Módulo de plataforma de confianza

Hace muchos años, décadas ya, utilizábamos algo muy sencillo para vincular una licencia uso de software a un hardware: leer el serial de volumen que se aplica de manera aleatoria al formatear un disco duro. Era algo casi que tonto pero la idea provino de la propia empresa Microsoft®, era un secreto a voces que aparte de este "truco" también usaba el serial de la tarjeta de red y la tarjeta madre.

Un ingeniero retirado que duró muchos años trabajando para esa empresa recién ahora abrió un canal en YouTube **donde relata y confirma muchas cosas que sospechábamos *pero no podíamos dar por ciertas debido al software privativo.*** Mucho hubo de ingeniería inversa (yo la verdad que trabajando como un burro para poder comer trigo no he tenido nunca tiempo para ello) pero eso tampoco podía comprobar al 100% e incluso hasta tal vez es ilegal. Vean y oigan en inglés, lo que revela Dave Plummer:

https://www.youtube.com/watch?v=FpKNFCFABp0

Retomando el tema, luego vinieron las llaves USB, suerte de dispositivo que también le hacíamos lo mismo: si esa memoria extraíble estaba conectado al equipo, la licencia de uso estaba activa y funcionaba el software. También pasó lo mismo, si bien recuerdo, con los discos ópticos. **Sí, el software privativo es así, nada podemos hacer para cambiarlo**, y para ser sinceros durante varios lustros nos permitió llevar comida a la casa de esa manera, garantizando el uso de un equipo por licencia de uso.

También existen unas memorias USB o *pendrives* con capacidades avanzadas para esto del reconocimiento unívoco de un dispositivo de hardware. De eso no tuvimos experiencia, tal vez algún día tengamos alguno a la mano para experimentar.

Windows 11

Ahora en el año 2021 se ha levantado un revuelo acerca de Windows 11 y el uso "obligatorio" de un artilugio electrónico "*con todas las de la ley*" para el uso práctico de llaves públicas y privadas. Hemos publicado un manual muy útil acerca de todo lo que hay que saber acerca de este software

de cifrado reversible o *criptográfico*.

El cacharro de marras es el **Módulo de plataforma de confianza** (*Trusted Platform Module* o simplemente **TPM**) el cual traemos hoy a colación, para no perder la costumbre de escribir en este vuestro y nuestro blog de software libre.

¿Qué diantres es un TPM?

En su forma más básica, el TPM es un diminuto chip en la tarjeta madre de una computadora, que a veces viene separado del CPU y la memoria RAM. El chip es similar al teclado que se utiliza para desactivar la alarma de seguridad de los comercios y tiendas cada vez que se abre, o a la aplicación de autentificación usada en un teléfono móvil para iniciar sesión en las cuentas bancarias. De esta manera, prender tu ordenador es análogo a abrir la puerta de tu negocio o introducir el nombre de usuario y contraseña en la página de inicio de sesión del banco. Si no se introduce un código en un breve periodo de tiempo, sonará la alarma o no se podrá acceder al dinero.

Del mismo modo, después de pulsar el botón de encendido en una computadora reciente (desde el año 2019) que utiliza cifrado de disco completo y un TPM, el pequeño chip proporcionará un código único llamado clave criptográfica. Si todo va bien, el cifrado de la unidad se desbloquea y el ordenador se pone en marcha. Si hay un problema con la clave -quizás un alguien robó el equipo e intentó manipular la unidad cifrada del interior- el ordenador no arrancará.

