TRUSTED PLATFORM MODULE

Relación con el sistema operativo

Materia: Sistemas Operativos

Profesor: Ing. Gunnar Eyal Wolf Iszaevich

Grupo: 06

Semestre: 2024-2

Integrantes del equipo:

Marco Alejandro Vigi Garduño

Francisco Daniel López Campillo

Fecha: 24/04/2024

Contenido

Introducción

El Trusted Platform Module (TPM) es considerado seguro por varias razones clave:

1. **Chip Dedicado:** El TPM es un chip dedicado y físicamente separado del resto del hardware de la computadora. Esta separación ayuda a proteger las claves y datos sensibles almacenados en el TPM de accesos no autorizados.
2. **Hardware Resistente:** Los chips TPM están diseñados para resistir una amplia gama de ataques físicos y de software, incluidos intentos de manipulación, extracción y ataques de fuerza bruta.
3. **Almacenamiento Seguro:** El TPM utiliza técnicas de almacenamiento seguro para proteger las claves criptográficas y otros datos sensibles almacenados en su memoria.
4. **Protección de Claves:** El TPM proporciona un entorno seguro para generar, almacenar y utilizar claves criptográficas.
5. **Funciones Criptográficas:** El TPM implementa algoritmos criptográficos robustos para realizar operaciones criptográficas de manera segura.
6. **Seguridad en el Arranque:** El TPM puede verificar la integridad del proceso de arranque del sistema operativo y proteger contra ataques de malware de arranque.
7. **Certificaciones de Seguridad:** Los chips TPM suelen estar certificados por estándares de seguridad reconocidos, como FIPS (Federal Information Processing Standards) en los Estados Unidos o Common Criteria a nivel internacional.

Historia y contexto

Origen y desarrollo del TPM

El TPM fue ideado por un consorcio de computadoras industriales llamado Trusted Computing Group (TCG). En 2011 se publicó la versión *TPM Main Specification Version 1.2*, que fue estandarizada en 2009 por la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés) como ISO/IEC 11889:2009. Finalmente, en 2014, TCG anunció una nueva versión llamada *TPM Library Specification 2.0*. Esta versión convirtió su estandarización en 11889:2015. La actualización del chip agregó las siguientes funcionalidades:

- Optimización de algoritmos como AES y RSA.

AES (Advanced Encryption Standard) – Algoritmo simétrico que es ampliamente utilizado para proteger datos confidenciales. En la versión 2.0 se pueden utilizar variantes de AES con longitudes de clave de 128, 192 y 256 bits.

RSA (Rivest, Shamir-Adleman) – Algoritmo asimétrico que se utiliza para la encriptación y la firma digital. En la versión 2.0 de TPM, se mejoró el soporte para operaciones, lo que permite una mayor flexibilidad y seguridad en la generación y el intercambio de claves criptográficas.

- Mayor integración con Sistemas Operativos.

El TPM puede integrarse con mecanismos de autenticación de usuario del sistema operativo, como contraseñas, pines o biometría para proporcionar una capa adicional de seguridad en el proceso de inicio de sesión.

Importancia del TPM en la seguridad de la computación moderna

El TPM no está directamente asociado con sistemas operativos específicos, sino que es una especificación de hardware que proporciona funciones de seguridad y protección de datos en una variedad de plataformas y dispositivos. A continuación, se presenta algunos beneficios que este chip puede aportar a Windows y Linux:

- Windows 11

Requiere TPM 2.0 para características de seguridad como Windows Hello, Bit Locker, Device Gaurd y Secure Boot. Estas características emplean el TPM para almacenar claves criptográficas y garantizar la integridad del sistema operativo durante el arranque.

- Linux

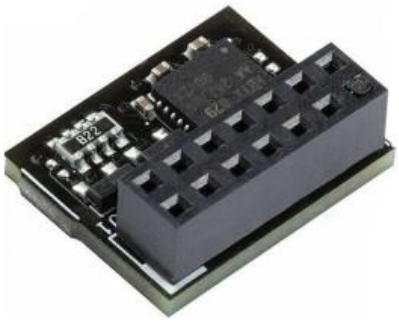
Varias distribuciones de Linux, como Ubuntu, Fedora y CentOS, admiten el uso de TPM para características de seguridad como la autenticación de arranque seguro (Secure Boot), el cifrado de disco y la protección de claves criptográficas. Se pueden utilizar herramientas como “tpm2-tools” para interactuar con el TPM 2.0 desde Linux.

