(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 664 413**

(51) Int. CI.:

G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.04.2007 PCT/US2007/009713**

(87) Fecha y número de publicación internacional: **01.11.2007 WO07124091**

(96) Fecha de presentación y número de la solicitud europea: **23.04.2007 E 07755830 (2)**

(97) Fecha y número de publicación de la concesión europea: **10.01.2018 EP 2013808**

(54) Título: **Aparato y métodos para realizar informes de mediciones de integridad informática de confianza**

(30) Prioridad:

21.04.2006 US 794165 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.04.2018

(73) Titular/es:

INTERDIGITAL TECHNOLOGY CORPORATION (100.0%)
200 Bellevue Parkway, Suite 300
Wilmington, DE 19809, US

(72) Inventor/es:

MOVVA, SASIDHAR;
HERSCHAFT, RICHARD, D.;
RACHA, RENUKA y
CHA, INHYOK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Aparato y métodos para realizar informes de mediciones de integridad informática de confianza

Campo de la invención

La presente invención se relaciona con la informática de confianza, (esto es, seguridad informática), a través de múltiples plataformas, (esto es, subsistemas). Más particularmente, la presente invención se relaciona con un aparato y métodos para realizar informes de mediciones de integridad informática de confianza.

Antecedentes

Los Registros de Configuración de Plataformas (PCR) son ubicaciones de memoria dentro de un módulo de plataforma de confianza (TPM) que se usan para almacenar resúmenes de datos. La memoria del TPM usada para los PCR puede ser de naturaleza volátil o no volátil.

Las especificaciones del Grupo Informático de Confianza Convencional (TCG) permiten las operaciones de Lectura, Extensión y Citar en los PCR, que son realizadas por el TPM. La operación de Lectura se usa para leer el valor de un PCR dado. La operación de Extensión se usas para modificar el valor de los PCR mediante la extensión de los viejos contenidos con los nuevos contenidos. Esto permite a un retador ver cómo los resúmenes de PCR finales fueron construidos. La operación de Citar se usa para informes de integridad donde los valores de los PCR están encriptados mediante el uso de una clave de identificación de atestación (AIK) por el TPM. La atestación en este contexto se refiere a una actividad de la plataforma para suministrar una medida de la confiabilidad del sistema a retadores internos o externos o solicitantes de tal información. Los informes de integridad se pueden usar para determinar la configuración actual de una plataforma.

Cuando el TPM realiza operaciones para generar métricas de integridad, para ser usadas más tarde para verificación de la integridad de una pieza de código o datos que está resumida, el TPM no computa simplemente el resumen del valor más reciente de los datos o código objetivo y entonces introduce ese valor en un PCR. En su lugar, el TPM realiza una operación de Extensión mediante la concatenación del valor existente actual del PCR con un nuevo valor de un componente del sistema a ser medido, y la realización de un algoritmo de resumen seguro (SHA) en los datos concatenados, e introduce el resultado en el PCR objetivo.

Cada vez que un PCR es extendido, una entrada de registro también se hace en el registro de eventos del TCG. Un registro de eventos del TCG, también llamado un registro de medición almacenado (SML), es un registro de eventos que tienen lugar en la plataforma en la cual reside el TPM. Un SML es un registro de valores medidos de un componente, (por ejemplo, una pieza de código), en una plataforma de sistema que incluye un TPM. El TPM realiza una medición de eventos, (tal como la carga de un software (SW) de aplicación particular), que tiene lugar en la plataforma en la cual reside el TPM. El núcleo de medición, que es una parte de confianza del sistema operativo (OS) de la plataforma que controla el TPM, genera eventos de mediciones tras la solicitud del OS. Observe que un “evento de medición” no es el evento que tiene lugar en la plataforma en sí, sino un término que significa la actividad o evento de la “medición” realizada por un evento que ocurre en la plataforma. Un ejemplo de tal evento de plataforma sería la lectura, en la memoria del sistema, de una pieza de código software. Un evento de medición consiste en dos clases de datos: 1) valores medidos – una representación de datos incorporados o código de programa; y 2) resúmenes de mediciones – un resumen SHA de esos valores. Los datos son escaneados por el TPM que genera un resumen de mensaje. Los resúmenes son capturas del estado de operación de la máquina. Los dos elementos de datos, (valores medidos y resúmenes de mediciones), son almacenados por separado. Los resúmenes de mediciones se almacenan en los PCR en el TPM. Los valores medidos pueden almacenarse virtualmente en cualquier sitio, típicamente en un SML, pero deben almacenarse de forma encriptada. De hecho, los valores medidos pueden no almacenarse en absoluto, sino volver a calcularse cuando la representación serializada sea necesaria. Los datos de mediciones describen propiedades y características de los componentes medidos. El SML contiene secuencias de valores medidos relacionados. Cada secuencia comparte un resumen de medición común. Los valores medidos son añadidos al resumen de medición común y vueltos a resumir. Esto se refiere más comúnmente con una extensión del resumen. Extender asegura que los valores medidos relacionados no serán ignorados, y el orden de las operaciones se preserva.