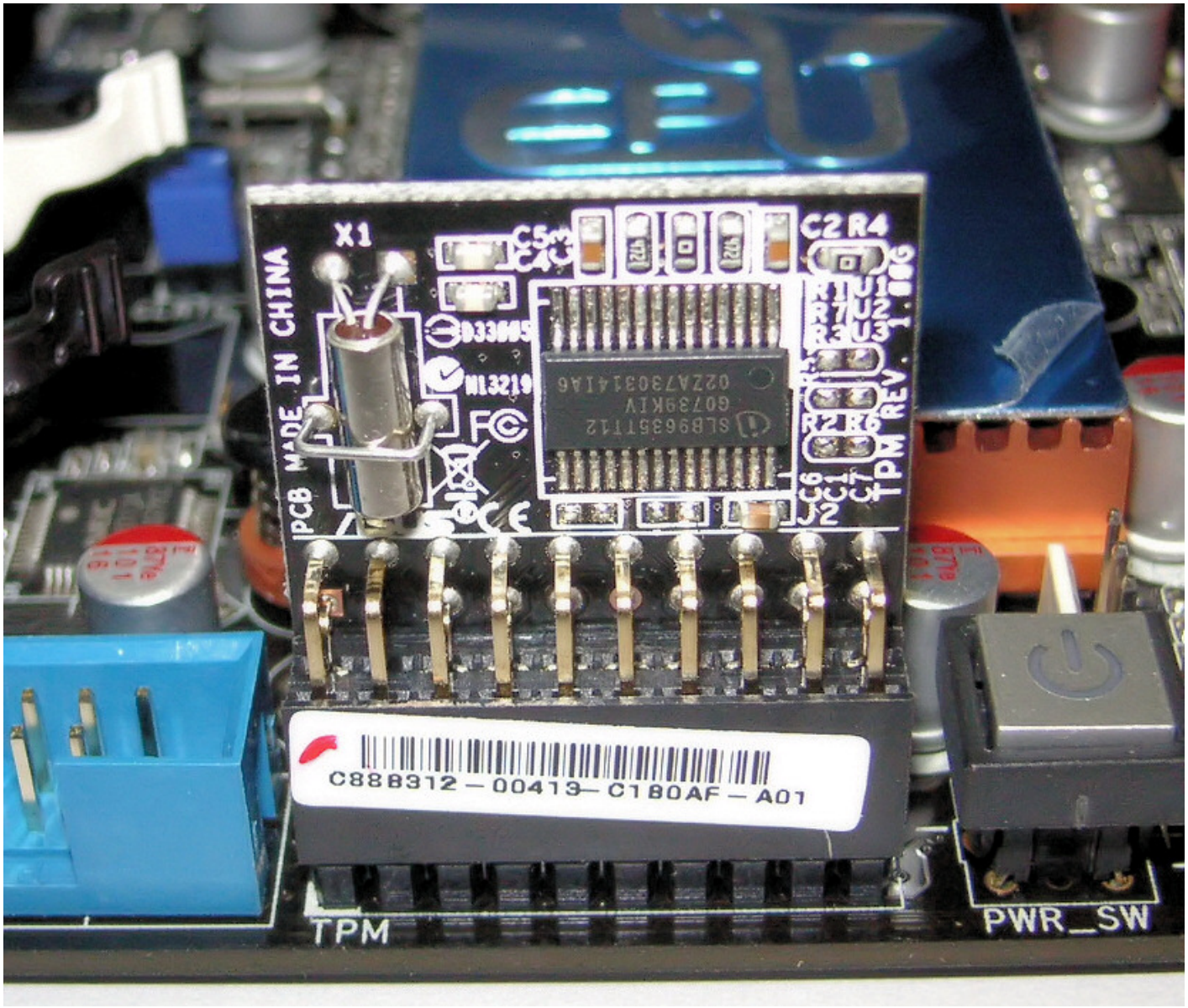
Aunque así es como funcionan las implementaciones modernas de TPM (versi) en un nivel más básico, no es ni mucho menos todo lo que pueden hacer. De hecho, muchas aplicaciones y otras funciones hacen uso del TPM después de que el sistema haya arrancado. Los clientes de correo electrónico Thunderbird y Outlook utilizan el TPM para gestionar los mensajes cifrados o con clave. Los navegadores web Firefox y Chrome también emplean el TPM para ciertas funciones avanzadas, como el mantenimiento de certificados SSL para sitios web. Además de las computadoras, muchos otros dispositivos de consumo utilizan TPM, desde impresoras hasta accesorios para el hogar.

Tipos de TPM

Al igual que los TPM pueden realizar muchas otras funciones además de su propósito básico de proporcionar protección de arranque para los ordenadores, también pueden adoptar muchas formas diferentes además de un chip independiente. El **Trusted Computing Group** (TCG) es responsable del mantenimiento de los estándares TPM y señala que hay dos tipos adicionales de TPM.

