Informe técnico

HP Sure Start con detección de intrusiones en tiempo de ejecución

Según la implementación en los producto HP Elite con procesadores AMD de 7ª generación
Octubre de 2017

Table of contents

1 HP Sure Start con detección de intrusiones en tiempo de ejecución

1.1 Contexto

HP tiene una visión holística de la seguridad del cliente que busca responder a las necesidades de protección en cada nivel de la pila de computación de los dispositivos clientes. Nuestro foco no está solo en el SO o en las soluciones de seguridad basadas en la nube: creemos que la seguridad del firmware y el hardware de los dispositivos por debajo del SO también es crucial.

A medida que nuestro mundo se vuelve más conectado, los ciberataques están afectando el firmware y el hardware de los dispositivos cada vez con más frecuencia y sofisticación. Como el firmware del dispositivo ejecuta primero en el hardware y es responsable por el inicio seguro del sistema operativo, usted no puede confiar en el SO del dispositivo cliente si no confía en el firmware.

Es extremamente difícil, si no imposible, prever y prevenir todos los posibles ataques, y es por eso que HP también diseña sus dispositivos cliente con resiliencia cibernética, es decir, la capacidad de detectar un ataque exitoso y recuperarse.

HP Sure Start es un enfoque exclusivo y revolucionario de HP para proporcionar a los dispositivos cliente protección debajo del nivel del sistema operativo (SO), que asegura mediante recursos de hardware que el sistema solo arranque con un HP BIOS original. Además, si HP Sure Start detecta que el HP BIOS fue alterado de alguna manera, tiene la capacidad de recuperar el HP BIOS original usando una copia de seguridad protegida.

1.2 Visión general de HP Sure Start con detección de intrusiones en tiempo de ejecución

HP Sure Start con detección de intrusiones en tiempo de ejecución incluye las mismas capacidades que las generaciones previas de HP Sure Start, además de nuevos recursos que mejoran la protección avanzada de HP Sure Start, la detección de ataques y la recuperación del firmware de sistema de HP.[1] Hay dos recursos primarios que se agregan al dispositivo cliente:

- Detección de intrusiones en tiempo de ejecución
- Protección de configuración del BIOS

Además, HP comenzará a ofrecer el Manageability Integration Kit (MIK), que incluye el plugin Microsoft System Center Configuration Manager (SCCM), que proporcionará a los administradores de TI un mecanismo directo para administrar las capacidades existentes y nuevas de HP Sure Start usando su infraestructura de SCCM existente. Este informe técnico se enfocará en las dos nuevas capacidades para dispositivos cliente en lugar de en las capacidades de administración remota llave en mano posibilitadas por el MIK.

1.3 Detección de intrusiones en tiempo de ejecución (RTID)

1.3.1 Contexto

Para proporcionar contexto sobre cómo HP Sure Start con detección de intrusiones en tiempo de ejecución difiere de las capacidades de referencia proporcionadas por HP Sure Start antes de RTID, es útil revisar dichas capacidades, que se muestran en la **Figura 1.** Esta figura ofrece una visión general de lo que proporcionan las capacidades de referencia de HP Sure Start. Observe que estas capacidades están centradas en asegurar que (en el arranque) la CPU host nunca se inicie ejecutando código de firmware que haya sido sustituido o modificado. Por lo tanto, HP Sure Start garantiza que el sistema solo arrancará con firmware original HP que configurará el hardware del dispositivo cliente de manera segura, algo necesario para el arranque seguro del SO.

Observe que el enfoque no está puesto en el monitoreo del código del BIOS en el flash del sistema ejecutado por la CPU host en el arranque. Esta es una distinción importante con respecto al código del BIOS que reside en la memoria principal (DRAM) para proporcionar gestión de energía y otros servicios críticos después de que el sistema inicia el SO. A continuación, exploraremos es distinción de manera más detallada.