De forma algebraica, las actualizaciones a un enésimo PCR, en cualquier momento t+1, siguen como:

$$PCR[n](t+1) = SHA\text{-}1\ (PC[n](t) + \text{datos medidos } (t+1)) \qquad \text{Ecuación (1)}$$

Los valores del PCR son temporales y son establecidos de nuevo al reinicio del sistema. La verificación de los eventos de mediciones requiere la creación de nuevo del resumen de medición y una comparación simple de los valores resumidos, (mediante el uso del valor del PCR como uno de los comparadores). El TCG no define reglas de codificación de datos para los contenidos del SML, pero recomienda seguir los estándares apropiados tales como Lenguaje de Marcado Extensible (XML) para asegurar amplia accesibilidad.

La Figura 1 muestra un procedimiento de atestamiento del TCG convencional, (esto es, protocolo), implementado por un sistema 100 que incluye un retador 105, un agente 110 de plataforma, un TPM 115 y un repositorio 120.

El retador 105 solicita uno o más valores del PCR del agente 110 de plataforma (paso 125). El agente 110 de plataforma recoge entradas del SML, que son valores de mediciones de integridad (paso 130). El agente 110 de plataforma solicita valores del PCR del TPM 115 (paso 135). Los valores del PCR son resúmenes de mediciones de los valores de mediciones de integridad, (esto es, resumen firmado de los valores de mediciones de integridad). El TPM 115 señala los valores del PCR que usa una AIK (paso 140), y envía los valores del PCR firmados al agente 110 de plataforma (paso 145). El agente 110 de plataforma también recoge credenciales que responden por el TPM 115 del repositorio 120 (pasos 150, 155). El agente 110 de plataforma envía los valores del PCR firmados, las entradas del SML y las credenciales al retador 105 (paso 160). El retador 105 entonces verifica la configuración de la plataforma (paso 165). Para la verificación, el retador 105 computa un resumen de medición a partir de las entradas del SML y compara el resumen de medición computado con los valores del PCR. El retador 105 también evalúa las credenciales de la plataforma y comprueba las firmas.

Los valores del PCR son extendidos cada vez que se hace una nueva medición, y esta información es registrada por el TPM 115. Esta extensión asegura que el orden de las mediciones se preserva y que todos los valores de mediciones son tenidos en cuenta. Uno de los retos asociados con la extensión de los valores del PCR es que el estado de una plataforma cambia cuando se realiza cualquier medición, de forma que el estado del sistema podría no ser preciso si una aplicación que no es relevante para la aplicación actual extiende los PCR.

Actualmente no hay una asignación estandarizada de los PCR a aplicaciones más que la reserva del PCR para el proceso de inicio. Esto puede causar situaciones donde más de una aplicación esté usando el mismo PCR que es problemático por las razones perfiladas a continuación.

Por ejemplo, si una aplicación de navegación es cargada antes que una aplicación de gestión de derechos digitales de confianza (DRM), el estado del sistema como es necesitado por la aplicación del DRM puede no coincidir con el estado esperado si ambas aplicaciones hacen uso de los mismos PCR. Esto podría resultar potencialmente en un fallo al cargar la aplicación pues el estado del sistema no es el que debería ser. El retador para la aplicación del DRM también obtendrá información de que el navegador está en ejecución. Esto compromete la privacidad del usuario.

Por ejemplo, la Figura 2 muestra un procedimiento del TCG convencional implementado por un sistema 200 que incluye un primer retador 205, un segundo retador 210 y un dispositivo 215 de usuario que incluye un agente 220 de plataforma y un TPM 225, mediante el cual diferentes aplicaciones extienden un PCR a partir de diferentes estados, inconscientes de las operaciones de extensión de cada una. Si el primer retador 205 solicita el mismo cambio a los valores del PCR que solicita el segundo retador 210, la verificación de la configuración de la plataforma por el segundo retador 210 va a fallar aun cuando la configuración de la plataforma sea válida.

