema GPT que soluciona el problema de limitación de particiones del MBR. La misma, luego paso a llamarse UEFI en referencia a Unified EFI, al momento en que se unificaron otras empresas tales como AMD, HP, American Megatrends, Apple, Dell, etc. UEFI aporta a EFI criptografía, autentificaron por red y una interfaz gráfica.

EFI / UEFI se diferencian de una BIOS común, mas allá de que anteriormente aclaramos que UEFI es una aplicación que suplanta a la BIOS trabajando como una interfaz de la misma, siendo mas amigable y comprensible para el usuario; superando ciertas limitaciones del anterior sistema relacionadas a la seguridad, compatibilidad y administración de recursos.

UEFI y la relación con el SO de Microsoft

Una de las cuestiones mas planteadas es la relación costo beneficio que se presenta respecto a las desventajas en cuanto a incompatibilidad por parte de los

Sistemas Operativos que no pertenecen a la empresa Microsoft, y que tanto se benefician los usuarios de Windows al utilizar el SO creado por la misma empresa miembro de la alianza UEFI Forum y a su ves dueño de UEFI.

Dicha limitación puede darse a travez de una capacidad que incluye UEFI en sus ultimas versiones que es el estándar “Secure Boot”.

Recordemos que la especificación EFI es propia de Intel, y la especificación UEFI es propiedad de UEFI Forum.

Secure Boot

Secure Boot propone mecanismos para tener un proceso de arranque seguro y libre de código malicioso. De ser bien implementados, estos mecanismos pueden ser aprovechados por cualquier SO libre o privativo para garantizar un arranque donde no sea posible la ejecución de código malicioso. Sin embargo si este mecanismo no es implementado de forma completa o correcta puede ser restrictivo impidiendo la instalación de sistemas operativos que no sean de Microsoft, lo que afecta la libertad de optar por otros sistemas operativos.

Esta especificación propone utilizar un par de claves asimétricas, una publica y la otra privada, la primera se guarda en el firmware y cada ejecutable UEFI estará firmado con una clave privada por el proveedor autorizado; fallando la autorización si, esta esta vencida, no es confiable o no corresponde con el ejecutable analizado porque fue alterado.

-Los equipos que cumplan con la especificación UEFI de Secure Boot deben contar con dos modos:

Modo Setup: En este modo el Firmware no verifica el gestor de arranque ni que los drivers estén firmados por clave confiables.

Modo usuario: En este modo solamente es posible cargar drivers y aplicaciones UEFI firmados con claves confiables. Sera fallido cualquier intento de cargar un gestor de arranque sin firmar.

-Se utilizan dos clases distintas de pares de claves asimétricas:

Key Exchange Keys (KEKs): Se utiliza para establecer una relación de confianza entre el sistema operativo y el firmware de la plataforma.

Platatform Key (PK): su función es establecer una relación de confianza entre el dueño de la plataforma y el firmware.

Además de la PK y la base de datos KEKs, el firmware debe almacenar una base de datos de firmas aceptadas (DB) y no aceptadas (DBX) de manera que al arrancar el sistema se verifica que cada aplicación o driver UEFI tenga su firma registrada en DB y no en DBX, si esto se cumple el driver o aplicación se ejecuta, pero de no ser asi, no lo hará.

Para modificar las bases DB y DBX hay que contar con la parte privada de la clave PK o de alguna KEK. Hasta que no se registre la PK, la plataforma opera en modo “Setup”. En este modo el firmware no debe requerir autenticación para modificar la PK o la base de datos KEK.

Como se dijo anteriormente Secure Boot propone un mecanismo para tener un proceso de arranque seguro pero su mala utilización (intencional o no) puede ser muy restrictivo no dejando instalar Sistemas Operativos que no sean de Microsoft, esto es el caso de la certificación de Microsoft Windows que exige que los equipos tengan Secure Boot habilitado por defecto y plantea que la clave PK es controlada por el fabricante y no por el dueño del equipo que es lo que propone el estándar UEFI. Esta es una

diferencia fundamental entre el estándar y la certificación de Windows que tiene que ver con la libertad de elección del software a instalar.

Para resumir, podríamos decir que desde un punto de vista general, la implementación del Secure Boot presente en UEFI, nos brinda seguridad a un nivel mas profundo, mas presenta el inconveniente de volverse privativo en potencia, al restringir o dificultar de cierta forma la instalación de otros Sistemas Operativos tales como las múltiples versiones y/o distribuciones de GNU/Linux.