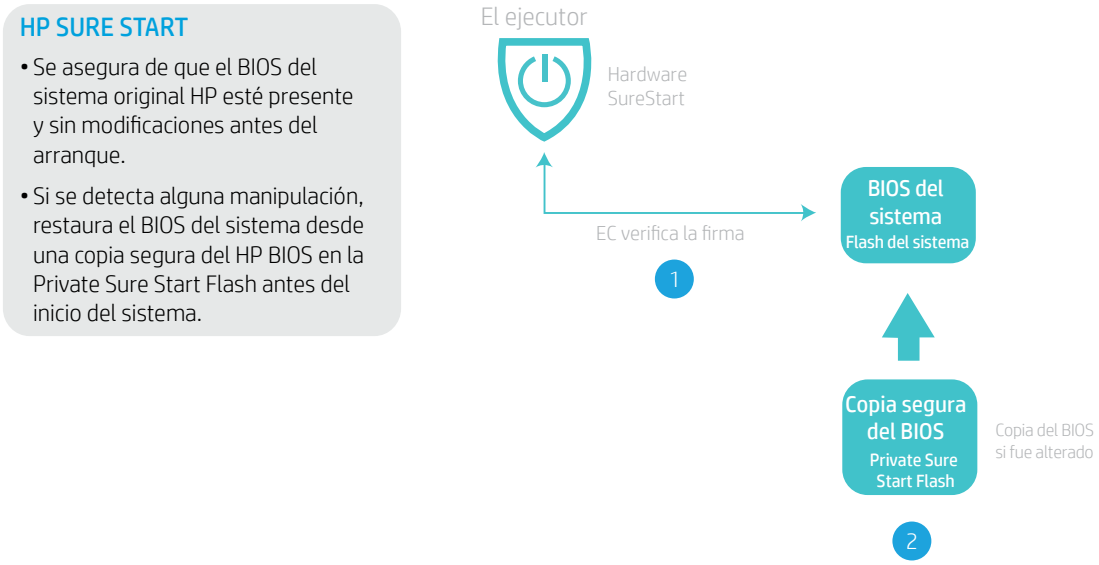

Figura 1. Visión general de las capacidades de referencia de HP Sure Start (se aplica a los productos HP Elite equipados con la 6ª generación de procesadores AMD y posteriores).

1.3.2 Código de BIOS en tiempo de ejecución en comparación con código de BIOS de arranque

En cada arranque, la CPU comienza la ejecución del código de BIOS desde la memoria flash en una dirección fija. Entonces, ese código de BIOS inicializa el hardware incluyendo la memoria DRAM y copia todas las rutinas desde la memoria flash a la memoria volátil (DRAM). Una gran parte de ese código de BIOS se usa para proporcionar capacidades previas a la carga del SO que son necesarias antes del inicio del sistema operativo. Algunos ejemplos de esas capacidades previas a la carga del SO incluyen los controladores de video, soporte para arranque PXE, los controladores del teclado y el mouse, autenticación de preinicio y desbloqueo de cifrado de almacenamiento masivo, por solo nombrar algunas. La mayoría de estas rutinas ya no son necesarias una vez que el SO está en ejecución, ya que las capacidades o solo son relevantes antes de que el SO asuma el dispositivo o porque el SO tiene sus propios controladores.

Sin embargo, hay una parte del BIOS que permanece en la DRAM que es necesario para proporcionar recursos de administración de la energía avanzados, servicios del SO y otras funciones independientes del SO mientras el SO está en ejecución. El código de BIOS, mencionado como código System Management Mode (SMM), reside en un área especial dentro de la DRAM que está oculta del SO.[2] También llamamos a este código "tiempo de ejecución" del BIOS en el contexto de HP Sure Start con detección de intrusiones.

La integridad del código SMM es crítica para la postura de seguridad del dispositivo cliente. La implementación inicial de HP Sure Start asegura que todo el código sea HP BIOS original cada vez que el sistema se inicia, incluso el código SMM que está presente en la DRAM cuando el SO se inicia.

La oportunidad es ir más allá, no solo asegurando que el código de HP SMM BIOS sea bueno al inicio del SO, sino proporcionando mecanismos para asegurar que continúe siendo bueno durante toda la ejecución del SO, suministrando medios de detectar cualquier ataque que logre superar los mecanismos existentes para proporcionar protección al código de HP SMM BIOS.

1.3.3 Arquitectura de la detección de intrusiones en tiempo de ejecución

La **Figura 2** muestra detalles de la implementación de la capacidad de detección de intrusiones en tiempo de ejecución (RTID). El recurso RTID utiliza hardware especial en el chipset de la plataformas para detectar modificaciones en el HP SMM BIOS durante el tiempo de ejecución. La detección de cualquiera de esas condiciones genera una notificación al hardware de HP Sure Start, que puede adoptar la acción de la política configurada independientemente de la CPU.