En referencia a la Figura 2, el primer retador 205 envía una solicitud de la configuración de la plataforma desde el agente 220 de plataforma (paso 230), que entonces extiende un PCR en el TPM 225 residente (paso 235) y entonces solicita el valor firmado del PCR desde el TPM 225 (paso 240), que envía de vuelta un valor del PCR firmado, (firmado por el TPM 225 con una AIK), de vuelta al agente 220 de plataforma (paso 245). El primer retador 205 entonces recibe la configuración de la plataforma del agente 220 de plataforma (paso 250). Observe que en este proceso (paso 250) el primer retador 205 normalmente también recibiría el valor del PCR firmado y una entrada del SML, (ninguno de los dos mostrados en la Figura 2), y usa los datos de configuración de la plataforma, los valores del PCR firmados, y las entradas del SML que son recibidas, para verificar la configuración de la plataforma (paso 255).

De manera separada, el segundo retador 210 podría solicitar (paso 260) y después recibir (paso 280) la configuración de la plataforma del agente 220 de plataforma, que extiende el mismo PCR (paso 265) en el TPM 225, y solicita (paso 270) y entonces recibe (paso 275) los valores firmados del PCR del TPM 225. El segundo retador 210 entonces podría verificar la configuración de la plataforma (paso 285) que recibió. El primer retador 205 y el segundo retador 210 pueden no ser conscientes del otro, y dado que las especificaciones del TCG actuales no especifican un método sistemático para asignar qué PCR pueden ser usados para registrar los resúmenes de mediciones que son apropiados y útiles para diferentes retadores en un modo seguro y protector de la privacidad, el mismo PCR puede ser usado para registrar los resúmenes de mediciones para ambos retadores no relacionados. Esto crea un problema donde el segundo retador 210 puede no necesariamente ser consciente del estado del sistema representado por los valores del PCR que son extendidos con las mediciones destinadas al primer retador 205. Así, en el punto de vista del segundo retador 210, a menos que ya haga seguimiento del hecho de que el mismo PCR ha sido extendido por la medición y verificación del primer retador 205, el segundo retador 210 puede comparar conjuntos de datos erróneos en su proceso de verificación porque puede no recibir todos los SML que son requeridos para recrear el orden de la extensión del PCR que tuvo lugar antes de su propia verificación del PCR. De manera alternativa, porque tales SML pueden volverse demasiado grandes tras muchas iteraciones de la extensión del PCR, el segundo retador 201 puede simplemente agotar su capacidad de procesamiento para procesar todas las entradas del SML previas para recrear el estado previo más reciente del PCR.

El procedimiento del TCG de la Figura 2 puede también crear filtraciones de información privada que se puede permitir a un retador pero no a los otros. También el proceso actual puede crear verificaciones no garantizadas,

(cuando la verificación no debería ocurrir), o una decisión no intencionada de no-verificación, (cuando la verificación debería ocurrir), puede ocurrir en los lados de los retadores.

Actualmente, este problema está dirigido mediante el uso de uno o más de los siguientes enfoques:

Reserva de PCR: Como el estado del sistema es representado mediante el uso de los PCR, ciertos PCR pueden ser asignados a ciertas aplicaciones. La desventaja de este enfoque es que el número de los PCR en el TPM está normalmente en torno a 16, (el estándar de TCG no limita el número de los PCR), basándose en consideraciones de coste y tamaño. Esto limita la habilidad de asignar PCR fijos a cada tipo de aplicación.

Uso del Registro de Eventos del PCR: Cualquier cambio de los valores del PCR son registrados por el TPM. Este registro puede ser usado junto con los valores del PCR para ver si el sistema está en un estado correcto. Sin embargo, el problema con este enfoque es que el registro podría contener información que no sea directamente relevante a la aplicación en cuestión y por tanto puede comprometer la privacidad del usuario.

Cargar todas las aplicaciones durante un inicio en un orden predeterminado también elimina el problema. Sin embargo, los tiempos de inicio serán mayores pues todas las aplicaciones tienen que ser verificadas y cargadas durante el inicio lo que hace este enfoque no práctico para usar.

Estos enfoques tienen serias limitaciones, bien en términos de limitar la funcionalidad de la plataforma de confianza o en términos de pérdida de privacidad del usuario.