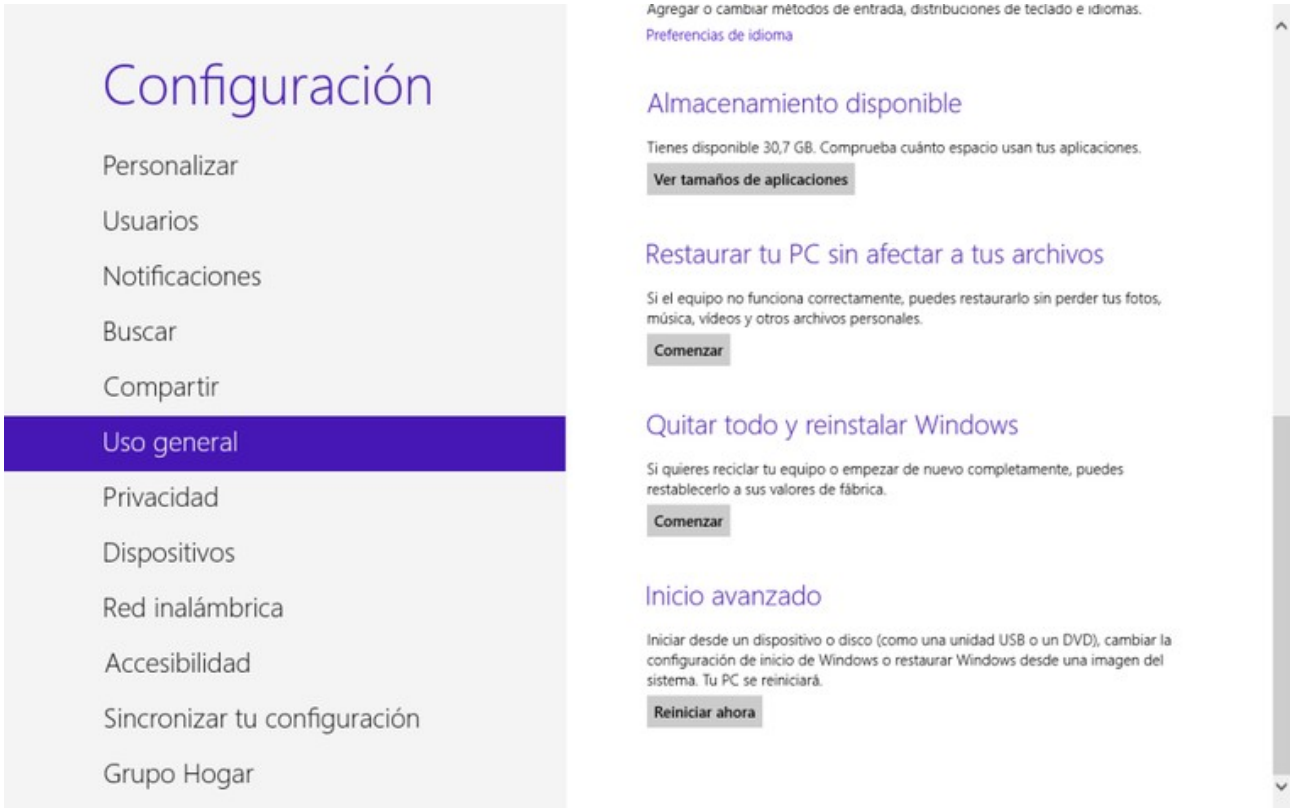
Adentrándonos ahora en casos prácticos, veremos de que manera actúa UEFI a la hora de instalar un nuevo sistema operativo en una PC. Ya sea perteneciente a Microsoft o sea de libre distribución.

CASO 1: ¿Como deberíamos proceder en caso de querer instalar Ubuntu (Derivado de Debian) en una PC que ya poseía instalado Windows 7 u 8 (Microsoft)?

Teniendo preparados los elementos necesarios para la instalación (Imagen del SO montada en alguna memoria flash, disco extraíble; y la PC en la que instalaremos el nuevo sistema)

