# “Windows 8, Secure Boot and Linux Installation”

Tanto si planeamos utilizar Windows 8 o no, cualquier que compre un PC actualmente acabará con una máquina que tiene la utilidad “*Microsoft-driven Secure Boot*” activada. *Secure Boot*  evita que sistemas operativos no autorizados u otro software se puedan cargar durante el arranque.

*Secure Boot* es una característica activada por UEFI (“*Unified Extensible Firmware Interface”)* que reemplaza al BIOS tradicional del PC. Cualquier computador con una pegatina Windows 8 tendrá *Secure Boot* activado.

## Ventajas de *Secure Boot*  para promover la seguridad

El BIOS tradicional arrancará con cualquier software de Sistema operativos (Windows, Linux, etc.). Normalmente el BIOS carga el programa de arranque de Windows o de Linux (por ejmplo el GRUB). Sin embargo, es posible que un *software malicioso (“malware”)*, tal como un rootkit, pudiera reemplazar al cargador de arranque. El *rootkit* podría cargar nuestro sistema operativo normal sin darnos ninguna indicación de que ocurra nada anómalo, permaneciendo completamente invisible e indetectable en nuestro sistema. El BIOS no puede distinguir entre software malicioso y un cargador de arranque confiable, por lo tanto, permite a cualquiera de los dos arrancar.

Los PCs con Windows 8 vienen con el certificado de Microsoft almacenado en la UEFI y ésta comprobará el cargador de arranque antes de lanzarlo, asegurándose que está firmado por Microsoft. Si un *rootkit* o cualquier otro software malicioso reemplazase nuestro cargador de arranque, UEFI no lo va a dejar arrancar. Esto impide al software malicioso secuestrar nuestro proceso de arranque, ocultándose del sistema operativo.

Para obtener información técnica más precisa acerca de cómo funciona *Secure Boot* revisar la nota de Microsoft relativa al asunto en:

<http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx>

## Lo que podemos controlar

Si todo lo controlase *Secure Boot*, entonces no podríamos ejecutar ningún sistema operativo que no fuera de Microsoft en nuestro PC. Afortunadamente, podemos controlar el arranque seguro en UEFI (de forma parecida a lo que hacíamos con el antiguo BIOS de los PCs). Podemos desactivar el arranque seguro completamente o bien incluirle certificados adicionales. Podríamos incluso ser capaces de eliminar el certificado de Microsoft. Si quitamos el certificado de Microsoft y le añadimos uno nuestro, entonces nuestro computador sólo lanzará cargadores de arranque que hayamos formado nosotros mismos.

## Instalar Linux

No hay nada que impida que los computadores salgan con el certificado de Ubuntu. Las distribuciones de Linux pueden también publicar su propio certificado y pedirle a los usuarios que lo instalen, o bien pedirles que desactiven *Secure Boot* completamente. Por ejemplo, las distribuciones Linux *Fedora* se instalarán en cualquier PC certificado con Windows 8 sin necesidad de ninguna configuración adicional. Otras distribuciones de Linux pueden seguir el mismo camino.

Para obtener más información acerca de la situación de otras distribuciones Linux podemos revisar:

<http://mjg59.dreamwidth.org/12368.html>

## x86 vs. ARM

Ahora vienen las malas noticias: todo lo que hemos dicho anteriormente acerca de cómo podemos controlar *Secure Boot* e instalar nuestro propio sistema operativo solo es de aplicación a los PCs y Tablets con Windows (Intel) x86, que corran el sistema operativo Windows 8 estándar.

Habrá máquinas basadas en ARM que ejecuten Windows-RT (veremos portátiles con Windows basados en ARM, no sólo tablets). Además de no soportar aplicaciones de terceras partes en los computadores Windows de sobremesa tradicionales y limitarse a aplicaciones específicas, las máquinas Windows-RT basadas en ARM tendrán un cargador de arranque bloqueado. No podremos desbloquear el sistema *Secure Boot* para instalar nuestro propio sistema operativo. La directiva de Microsoft dice que cualquier dispositivo ARM con Windows RT no nos permitirá desactivar *Secure Boot.* Microsoft quiere que que pensemos en los sistemas Windows-RT basados en ARM como “dispositivos”, no como PCs completos, ya que como le dijo Microsoft a Mozilla: “Windows-RT ya no será considerado más otro Windows”.