Los TPM pueden integrarse en la CPU principal, ya sea como un añadido físico o como un código que se ejecuta en un entorno dedicado, conocido como *firmware*. Este método es casi tan seguro como un chip TPM independiente, ya que utiliza un entorno de confianza discreto del resto de los programas que utilizan la CPU.

El tercer tipo de TPM es virtual. Se ejecuta completamente en software. El TCG **advierte que no se recomienda su uso en el mundo real**, ya que es vulnerable tanto a la manipulación como a los fallos de seguridad que pueda haber en el sistema operativo.



TMP instalado en una tarjeta madre marca Asus (By FxJ - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=7637561)

TPM y los sistemas operativos

Para el kernel Linux, TPM está disponible desde la versión 3.2 (año 2015). Podemos detectar si nuestro placa madre posee TPM si ejecutamos:

```
journalctl -k --grep=tpm
```

O directamente revisar si existen los siguientes valores:

```
/sys/class/tpm/tpm0/device/description
/sys/class/tpm/tpm0/tpm_version_major
```

Si queremos usar SSH para proteger nuestras conexiones, recuerden que con la tecnología actual añadirá 1 ó 2 segundos a ese proceso. La empresa **wolfSSL** (propiedad de Daniel Stenberg, creador de **curl**) ofrece en venta la tecnología wolfTPM, revisen enlace web en las sección de fuentes consultadas. Allí ponen ejemplos concretos con marcas de chips específicos que se deben compilar especialmente para cada uno de ellos a ser utilizado.

https://twitter.com/shen/status/1408284995131645956

Los TPM son alternativas eficientes a los antiguos métodos de seguridad de los ordenadores con Windows. De hecho, desde julio de 2016 Microsoft ha exigido la compatibilidad con TPM 2.0 en todos los ordenadores nuevos que ejecuten cualquier versión de Windows 10 para escritorio (Home, Pro, Enterprise o Education). Del mismo modo, Windows 11 solo se ejecutará en PCs que tengan capacidades TPM. Los dispositivos que tengan TPM 1.2 recibirán una notificación indicando *que no se aconseja la actualización.*

https://twitter.com/askubuntumemes/status/1410988507007533069

Generador de números aleatorios

Una tarea un tanto complicada sobre la cual hemos hablado antes, es poder obtener números aleatorios puros. Para poder usar esta características tenemos que ir un poco más allá con nuestro equipo con GNU/Linux Debian/Ubuntu:

```
sudo apt-get install tpm-tools trousers libtspi-dev libopencryptoki-dev libssl-dev python-pip python-dev build-essential
```

Recuerden habilitar un espacio virtual para Python y así impedir que otros proyectos de programación que tengamos resulten afectados. Luego sí podemos instalar una utilidad para Python llamada:

```
pip install pytpmutils
```

Ya teniendo todo esto a punto podemos generar un número aleatorio con:

```
tpm-rndgen --bs=128 --count=2 | hexdump
```

https://twitter.com/askubuntumemes/status/1309327453131862018

Métodos alternos al TPM

Actualizado el domingo 4 de julio de 2021.

Evidentemente que esto del TMP es insuperable: el fabricante del artilugio solo conoce la clave privada y "garantiza" que ese chip específico pertenece a esa clave privada.

Un proceso parecido es suponer que nosotros como usuario *root* damos derecho a un usuario(a) como administrador y luego ese administrador(a):