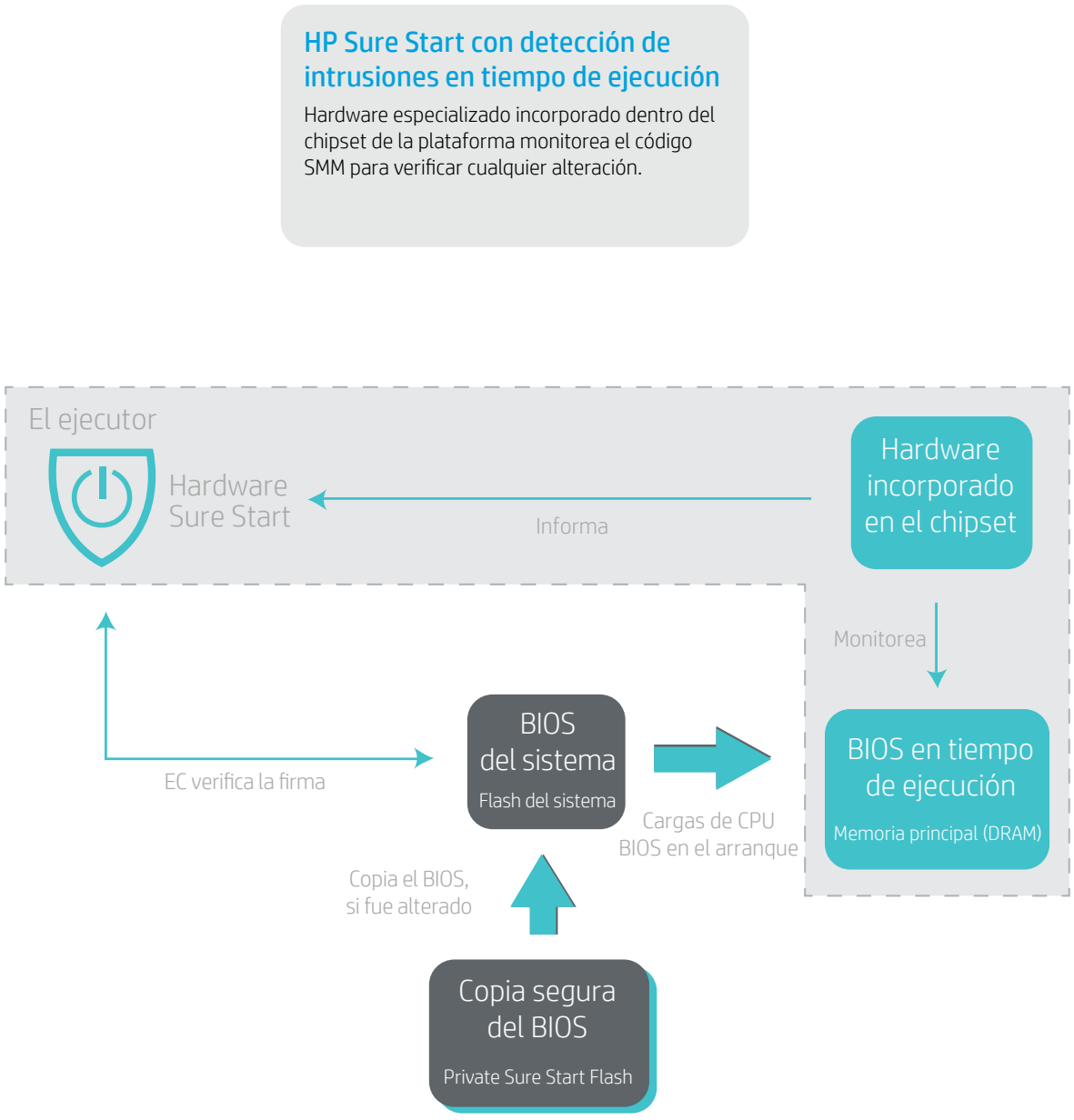

Figura 2. Arquitectura de detección de intrusiones en tiempo de ejecución (se aplica a los productos HP Elite equipados con la 7ª generación de procesadores AMD).

1.3.4 Eventos

El recurso HP Sure Start RTID generará eventos para el hardware de HP Sure Start cuando se detecte cualquier modificación en el código HP SMM BIOS. El hardware de HP Sure Start adoptará las acciones asociadas con la política de evento establecida en la configuración del BIOS.