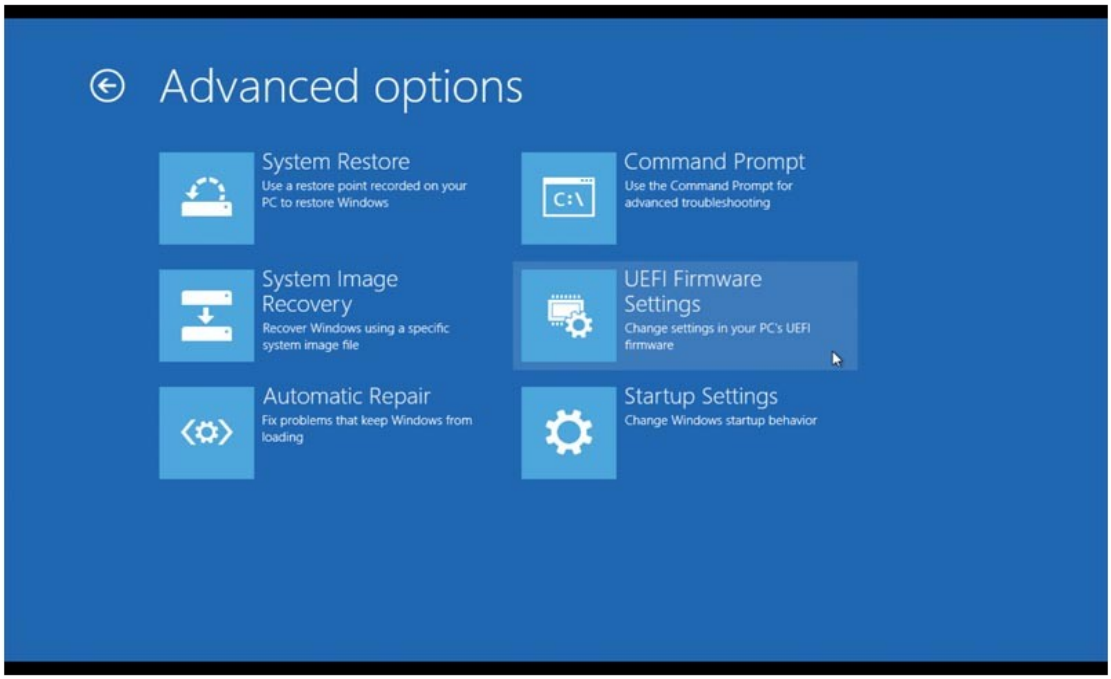
Paso 1: Preparar nuestro sistema para la instalación.

-Nos dirigimos a: >>Configuración de nuestro sistema>>Cambiar configuración del PC>>Uso general. Hacemos clic en “Inicio avanzado” y luego en “Reiniciar ahora”.



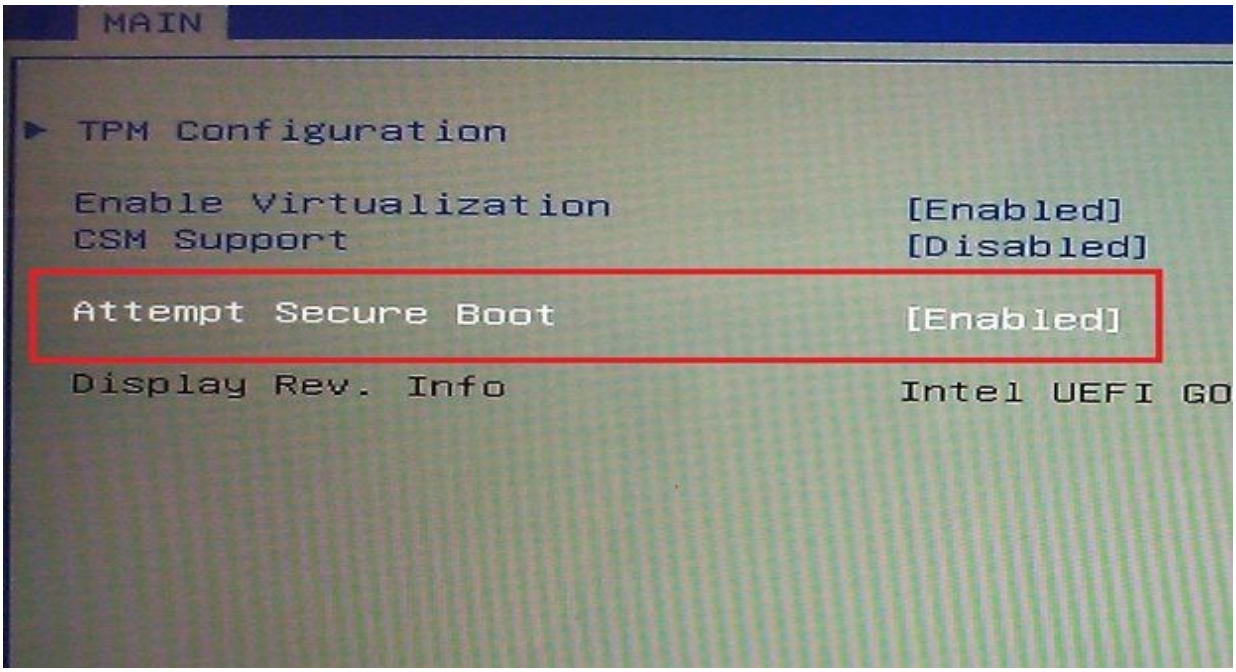
(Imagen extraida de: “http://www.taringa.net/post/info/16700378/Desactivar-secure-boot-Windows-8.html”)

-Al reiniciar seleccionamos la opción “Solución de problemas”, “Opciones avanzadas”, “Configuración UEFI” (UEFI Firmware Settings, en la imagen)y por ultimo Reiniciar.