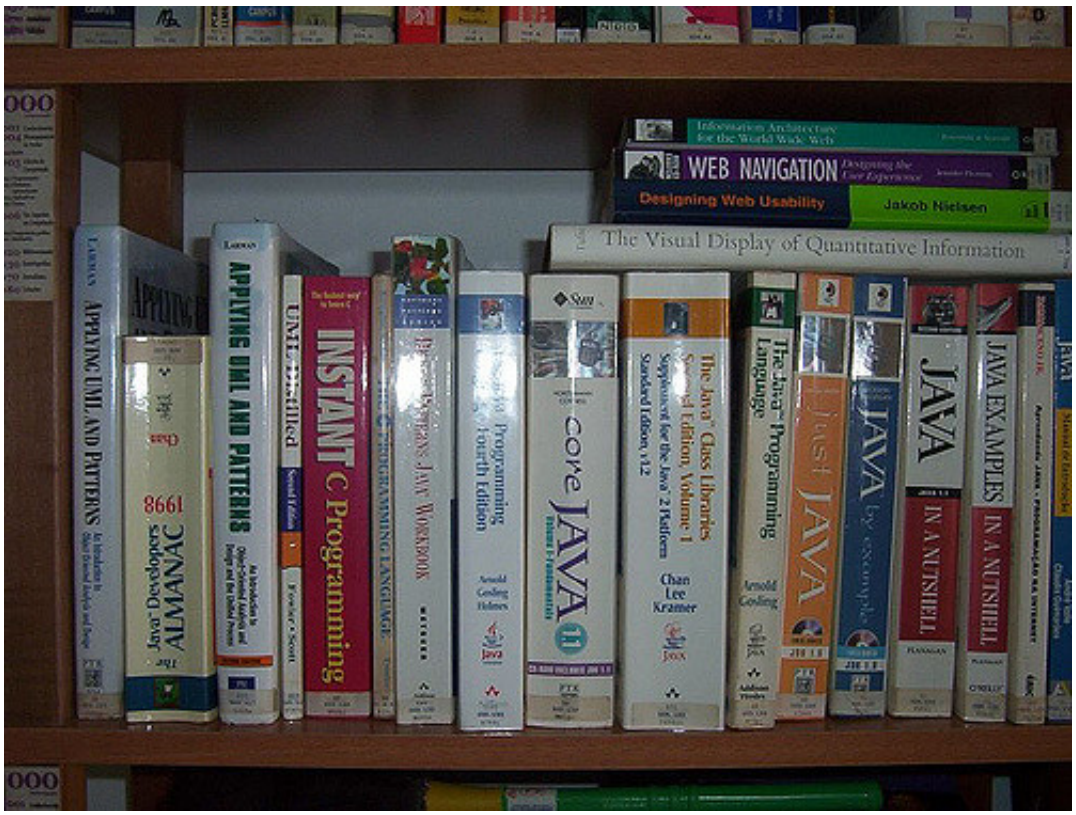
- Crea una partición cifrada.
- Genere y guarde sus pares de claves privadas y públicas.
- Además marca todos sus ficheros con claves para que solamente él o ella pueda leerlos y

escribirlos.
- Siempre podemos, como usuario raíz, acceder a todos esos recursos.

Así que de esta manera esos fabricantes que vendan esos chips se enfrentan a las siguientes dificultades:

- Que por error una clave privada la asignen a varios chip.
- Que dichas claves privadas, que imagino han de tener guardadas en una base de datos, sea filtrada al exterior.
- Que agencias de seguridad de cualquier gobierno del mundo presionen legalmente para que entreguen dichas claves privadas.

Por esto **pienso seriamente** que volvemos al esquema anterior de los *pendrive* criptográficos pero con mejoras en cuanto que podemos utilizar el generador de números aleatorios en nuestro beneficio y además la placa madre colabora con nosotros a fin de garantizar que solamente el chip que nos vendieron de fábrica, con la clave privada hecha por ese fabricante, sea el mismo chip donde nosotros guardamos nuestras claves privadas generadas (y guardadas en la memoria volátil del cacharro de marras).



Fuentes consultadas

En idioma castellano

- «Módulo de plataforma de confianza» Wikipedia.
- «».
- «».

En idioma italiano

- «Trusted Platform Module» Wikipedia (muy buen artículo).
- «».
- «».

En idioma inglés

- «Using a TPM» (Setting up SSH).
- «Trusted Platform Module» Wikipedia.
- «TPM 2.0 Support Sent In For The Linux 3.20 Kernel».
- «wolfTPM with even more TPM 2.0 examples».
- «Trusted Platform Module» Wiki Archlinux.
- «What Is a TPM, and Why Do I Need One for Windows 11?» (por Tom Brandt https://www.pcmag.com/news/what-is-a-tpm-and-why-do-i-need-one-for-windows-11).
- «pytpmutils 0.1.2».
- «http://trousers.sourceforge.net/faq.html#1.5».
- «Linux TPM2 & TSS2 Software».
- «».
- «».
- «».

https://twitter.com/qwakaw/status/1025467624434499584

Crédito de la imagen Gerd Altmann, trabajo, licencia de uso:Pixabay