El documento US 2005/033987 describe un sistema y método que establece y mantiene confianza condicional mediante la exposición de una señal de no confianza de una plataforma informática de confianza a una plataforma informática que necesita la confianza.

La presente invención es definida por las reivindicaciones independientes. Las realizaciones preferidas son especificadas en las reivindicaciones dependientes.

Breve descripción de los dibujos

Se puede tener un mejor entendimiento de la invención a partir de la descripción a continuación de una realización preferida, dada de manera de ejemplo y para ser entendida en conjunto con los dibujos que acompañan:

La Figura 1 muestra un procedimiento de atestación del TCG convencional implementado en un sistema que incluye un retador, un agente de plataforma, un TPM y un repositorio;

La Figura 2 muestra un procedimiento del TCG convencional implementado en un sistema que incluye dos retadores y un dispositivo de usuario por el cual diferentes aplicaciones extienden un PCR desde diferentes estados, inconscientes de las operaciones de extensión de los otros.

La Figura 3 muestra un procedimiento del TCG implementado en un sistema que incluye dos retadores y un dispositivo de usuario que usa una extensión de estado a partir de un estado base común como un ejemplo;

La Figura 4 compara la técnica anterior a la presente invención por la cual diferentes estados extendidos son implementados por diferentes retadores;

La Figura 5 muestra ubicaciones de diferentes estados extendidos en diferentes PCR como un ejemplo;

La Figura 6 muestra un procedimiento del TCG implementado en un sistema que incluye dos retadores y un dispositivo de usuario que usa una extensión de estado base con certificados de estados base de referencia (RBS) según la presente invención;

La Figura 7 ilustra solicitudes selectivas para mediciones como un ejemplo;

La Figura 8 muestra un PCR virtual que usa memoria externa protegida por la capacidad de encriptado de un TPM físico, y cómo un sistema que tiene un TPM y un PCR virtual puede ser usado para suministrar datos para la verificación de la integridad de la configuración de la plataforma por un retador como un ejemplo.

Descripción detallada de las realizaciones preferidas

Las Figuras 3 y 4 muestran diagramas de señales en los cuales se recuperan PCR con respecto a un estado base como un ejemplo.

La Figura 3 muestra un procedimiento del TCG implementado por un sistema 300 que incluye un primer retador 305, un segundo retador 310 y un dispositivo 315 de usuario que incluye un agente 320 de plataforma y un TPM 325, por el cual se usa una extensión de estado a partir de un estado base común. En referencia a la Figura 3, el primer retador 305 solicita la configuración de la plataforma que es computada a partir de un estado base (paso 330) a partir del agente 320 de plataforma, que entonces extiende (paso 335) a partir del estado de base el PCR en el TPM

325, y entonces solicita (paso 340) el valor firmado del PCR del TPM 325, que envía de vuelta (paso 345) el valor del PCR firmado de vuelta al agente 320 de plataforma. El primer retador 305 entonces recibe la configuración de la plataforma (paso 350) del agente 320 de plataforma. El primer retador 305 entonces compara los datos de configuración de la plataforma que recibió en el paso 350 con un valor que computa él mismo y verifica la configuración de la plataforma (paso 355).

De manera separada, el segundo retador 310 podría solicitar más tarde (paso 360) y recibir más tarde (paso 380) la configuración de la plataforma computada otra vez a partir del mismo valor del estado de base que se usa en el paso 335 pero entonces se extiende con un valor de medición diferente, apropiado para el segundo retador 310 y su objetivo y propósitos de verificación. Así, el agente 320 de plataforma, a petición del segundo 310 retador, extendería entonces el mismo PCR (paso 365), no a partir de su último valor sino otra vez a partir del mismo estado base usado en el paso 335. El agente 320 de plataforma entonces solicita (paso 370) y recibe (paso 375) valores firmados (firmados por el TPM 325 con una AIK) del PCR del TPM 325). El segundo retador 310 entonces podría verificar la configuración de la plataforma (paso 385) que recibió. Dado que el primer retador 305 y el segundo retador 310 ambos reciben sus datos de configuración de la plataforma como computados de manera independiente a partir del estado base pero con sus propios valores de mediciones, los procedimientos descritos en la Figura 3 pueden evitar los problemas descritos en el procedimiento convencional de la Figura 2.