Funcionamiento y componentes

Descripción de la estructura del TPM

Las especificaciones de un Trusted Platform Module (TPM) pueden variar dependiendo del fabricante y del modelo específico del chip. Sin embargo, aquí hay una lista de especificaciones comunes que suelen estar presentes en un TPM:

1. **Interfaz de Conexión:** Los TPM suelen utilizar una interfaz de conexión estándar, como LPC (Low Pin Count), SPI (Serial Peripheral Interface) o I2C (Inter-Integrated Circuit), para conectarse a la placa base de un dispositivo.
2. **Tamaño Físico:** Los TPM suelen ser pequeños y compactos, con dimensiones típicas de alrededor de 10 mm x 10 mm. Esto permite su integración en una variedad de dispositivos y plataformas informáticas.
3. **Memoria Interna:** El TPM contiene una pequeña cantidad de memoria no volátil (NVRAM) que se utiliza para almacenar datos sensibles de forma segura, como claves criptográficas y medidas de integridad del sistema.
4. **Algoritmos Criptográficos:** Los TPM suelen implementar una variedad de algoritmos criptográficos estándar, como AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) y SHA (Secure Hash Algorithm), para realizar operaciones criptográficas seguras.
5. **Certificaciones de Seguridad:** Los TPM suelen estar certificados por estándares de seguridad reconocidos, como FIPS (Federal Information Processing Standards) en los Estados Unidos o Common Criteria a nivel internacional, lo que garantiza que cumplen con requisitos de seguridad establecidos.
6. **Compatibilidad con Plataformas:** Los TPM están diseñados para ser compatibles con una amplia variedad de plataformas informáticas, incluidas computadoras de escritorio, laptops, servidores y dispositivos integrados.
7. **Consumo de Energía:** Los TPM suelen tener un bajo consumo de energía para minimizar su impacto en la duración de la batería en dispositivos móviles y portátiles.



TPM Asus 2.0 14 pines - $527 en Amazon México

Funciones criptográficas y de seguridad que proporciona el TPM

- Almacenamiento de claves criptográficas.

Función que permite al TPM generar y almacenar claves criptográficas de manera segura, protegiéndolas contra accesos no autorizados y asegurando su confidencialidad.

- Generación de claves.

Capacidad del TPM para crear claves criptográficas únicas y aleatorias que pueden utilizarse para cifrar, firmar o autenticar datos de manera segura.

- Autenticación del sistema.

Proceso mediante el cual el TPM verifica la integridad del firmware y del sistema operativo durante el arranque, asegurando que no se haya modificado de manera no autorizada.

- Anti - Hammering

El término *anti-hammering* se refiere a la protección implementada en los Módulos de Plataforma Confiable (TPM) para prevenir ataques de fuerza bruta o ataques de diccionario, que intentan determinar los valores de autorización para el uso de una clave criptográfica. Esta protección está diseñada para evitar que un atacante intente repetidamente valores de autorización incorrectos, lo que podría bloquear el TPM y dificultar el acceso legítimo.

El TPM procesa comandos en un entorno protegido, como un microcontrolador dedicado en un chip discreto o un modo especial protegido por hardware en la CPU principal. Cuando se proporciona el valor de autorización correcto, se utiliza para crear una clave criptográfica que no se revela fuera del TPM.

El TPM registra un número limitado de fallas de autorización antes de bloquear los intentos adicionales de uso de claves. Si se producen demasiadas fallas de autorización, el TPM entra en un estado de bloqueo global, evitando que cualquier entidad pueda utilizarlo hasta que se restablezca.

