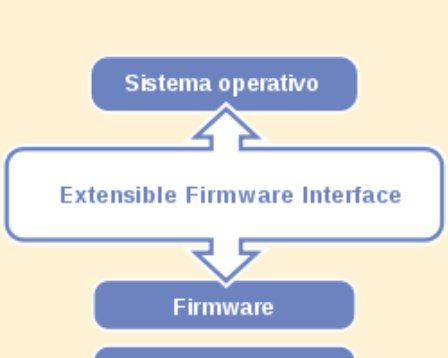
Trusted Platform Module

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

SISTEMAS OPERATIVOS

AGUILAR LUNA GABRIEL
GARCÍA RACILLA SANDRA

CONCEPTOS PREVIOS



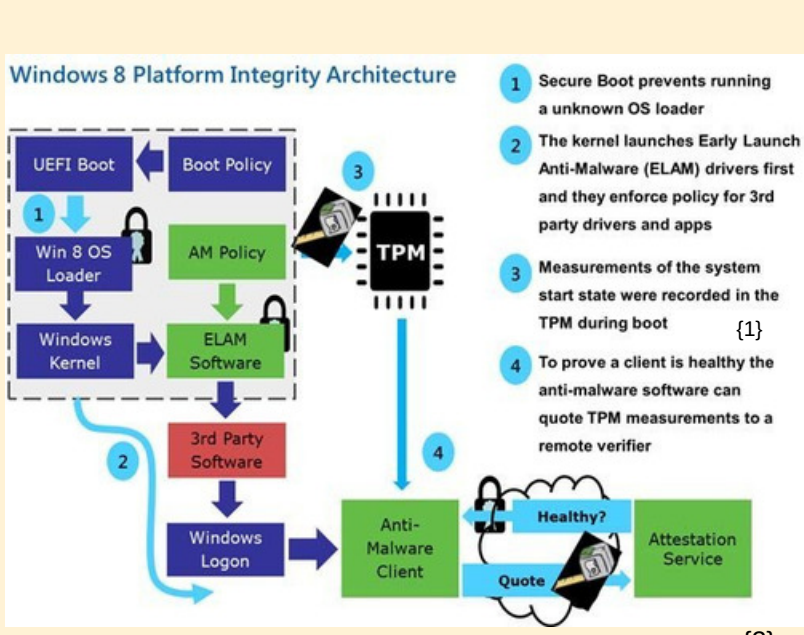
{1}

Firmware: Establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.
BIOS: Es un firmware cuyo propósito es activar una máquina desde su encendido y preparar el entorno para cargar un sistema operativo en la memoria.
UEFI: Una interfaz entre el sistema operativo y el firmware.
COREBOOT: Es un proyecto dirigido a reemplazar el firmware no libre de los BIOS propietarios por un BIOS libre y ligero diseñado para realizar solamente el mínimo de tareas necesarias para cargar y correr un sistema operativo.

Secure Boot

El secure boot es una característica de la UEFI, que sirve para resistir ataques e infecciones por malware.
Detecta la manipulación de cargadores de arranque, archivos clave del sistema operativo y ROM's y valida sus firmas digitales.

Se asegura que durante el proceso de arranque sólo se ejecutará software que cumpla con una de las firmas criptográficas preinstaladas.



{2}

Polemica

Microsoft pide a los fabricantes que los equipos soporten secure boot.
¿El fin de las máquinas de propósito general?
¿Y los sistemas operativos alternativos?

Desde que Microsoft empezó a pedir a los fabricantes que todas las computadoras deben ser capaces de arrancar con un Secure Boot han surgido rumores sobre un posible cambio en la industria que pondría fin a las computadoras de propósito general. Sin embargo ninguna de estas cuenta con fundamentos solidos.

Criptografia

La Criptografía es el arte o ciencia de escribir mensaje de forma cifrada o en código.
Esta práctica se ha realizado desde hace más de 4000 años pasando por los jeroglíficos del Antiguo Egipto, los espartanos, el cifrado César de la Antigua Roma, mensajes de la máquina Enigma en la Segunda Guerra Mundial; hasta la comunicación de nuestras computadoras con los servidores de Google al abrir nuestro correo.