La Figura 4 compara la técnica anterior a la presente invención por el cual diferentes estados extendidos son implementados para diferentes retadores. Como se muestra en la Figura 4 un sistema es representado habiendo completado el inicio 405 y habiendo alcanzado un estado 410 base. En la técnica anterior, cuando una primera aplicación es cargada y entonces es verificada por un retador, el estado 415 del sistema es cambiado para reflejar la carga de la primera aplicación. A continuación, cuando una segunda aplicación 425 es cargada y necesita ser verificada por otro retador, el estado 420 del sistema ahora reflejará un cambio a partir del estado 415 del sistema, no a partir del estado 410 base.

Según un ejemplo, dado que los PCR, (o PCR virtuales), que están ubicados para retadores diferentes estarían todos extendidos a partir del estado base, todos los retadores verificarían su estado objetivo con solo el efecto neto de la carga de las aplicaciones que ellos necesitan verificar específicamente. Dos de estos retadores, el retador 1 y el retador 2 son representados en este ejemplo, y ambos verificarían sus estados objetivos derivados, (estado 425 derivado para el retador 1 y estado 430 derivado para el retador 2), como extendidos de manera independiente a partir del estado 410 base.

Según un ejemplo, el TPM establece de nuevo los valores del PCR a sus valores por defecto durante el reinicio del sistema. El sistema referido en este documento es cualquier plataforma tal como un ordenador personal (PC), un asistente de datos personal (PDA), sistemas incorporados, teléfonos móviles, periféricos con sistemas incorporados, elementos de red, y otras plataformas que estén equipadas con tecnologías del TCG, específicamente funciones y servicios habilitados por o habilitados para el uso de un TPM o entidades equivalentes. Los valores del PCR son informados con respecto a un estado base conocido del TPM. Este estado base del TPM es almacenado preferiblemente en el TPM y puede ser usado siempre que una nueva aplicación tenga que ser medida. El estado base del TPM puede representar el estado de la plataforma cuando el proceso de inicio del sistema se completa y el estado de cada aplicación se calcula con respecto a este estado base.

Un estado base de un TPM es un concepto diferente que un estado base para un sistema. Según la presente invención, funcionalidades adicionales de los TPM actuales se definen para que no se tengan que volver a establecer todos los valores del PCR en el inicio, en cambio tendría ciertos valores que pueden representar el 'estado del TPM tras un inicio exitoso' como 'estado base del TPM' y almacenar esos valores en la memoria no volátil escudada dentro del mismo TPM. Observe que tal memoria no volátil es diferente que el PCR, que otra vez, se establece de nuevo tras el inicio. Dado que el estado base del TPM es un valor que representa el estado del TPM tras un inicio exitoso del sistema que alberga el TPM, tal estado base puede representar, indirectamente, un estado 'limpio' del propio sistema. Además, tal estado base del TPM sería no volátil, y puede ser traído de vuelta tras el inicio, para servir como estado base para operaciones de extensión de los PCR. Memoria no volátil escudada, (esto es, protegida), adicional es necesaria para almacenar el estado base dentro del TPM, y también como indicación de la pila de software (TSS) del protocolo de control de transmisión (TCP) para indicar que el estado actual tiene que calcularse a partir del estado base del sistema.

TSS es la pila de software que habilita la inicialización y control de tales procedimientos para mediciones e informes de integridad así como verificación, (por ejemplo, pasos 330, 335, 340, 345, 350, representados en la Figura 3), que tienen lugar fuera del TPM pero dentro o bajo el control de la propia plataforma, (tal como el SO de la plataforma), o sus agentes, (esto es, agente 320 de plataforma en la Figura 3).

Según este ejemplo, un estado base del TPM, es almacenado de manera segura en el propio TPM, y es conocido a través del TSS tras el inicio al exterior del TPM, esto es, al agente de plataforma o el SO de la plataforma, de forma que los retadores pueden usar tales 'estados base del TPM' como el estado base de referencia a partir del cual se pueden construir las mediciones de integridad de las aplicaciones que el retador necesita verificar. Solo una cantidad fija de capacidad de memoria es requerida en el TPM, (igual al número de PCR que contiene el TPM). Este estado base conocido se usa cuando quiera que una nueva aplicación sea cargada por el sistema, de este modo

permitiendo que las mediciones de integridad funcionen del modo que estaban destinadas. Por ejemplo, cuando el TPM tiene un número X de PCR, hay también un número X de 'estados base del TPM', uno por cada uno del número X de PCR. Los estados base del TPM almacenados se usan para extender cada uno de los PCR, cada uno ubicado para medir la integridad de una aplicación cargada particular. Por lo tanto, la integridad de las cargas de al menos X aplicaciones diferentes se les puede hacer seguimiento y medir de esta forma.