Independientemente de la política de evento establecida, el evento siempre será registrado en el registro de auditoría de HP Sure Start y el usuario local recibirá una notificación del BIOS en el próximo arranque a continuación de un evento de RTID.

1.3.5 Política de controles

El recurso RTID viene activado de manera predeterminada para todas las plataformas enviadas desde las fábricas de HP. ¡El cliente final o el administrador no necesita activar o de alguna otra manera "implementar" el recurso para aprovechar las ventajas de HP Sure Start RTID!

Hay dos políticas de BIOS relacionadas con el recurso RTID que pueden ser configuradas por el propietario o administrador de la plataforma:

- **Detección de intrusiones de firmware en tiempo de ejecución HP** (activar/desactivar)
- **Política de evento de seguridad de Sure Start**

1.3.5.1. Detección de intrusiones de firmware en tiempo de ejecución HP

Esta configuración de política de BIOS activará o desactivará la capacidad de RTID. La configuración predeterminada de esta política es **activada**.

1.3.5.2. Política de evento de seguridad de Sure Start

Esta configuración de política de evento controla qué acciones se adoptan cuando el recurso RTID detecta un ataque o un intento de ataque. Hay tres posibilidades de configuración para esta política:

- Solo registrar el evento: Cuando se selecciona esta configuración, el hardware de HP Sure Start registrará los eventos de detección, que podrán verse en el camino "Registros de aplicaciones y servicios/HP Sure Start" de Microsoft Windows Event Viewer.[3]
- Registrar el evento y avisar al usuario: Esta es la configuración predeterminada. Cuando esta configuración esta seleccionada, el hardware de HP Sure Start registrará los eventos de detección, que podrán verse en el camino "Registros de aplicaciones y servicios/HP Sure Start" de Microsoft Windows Event Viewer. Además, se le comunicará al usuario dentro de Windows que se produjo el evento.[4]
- Registrar el evento y apagar el sistema: Cuando esta configuración esta seleccionada, el hardware de HP Sure Start registrará los eventos de detección, que podrán verse en el camino "Registros de aplicaciones y servicios/HP Sure Start" de Microsoft Windows Event Viewer. Además, se le comunicará al usuario dentro de Windows que se produjo el evento y que el apagado del sistema es inminente.

1.4 Protección de la configuración del BIOS

1.4.1 Contexto

La capacidad de referencia de HP Sure Start verifica la integridad y la autenticidad del código de HP BIOS. Como este código es estático después de que fue creado por HP, es posible usar firmas digitales para confirmar ambos atributos del código. La naturaleza dinámica y configurable por el usuario de la configuración del BIOS crea desafíos de protección adicionales, ya que HP no puede generar las firmas digitales y estas no pueden ser usadas por el hardware de HP Sure Start para verificar las configuraciones.

1.4.2 Visión general de la protección de la configuración del BIOS

La protección de la configuración del BIOS de HP Sure Start ofrece la capacidad de configurar el sistema, como la manera en que el hardware de HP Sure Start se usa para realizar copias de seguridad y verificar la integridad de todas las configuraciones del BIOS preferidas por el usuario.

Cuando este recurso está activado en la plataforma, se realiza una copia de seguridad de todas las configuraciones de política usadas por el BIOS y se verifica su integridad en cada arranque, para asegurarse de que ninguna configuración de política del BIOS haya sido modificada. En caso de que se detecte un cambio, el sistema usa la copia de seguridad del área protegida de HP Sure Start para revertir automáticamente a las configuraciones definidas por el usuario.

1.4.3 Eventos

El recurso de protección de la configuración del BIOS de HP Sure Start generará eventos para el hardware de HP Sure Start cuando se detecte cualquier intento de modificar las configuraciones del BIOS. El evento se registrará en el registro de auditoría de HP Sure Start y el usuario local recibirá una notificación del BIOS durante el arranque.

1.4.4 Política de controles

La política de protección de las configuraciones del BIOS está **desactivada** de manera predeterminada.

Para activar este recurso, el propietario/administrador del dispositivo cliente primero debe configurar todas las políticas del BIOS de acuerdo con su preferencia. El propietario/administrador también debe configurar una contraseña de administrador de configuración del BIOS para usar la protección de configuración del BIOS de HP Sure Start.