Una comunicación está cifrada cuando solamente emisor y receptor son capaces de extraer la información del mensaje

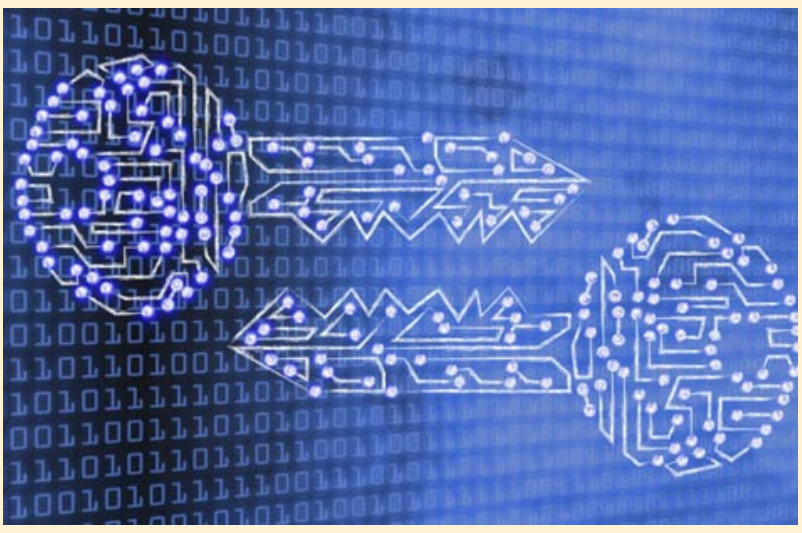
¿Qué es TPM?

Los TPM son dispositivos que se unen a las especificaciones del Módulo de Plataforma Confiable (TPM) del Grupo de "Trusted Computing". Por lo general son microcontroladores con una pequeña cantidad de memoria, que pueden ser agregados ya sea por el protocolo de comunicación i^2C para los dispositivos embebidos; o por medio del bus LPC (Low Pin Count) en las computadoras.

Guardando secretos con una TPM

Todos los TPM cuentan con algo llamado Storage Root Key (SRK), (Almacenamiento de la Llave Raíz); ésta es generada cuando el TPM es configurado inicialmente.
Puedes pedirle a la TPM que genere un nuevo par de llaves, lo hará, cifrará con otra llave y lo regresará a ti; pero realmente estas llaves no se guardan en el TPM; el SO lo almacena en el disco.

Lo anterior significa que a las llaves están ligadas a un sistema, lo que es bueno para la seguridad. De esta forma un atacante no puede obtener las llaves descifradas, ni aunque tuviera total acceso a tu sistema de archivos o un keylogger.



Esto funciona muy bien en un mismo sistema, pero las cosas cambian cuando queremos trabajar en múltiples sistemas usando las llaves proporcionadas por el TPM. Las llaves pueden ser marcadas como "migratable" , esto hace posible exportarlas de TPM e importarlas desde otro TPM.
Pero con esto volvemos prácticamente al problema inicial pues el atacante podría interceptar la llave o robarla en el momento en el que salga del sistema para migrar a otro. Es por eso que se implementa una serie de reglas para evitar que al migrar una llave, pierda sentido usar un TMP

Al usar llaves del TPM en múltiples sistemas:

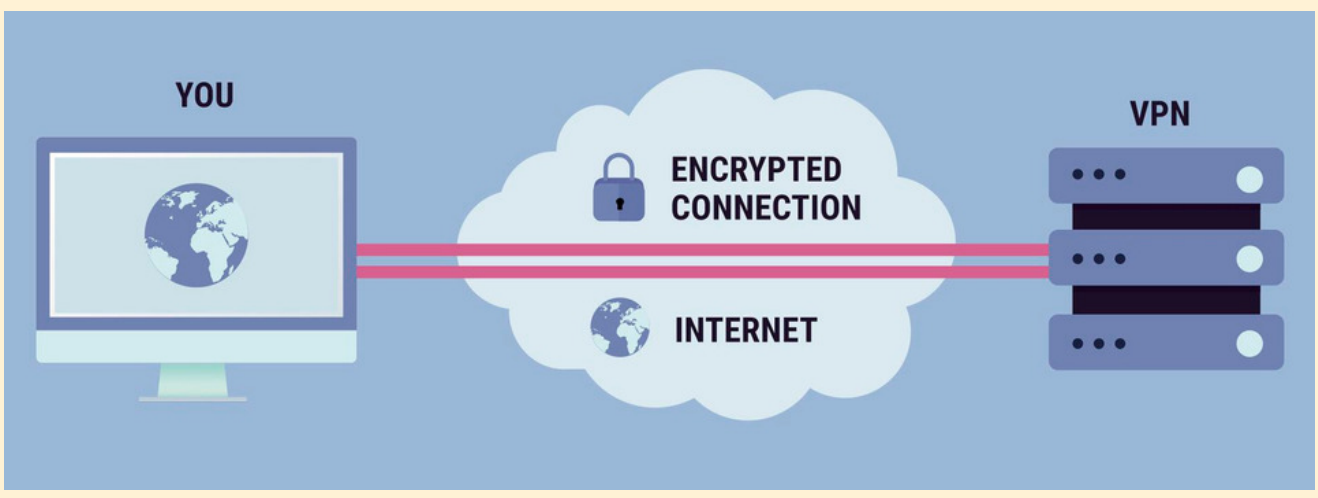
- Necesitas la contraseña del TPM del propietario; que se establece durante la configuración inicial del TPM.
- Es posible establecer límites en la migración cuando importas la llave inicialmente. En este escenario la TPM sólo estará dispuesto a exportar la llave cifrándola con una llave pública pre-configurada.

Usos Comunes

A través de TPM's, corporaciones pueden enlazar llaves VPN (Virtual Private Network) a máquinas corporativas, haciendo posible imponer diferentes políticas de seguridad. Lo que se busca lograr es crear un canal seguro de comunicación entre estas máquinas, pero todo a través del internet.

En el año 2006, Intel usa TPM como parte de su tecnología anti robo en dispositivos orientados a la educación como “Classmate”, esto surge a través del programa 'World Ahead', en el que se platea la creación de computadoras para niños en países en desarrollo; cabe aclarar que la empresa sólo se encargó de la creación de los chips usados en los dispositivos finales.

Y en la nube, proyectos como “Trusted Computing Pools” (Grupo de Computadoras de confianza), usan atestación (testificación) remota para verificar que las nodos de cómputo se encuentran en buen estado antes de programar trabajos en ellos.



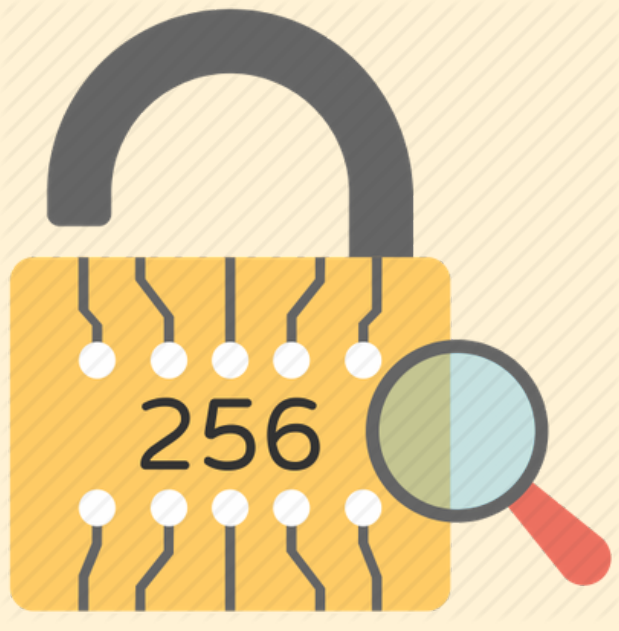
¿Por qué no reemplazar el Sistema Operativo con uno que obtenga la llave secreta?