Según otro ejemplo, no hay una restricción de tamaño fijo en el número de PCR que podría tener un sistema. Sin embargo, en la práctica el número en la mayoría de implementaciones es aproximadamente de 16 PCR. La extensibilidad en términos de números de identificación del PCR, (las direcciones del PCR pueden estar en un intervalo desde 0 a 2^{32}-1, con valores por encima de 2^{30} reservados para usos futuros), se pueden usar para crear el concepto de PCR virtuales que no están presentes físicamente en el TPM sino que son virtuales en naturaleza. Estos contenidos de los PCR virtuales se pueden almacenar como datos encriptados en almacenamientos externos o en el mismo TPM. El contenido de esos valores de PCR virtuales se puede extender solo desde otros valores de PCR. Esto permite que las aplicaciones definan un estado base basado en que los valores de los PCR se pueden extender. A cada aplicación se le da preferiblemente un número o números de PCR virtuales que pueden ser usados para realizar mediciones de integridad. Esto permite la ubicación de números de PCR para aplicaciones algo similar a la ubicación de números de puertos para aplicaciones de Internet bien conocidas.

Así, según este ejemplo, el espacio de almacenamiento protegido encriptado que una plataforma puede crear, se usa con la funcionalidad criptográfica del TPM, como sustitutos para los PCR implementados en hardware. Dado que el espacio de direccionamiento reservado para los PCR es bastante grande, del orden de 2^{32}, uno simplemente podría usar el espacio de direccionamiento para designar cualquier elemento de memoria protegido criptográficamente en el sistema de la plataforma, (tal como memoria de acceso aleatorio (RAM)), como un sustituto para el PCR. De este modo, uno podría tener muchos más tales 'PCR virtuales' que PCR de hardware, reales. Por lo tanto, uno podría también usar esos muchos más 'PCR virtuales' para hacer seguimiento de la integridad de muchas más cargas de aplicaciones y otros eventos 'merecedores de mediciones'.

Según otro ejemplo, todo el contenido de los PCR es establecido de nuevo durante el inicio del sistema. Como en el ejemplo anterior descrito anteriormente, si hay muchos PCR virtuales o reales, el o los PCR asignados a la aplicación son computados preferiblemente a partir del estado inicializado directamente. Esto podría requerir asignaciones de PCR fijas a aplicaciones pero no requeriría que se almacenara el estado base.

Según este ejemplo, cuando uno tiene numerosos PCR reales o virtuales en un sistema, uno puede repartirlos de manera básica en grupos, y cada grupo de PCR sería entonces ubicado de manera previa para hacer seguimiento de las mediciones de integridad para solo una aplicación, y no se registraría ninguna otra medición de aplicación en cualquiera de los PCR virtuales o reales que no pertenezcan al grupo al cual la aplicación particular se ha asignado. De este modo, aun cuando todos los PCR han sido establecidos de nuevo, y no hay realmente un 'estado base' especial a partir del cual construir la historia de las mediciones de integridad, un PCR puede ser usado por cada grupo como el espacio de tenencia de estados para el 'estado inicial, limpio', tras inicio del sistema, y entonces usar los otros PCR en el mismo grupo para registrar capturas detalladas de las historias de los eventos, (tal como carga de diferentes versiones de la misma aplicación), de una forma predeterminada, secuencial. Así, uno puede no necesitar extender todos los eventos en el mismo PCR, sino más bien, solo registrar las capturas de tales extensiones en diferentes PCR sin extender realmente los PCR individuales. Además, uno puede crear, mediante el uso de un gran número de PCR (todos pertenecientes al mismo grupo) y sus valores, y el conocimiento del orden de los PCR actualizados, un registro histórico de los resúmenes de mediciones de integridad cuyas capturas son mantenidas en cada uno de los PCR pertenecientes a ese grupo, aplicables a solo esa historia de aplicación particular con la plataforma.

La Figura 5 muestra tal configuración del PCR en el cual los PCR para la Aplicación 1 y la Aplicación 2 están disponibles. Los contenidos del PCR se pueden establecer de nuevo cada vez que la aplicación necesita ser medida y los contenidos del PCR serían extendidos a partir de este estado inicializado. Los contenidos de los PCR asignados a los sistemas que operan y controladores junto con los valores del PCR computados para la aplicación pueden ser enviados al retador para verificar la integridad del sistema.