En el caso de TPM 2.0, la protección anti-hammering está bien definida. Después de 32 intentos fallidos de autorización, el TPM se bloquea y olvida una falla de autorización cada 10 minutos. Este período de bloqueo garantiza que los intentos repetidos no puedan acceder al TPM durante un tiempo prolongado. La protección anti-hammering se puede restablecer manualmente mediante el envío de un comando de reinicio de bloqueo al TPM (tpm.msc) y proporcionando la contraseña del propietario del TPM. Windows, por defecto, almacena automáticamente esta contraseña para su uso por parte de los administradores del sistema.

TPM 2.0 permite crear algunas claves sin un valor de autorización asociado a ellas. Estas claves pueden ser utilizadas cuando el TPM está bloqueado. Por ejemplo, BitLocker con una configuración predeterminada de *solo TPM* puede usar una clave en el TPM para iniciar Windows, incluso cuando el TPM está bloqueado.

Vulnerabilidades y consideraciones de seguridad

Exploración de posibles vulnerabilidades

En 2010, Chistopher Tarnovsky llevó a cabo un ataque hacia el TPM en una de las conferencias anuales de Black Hat, donde demostró ser capaz de extraer información de un TPM. Pudo lograrlo después de 6 meses de intentarlo, tras insertar una sonda y espiar un bus interno para el Infineon SLE 66 CL PC.

Infineon SLE 66 CL PC es un chip de seguridad utilizado comúnmente en dispositivos como tarjetas inteligentes, TPM, sistemas de pago o incluso chips periféricos utilizados en la consola XBOX 360. Las técnicas usadas por Tarnovsky se basaron en ingeniería inversa y manipulación física.

Sin embargo, esta vulnerabilidad demostrada no parece especialmente alarmante, ya que expone una de las principales y reconocidas debilidades:

Vulnerabilidad a ataques físicos

Curiosamente, durante la intensiva investigación de Christopher (quien fue parte del campo de la inteligencia, seguridad y criptografía en el ejército) a través de la exploración de un control de XBOX 360, descubrió que los TPM creados por Infineon estaban diseñados para autodestruirse en caso de ser infiltrados. De esta manera podríamos establecer que, si bien tienen esa debilidad demostrada, sólo una persona capacitada podría lograr vulnerar este sistema.

Otro evento que demostró esta vulnerabilidad, aunque no directamente, se desarrolló durante un ataque de Dolos (grupo dedicado a la seguridad informática) a través de la extracción de la clave que descifra al disco duro de una Lenovo.

Esta investigación lo logró a través de la intercepción de otro chip: CMOS SOP 8, que es mucho más vulnerable que el TPM. En la arquitectura de dicha Lenovo, notaron que ambos chips comparten el mismo bus SPI (Serial Peripheral Interface), por lo que pudieron interceptar la información a través de este canal. Citándolos:

"Vulnerar el TPM en la forma en la que lo hicimos es similar a ignorar al Fuerte Knox y enfocarse en el automóvil no tan blindado que sale de él."

Recomendaciones para mitigar riesgos

Existen diversas recomendaciones para evitar riesgos con el uso del TPM:

1. Actualización del firmware y software: Mantener el firmware del TPM actualizado es fundamental para garantizar que se parcheen las vulnerabilidades conocidas y se mejore la seguridad. Además, actualizar el software del sistema operativo y los controladores relacionados con el TPM puede mejorar su compatibilidad y estabilidad.

2. Configuración adecuada del TPM: Asegurarse de que el TPM esté configurado correctamente según las mejores prácticas de seguridad puede ayudar a protegerlo contra ataques y garantizar su funcionamiento óptimo. Esto incluye configurar contraseñas seguras y habilitar las funciones de seguridad pertinentes, como Secure Boot y BitLocker.

3. Monitoreo de la integridad del TPM: Implementar herramientas y procesos de monitoreo para detectar y responder a posibles compromisos de seguridad del TPM. Esto puede incluir la supervisión de registros de eventos y alertas de seguridad relacionadas con el TPM.

4. Respaldo y recuperación: Establecer procedimientos de respaldo regulares para los datos críticos almacenados en el TPM, como claves criptográficas, y tener planes de recuperación en caso de pérdida o corrupción de estos datos.

5. Evaluación periódica de la seguridad: Realizar evaluaciones regulares de la seguridad del TPM y su interacción con el sistema operativo para identificar y abordar posibles vulnerabilidades y riesgos de seguridad.