Una vez realizado esto, la política de protección de configuración del BIOS debe cambiarse a "activada". En este punto, se creará una copia de seguridad de todas las configuraciones del BIOS en el almacenamiento protegido de HP Sure Start. A partir de ese momento, ninguna de las configuraciones del BIOS podrá modificarse de manera local ni remota. En cada arranque, se verificará que las configuraciones de política del BIOS estén en el estado deseado y si se detecta alguna discrepancia, las configuraciones del BIOS se restaurarán desde el almacenamiento protegido de HP Sure Start.

Para modificar una configuración del BIOS, se debe proporcionar la contraseña del administrador del BIOS y con eso se desactivará la protección de la configuración del BIOS. Entonces, se podrán realizar las modificaciones deseadas.

2 Apéndice A

2.1 Visión general del System Management Mode

El System Management Mode (SMM) es un enfoque estándar del sector utilizado para los recursos avanzados de administración de la energía de las PC y otras funciones independientes del SO mientras el SO está en ejecución. Mientras las condiciones y la implementación del SMM son específicas de las arquitecturas x86, muchas arquitecturas de computación modernas usan un concepto arquitectónico similar.

El SMM es configurado por el BIOS en el momento del arranque. El código de SMM se completa en la memoria principal (DRAM) y entonces el BIOS usa registros de configuración especiales (bloqueables) dentro del chipset para bloquear el acceso a esta área cuando el microprocesador no está ejecutando en un contexto de SMM. Durante el tiempo de ejecución, el modo SMM es conducido por eventos. El chipset está programado para reconocer diversos tipos de eventos y plazos. Cuando se producen dichos eventos, el hardware del chipset impone el pin de entrada de System Management Interrupt (SMI). En el siguiente límite de instrucción, el microprocesador guarda su estado completo e ingresa en el SMM.

Cuando el microprocesador entra en el SMM, impone un pin de salida de hardware, SMI Active (SMIACT). Este pin sirve para avisar al hardware del chipset que el microprocesador está entrando en el SMM. Un SMI puede imponerse en cualquier momento, durante cualquier modo de operación de proceso, excepto desde dentro del propio modo SMM. El hardware del chipset reconoce la señal SMIACT y redirige todos los ciclos de memoria subsiguientes a un área protegida de la memoria (a veces denominada área SMRAM), reservada específicamente para el SMM. Inmediatamente después de recibir la entrada de SMI e imponer la salida SMIACT, el microprocesador comienza a guardar todo su estado interno en esta área de memoria protegida.

Una vez que el estado del microprocesador se almacenó en la memoria SMRAM, el código del controlador SMM, que también reside en SMRAM (colocado allí por el BIOS del sistema en el momento del arranque), comienza a ejecutar en un modo de operación SMM especial. Mientras está en ese modo, la mayoría de los mecanismos de aislamiento de hardware y memoria se suspenden y el microprocesador puede acceder prácticamente a todos los recursos de la plataforma para realizar las tareas requeridas. El código SMM completa la tarea requerida y a continuación es momento de hacer que el microprocesador vuelva al modo operativo previo. En ese punto, el código SMM ejecuta la instrucción Return from System Management Mode (RSM) para salir del SMM. La instrucción RSM hace que el microprocesador se restaure a sus datos de estado interno anteriores desde la copia guardada en SMRAM en el momento de la entrada en SMM. Al completarse la RSM, todo el estado del microprocesador se restaura al estado exactamente anterior al evento SMI y el programa anterior (SO, aplicaciones, hipervisor, etc.) reinicia la ejecución exactamente donde se había detenido.

[1] HP Sure Start con detección de intrusiones en tiempo de ejecución está disponible en los productos HP Elite equipados con procesadores AMD de 7ª generación.
[2] Para conocer más detalles sobre SMM y cómo funciona, consulte el Apéndice A.
[3] El software HP Notification debe estar instalado para ver los eventos de HP Sure Start en Windows Event Viewer.
[4] El software HP Notification debe estar instalado para recibir notificaciones.

Suscríbase para recibir actualizaciones
hp.com/go/getupdated

Compartir con colegas

© Copyright 2017 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin previo aviso. AMD es una marca comercial de Advanced Micro Devices, Inc. Microsoft y Windows son marcas comerciales o marcas comerciales o marcas registradas de Microsoft Corporation en EE. UU. y otros países.

4AA6-9340SPL, octubre de 2017