Es preciso recordar que al usar TPM las llaves generadas estarán ligadas al sistema. Digamos que un sistema de archivos raíz (root filesystem) es codificado y almacenado en la TPM. Entonces, puedo reemplazar el kernel con uno que atrape/obtenga la llave una vez que sea liberado por la TPM. Esta afirmación es incorrecta, TPM cuenta con un conjunto de pruebas y confirmaciones para comprobar que lo anterior no haya pasado.

Las TPM’s cuentan con un montón de Platform Configuration Registers (PCRs) (Registros de configuración de Plataforma) son usados para guardar el estado del sistema.

Estos PCRs se borran en el ciclo de alimentación pero las aplicaciones pueden concatenar en tiempo de ejecución un Secure Hash Algorithm (SHA 1). Cada vez que se agrega un SHA 1 al valor del PCR se calcula otro SHA 1 y ese valor se almacena en el PCR.

El firmware realiza un hash de sí mismo y también del bootloader, metiendo esos valores a algún PCR.
Por otra parte, del bootloader se hace un hash de su configuración y de los archivos que estaba leyendo antes de su ejecución.
Esto genera una cadena de confianza, pues es posible verificar que el componente del sistema anterior no haya sido modificado.



Si un atacante modifica el bootloader, el firmware calculará un valor diferente de hash y a partir de estos valores la TPM puede decidir si descifrar o no la información. Lo mismo pasa si se se cambia el kernel.

No hay forma de que un atacante reemplace cualquier componente fundamental del sistema sin cambiar el valor de hash.

Se hará una comparación entre los valores de los PCRs y la TPM, si no coinciden simplemente la TPM se negará a dar la llave

Evitando Evil Maid attack con TMP

Este ataque se basa en que la mayoría de los mecanismos de seguridad usados en las laptops pueden ser derribados si un atacante es capaz de ganar acceso físico al sistema.
Algunas formas de proteger a una computadora de esto es usando TPM's.

Una forma de evitar un ataque Evil Maid es:

●Es necesario elegir una frase secreta, cifrarla con la TPM y guardarla en una memoria USB.
●Si los valores del PCR están bien, la frase será decifrada de forma correcta e impresa en la pantalla.
●El usuario comprueba que la frase sea correcta y reinicia el sistema. De esta forma comprueba que el sistema no haya sido manipulado.

Una desventaja es que esta verificación no se lleva a cabo en la mayoría de los boots, y tendrás que confiar en que el usuario tome decisiones razonables sobre si es necesario realizar esta verificación en un boot específico.

¡Dato curioso!

Según el artículo escrito por Alberto García para ADSLZone en el año 2016:

"[...] Todos los fabricantes que lancen hardware compatible con Windows 10, tendrán que tener un módulo de seguridad TPM 2.0, en el hardware de los dispositivos" [3]

Así que si eres usuario de Windows lo más probable es que estés haciendo uso de una TPM y aún no lo sabes.

Resumiendo

Usar TPM's otorga de seguridad robusta a un dispositivo utilizando claves de cifrado válidas y seguras, que se encuentran ligadas al sistema de tal forma que hace más difícil su obtención por terceros.
Utilizado por Aplicaciones de cifrado de disco completo, como BitLocker para Windows.
Nos permite registrar el estado de un sistema a través de los registros de configuración de plataforma (PCR) . Verificación de integridad del sistema previa al arranque.

Bibliografía

A short introduction to TPMs. Garrett Matthew MJG59 , Mayo 6, 2013.

Anti evil maid 2 Turbo Edition. Garrett Matthew MJG59 , Julio 6, 2015.

Avoiding TPM PCR fragility using Secure Boot . Garrett Matthew MJG59 , Julio 17, 2017.

Secure Boot. Crisol Leandro, Marzo 20, 2013.

Secure Boot ¿Quien controla tu ordenador?. Kirschner Matthias,
Junio 1, 2016

{1} ¿Qué es el firmeware?,
Ana Muñoz de Frutos, 29 agosto 2016.

{2} Secure Boot,
Crisol Leandro, Marzo 20, 2013.

{3} ¿Qué es TPM 2.0 y por qué será obligatorio para los PC con Windows 10?,
Alberto García, ADSLZone, 28 julio 2016.