Conclusión

Recapitulación de puntos clave

Después de profundizar en el Trusted Platform Module (TPM) y su impacto en la seguridad informática, podemos ver que nos ofrece una defensa bastante robusta contra accesos no autorizados y ataques cibernéticos, respaldado por funciones criptográficas. Destacamos algunos de los puntos más importantes:

- El Trusted Platform Module (TPM) es un chip dedicado y físicamente separado del resto del hardware de la computadora, diseñado para proteger claves y datos sensibles contra accesos no autorizados.

- El TPM implementa funciones criptográficas robustas y estándares de seguridad reconocidos, como AES y RSA, para realizar operaciones criptográficas de manera segura.

- La protección anti-hammering en el TPM evita ataques de fuerza bruta y de diccionario al bloquear el acceso después de un número limitado de intentos fallidos de autorización.

- Las recomendaciones para mejorar la seguridad del TPM incluyendo mantener actualizado el firmware y el software, configurar correctamente el TPM, monitorear su integridad, realizar respaldos regulares y evaluaciones periódicas de seguridad.

- El TPM desempeña un papel fundamental en la seguridad de la computación moderna al proporcionar funciones de seguridad a nivel de hardware para una variedad de plataformas y dispositivos, incluidos Windows y Linux.

Reflexión sobre la importancia de la relación entre el TPM y el sistema operativo en la seguridad informática

La relación entre el TPM y el sistema operativo es un claro ejemplo de cómo la seguridad informática se construye sobre una colaboración bastante estrecha entre el hardware y software. El TPM, al ofrecer una capa de seguridad a nivel de hardware, establece los cimientos para proteger las claves criptográficas y verificar la integridad del sistema desde el inicio. Por otro lado, la forma en la que se conecta con el software es con el sistema operativo, al integrar y aprovechar las funcionalidades proporcionadas por el TPM, elevando esta seguridad al nivel de las aplicaciones y los procesos cotidianos del usuario por lo que esta unión entre ambos fortalece la seguridad informática y nos proporciona como usuarios una defensa sólida contra las amenazas cibernéticas en el mundo actual.

Posibles desarrollos futuros en el campo de la seguridad del TPM y su integración con el sistema operativo

Si lo pensamos bien para el futuro de la seguridad del TPM podemos llegar a imaginarlo incorporado en varias áreas de desarrollo prometedoras. Por ejemplo, una de ellas podría ser para abordar desafíos emergentes en seguridad, como la protección de datos en entornos de cómputo en la nube o el Internet de las cosas (IoT). También podríamos verlo en quizás avances en la interoperabilidad entre el TPM y diferentes sistemas operativos, permitiendo una adopción más amplia y una integración más fluida en muchos dispositivos y plataformas. De igual forma se debe llevar a cabo futuras mejoras en la usabilidad y la accesibilidad del TPM, para que facilite su implementación y gestión para los usuarios finales. Por ello podemos decir que promete seguir evolucionando para adaptarse a las demandas cambiantes del panorama tecnológico teniendo en consideración el crecimiento que han tenido las tecnologías de la información, o bien (TIC), que propician muchas vulnerabilidades en donde la ciberseguridad se antepone y proporciona una protección cada vez más robusta contra las amenazas cibernéticas.

Fuentes bibliográficas

- https://www.dell.com/support/kbdoc/en-us/000189676/windows-10-how-to-enable-the-tpm-trusted-platform-module
- https://learn.microsoft.com/es-es/windows/security/hardware-security/tpm/trusted-platform-module-overview
- https://support.lenovo.com/mx/es/solutions/nvid500331-what-is-tpm-20
- https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/trusted-platform-module.html
- https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/tpm-fundamentals
- https://arstechnica.com/gadgets/2021/08/how-to-go-from-stolen-pc-to-network-intrusion-in-30-minutes/
- https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/
- https://learn.microsoft.com/es-es/windows/security/hardware-security/tpm/tpm-recommendations
- https://www.intel.la/content/www/xl/es/business/enterprise-computers/resources/trusted-platform-module.html
- https://web.archive.org/web/20100212050338/https://hackaday.com/2010/02/09/tpm-crytography-cracked/