(Imagen extraida de: “http://h30434.www3.hp.com/t5/Desktop-Operating-Systems-Software-Recovery/Accessing-UEFI-BIOS-in-Windows-8/td-p/2415097”)

-Cuando inicie nuevamente vamos a la pestaña Boot y desactivamos la opción Fast Boot. También nos dirigiremos a la pestaña Security y desactivamos la opción Secure Boot Control.



(Imagen extraida de: “http://www.taringa.net/post/info/16700378/Desactivar-secure-boot-Windows-8.html”)

-Guardamos cambios y reiniciamos.

-Repetimos el paso 1

Paso 2: Instalar el nuevo sistema operativo.

-Al reiniciar, esta vez seleccionaremos la opción “Usar un dispositivo”.

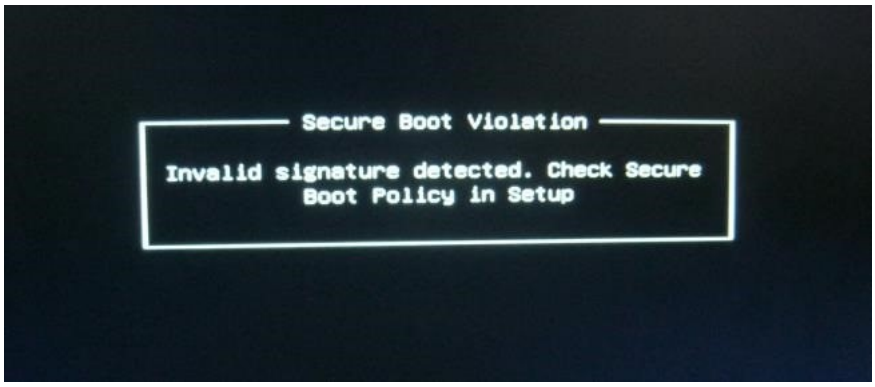
-Cuando inicie nuevamente seleccionaremos la unidad en la que tenemos la imagen del nuevo sistema operativo, y a partir de ahí, seguiremos los pasos habituales para la instalación de nuestro sistema operativo Ubuntu.

CASO 2: ¿Como deberíamos proceder en caso de querer instalar Fedora (Derivado de Red Hat) en una PC que ya poseía instalado Windows 7 u 8 (Microsoft)?

En este caso debemos proceder de la misma manera que en el CASO 1. La única diferencia radica en la forma de instalar el nuevo sistema, los pasos serán diferentes, pero la preparación de el equipo para su instalación es la misma.

Cita: “Añadir una clave de inicio al firmware de la UEFI: -Puede que algunas distribuciones de linux firmen sus boot loaders con una clave propia, la cual puede ser añadida al firmware de tu propia UEFI. Mas esto no parece ser algo muy común por el momento.” (Extraido de http://www.howtogeek.com/175641/how-to-boot-and-install-linux-on-a-uefi-pc-with-secure-boot/)

ATENCION: ¿Que pasaría si intentamos bootear desde una unidad deferente a la cual teníamos instalado nuestro SO predeterminado?



(Imagen extraida de: http://www.howtogeek.com/175641/how-to-boot-and-install-linux-on-a-uefi-pc-with-secure-boot/)

Este mensaje de error aparecerá al intentar violar el Secure Boot.

Conclusión: Dependiendo de la persona, la finalidad que busque, y la actividad que desea realizar, la UEFI y su security boot podrían presentar diversas ventajas y desventajas. Para el usuario común, el funcionamiento de su PC no cambiaría prácticamente en nada, por lo que un análisis desde su punto de vista es casi innecesario. Para un reparador de PC, o aquella persona que desee modificar el funcionamiento de su sistema, ya sea por la actualización del mismo, o por el cambio de su SO, se encontraría con barreras que antes no conocía, ya que de su procedimiento habitual, que comúnmente le llevaría unos cuantos minutos, ha pasado a una tarea que requiere su atención por al menos 1 hora. Mas debemos tener en cuenta el hecho de que esta característica nos proporciona una ventaja en cuanto a seguridad, la incapacidad de “robar” nuestra unidad de almacenamiento para ser usada en otro equipo y así lucrar de esta manera, o robar la información del usuario.