Todos los tres ejemplos presentes anteriormente asisten a los retadores en la verificación de si el estado de la plataforma es el que debería ser sin comprometer la privacidad del usuario.

Todos los tres de esos ejemplos pueden también ser aumentados con el uso del certificado de métricas de integridad de referencia (RIM). Un certificado de RIM convencional se define como un método particular para proporcionar extractos para el proceso de inicio para teléfonos móviles. El certificado de RIM convencional contiene un extracto sobre un estado de referencia que un sistema debería alcanzar tras un inicio. Tras un inicio, si el sistema determina que ha alcanzado el mismo estado que el especificado en el certificado de RIM, entonces el sistema solicita al TPM que actualice su PCR0, (el primer PCR), para contener el valor de la operación resumen SHA del extracto, que declara el estado alcanzado que también está verificado.

Según la presente invención, se usa un certificado de estado base de referencia (RBS). Diferente al certificado de RIM convencional, que puede proporcionar un extracto para solo un único estado, tras inicio común del OS de la

plataforma que es aplicable de manera común a todas las aplicaciones, el nuevo certificado de RBS se usa para proporcionar extractos sobre estados base de referencia específicos a aplicación. Esta diferencia en concepto también resulta en el hecho de que, para un sistema que usa certificados de RBS, una plataforma puede, en cualquier momento dado, alojar múltiples certificados de RBS diferentes, cada uno especificando el estado base para diferentes aplicaciones o grupos de aplicaciones. Esto contrasta con un sistema que solo soporta un certificado de RIM, por el cual en cualquier momento dado, la plataforma puede solo trabajar con un certificado de RIM. De nuevo, uno podría tener múltiples certificados de RBS, cada uno adaptado para especificar los estados base de referencia para eventos, (tal como carga), de muchas aplicaciones diferentes, y cada uno siendo alojado y usado por la plataforma para la referencia de estados base específicos a aplicación en un modo de tiempo simultáneo. En términos de PCR, cada certificado de RBS podría requerir al menos un PCR, (bien real o virtual), dedicado a él. Tal PCR dedicado, por cada certificado de RBS, sería usado para registrar el valor resumen de un extracto que el OS de la plataforma construye para indicar información sobre la verificación o no verificación de estados de la comprobación entre el estado real del sistema y el estado base. El valor resumen sería registrado tras la verificación por el agente de plataforma con la ayuda del TPM, de la igualdad del estado real del sistema al estado base que es indicado en un extracto relacionado con el estado contenido en el certificado de RBS.

Un ejemplo de tal extracto sería: “Se verifica que el estado del sistema real y el estado base son el mismo”. El resumen de tal extracto, que ahora está registrado en el PCR dedicado para ese certificado de RBS, puede proporcionar un punto de inicio para operaciones de extensión adicionales para ese PCR dedicado, así como cualquier otro PCR que puede ser usado para verificación de mediciones de integridad de la aplicación o grupo de aplicaciones asignado. Observe que un certificado de RBS también contiene el valor resumen de tal ‘extracto de comprobación de estado’ que es construido. Así, mediante la comparación del resultado de la operación de resumen, realizada en el extracto que es construido por el OS de la plataforma para indicar si el estado del sistema coincide con el estado base, con el valor resumen del mismo extracto contenido en un certificado de RBS diferente, el OS de la plataforma se provisiona con unos medios para extender los PCR que son asignados para el almacenamiento de los resúmenes de mediciones de integridad para aplicaciones específicas o grupos de aplicaciones, a partir de un valor de punto de inicio verificable externamente. De nuevo, ese valor es el resumen SHA-1 de un extracto referente a la comprobación entre el estado real del sistema y el estado base indicado en el certificado de RBS asociado.

Un certificado de RIM transporta información sobre la métrica de integridad del software del OS central e información relevante para tal OS, tal como el número de versión. Un PCR particular del TPM de la plataforma, a saber, el PCR0, es entonces asignado para llevar el extracto de ‘comprobado o no comprobado’ para el certificado de RIM después de que los valores de referencia de integridad contenidos en el certificado sean comprobados con las mediciones reales.

El estado base usado por la presente invención puede contener diferentes ‘extractos de comprobación de estado’ que pueden compararse con extractos incluidos en varios certificados diferentes. Cada uno de esos certificados puede incluir información sobre diferentes estados base, cada uno perteneciente a una aplicación particular o grupo de aplicaciones u otros contextos.

La Figura 6 muestra un procedimiento del TCG implementado por un sistema 600 que incluye un primer retador 605, un segundo retador 610 y un dispositivo 615 de usuario que incluye un agente 620 de plataforma, un TPM 625 y un certificado 630 de RBS. Como se muestra en la Figura 6, el primer retador 605 puede emitir un comando al agente 620 de plataforma para obtener la configuración de la plataforma computada a partir de una configuración inicial especificada por un estado base (paso 635) aplicable a la aplicación cargada de la cual el primer retador 605 está interesado en verificar la integridad. El agente 620 de plataforma entonces emite un comando (paso 640) al TPM 625 para comprobar el Certificado de RBS aplicable a la aplicación que el primer retador 605 quiere verificar el estado de integridad. El TPM 625 obliga y emite un comando para obtener el Certificado 630 de RBS (paso 645) desde un repositorio de certificados que el TPM 625 controla. El TPM 625 obtiene el Certificado 630 de RBS (paso 650) que también está firmado. El agente 620 de plataforma entonces emite un comando al TPM 625 (paso 655) para realizar una operación de verificación y extensión. En esta operación, el TPM 625 extiende un PCR específico, (bien real o virtual), controlado por el TPM 625 y específico a la aplicación que está siendo verificada su integridad por el primer retador 605, pero solo después de que verifique que el resumen de un extracto, que el agente 620 de plataforma construye tras verificar que el estado del sistema y el estado base, (indicado en el certificado de RBS), son el mismo, es el mismo que el valor resumen contenido en el certificado de RBS. El TPM 625 entonces firma el valor del PCR con una AIK y lo envía al agente 620 de plataforma (paso 660). El agente 620 de plataforma entonces envía la información de configuración de plataforma, que incluye los valores del PCR firmados, al primer retador 605 (paso 665). El primer retador 605 puede entonces verificar (paso 670), mediante el uso de los datos de configuración de la plataforma que recibió del agente 620 de plataforma, si la aplicación en la que está interesado ha sido cargada correctamente y sin comprometer la aplicación del estado del sistema base como se indica en el certificado de RBS.

Cuando otro retador, (esto es, el segundo retador 610), desea verificar la integridad de una aplicación en la cual está interesado, puede realizar de una manera similar, esencialmente los mismos procedimientos (pasos 675 y 698) con la ayuda del agente 620 de plataforma, (que realiza los pasos 680, 692, y 694), y el TPM 625, (que realiza los pasos

685, 690 y 694), pero usando un certificado de RBS diferente, este específico para la aplicación en la cual ese segundo retador 610 está interesado.

La Figura 6 representa el aumento del segundo ejemplo con un certificado de RBS propuesto. Los PCR virtuales son usados para almacenar información sobre los estados base; no mediante el almacenamiento de las mediciones de integridad reales que necesitan ser extendidas, sino mediante el almacenamiento de los extractos de 'comprobado' o 'no comprobado', al igual que el uso actual de los certificados de RIM en módulos de confianza móviles (MTM). Observe que, en vez de extender de manera unilateral el PCR, un comando diferente, (esto es, que extiende el PCR si un resultado de extensión simulado comprueba el estado contenido en el Certificado de RBS), debería ser usado. Además, el valor extendido en el PCR no son los resultados de mediciones reales, sino un extracto que declara si un evento 'comprobado' o 'no comprobado' ha ocurrido cuando la comparación de la extensión real y la información de estado contenida en el certificado de RBS ha sido realizada.

Observe que en la Figura 6, los diferentes retadores pueden usar, para la verificación de una verificación de configuración específica al retador, bien un Certificado de RBS único, común, o diferentes Certificados de RBS, uno para cada uno de los retadores específicos.

Hay ciertos aspectos en el procedimiento usado por la entidad remota para solicitar el estado del sistema que no están definidos por el estándar. Uno de tales aspectos es cómo la entidad remota puede solicitar las mediciones.

La Figura 7 muestra un diagrama de bloques para un ejemplo usando una lista maestra y sublistas. El solicitante identifica preferiblemente las mediciones exactas que necesita eligiendo una o más entidades de la lista maestra y entonces eligiendo uno o más elementos de la sublista para la cual le gustaría recibir las mediciones. Si no hay una sublista específica, se puede asumir que los valores de las mediciones para todas las entidades en la lista maestra son enviados al solicitante. La solicitud puede ser en la forma de solicitud[x][y], donde x representa la información de identificación para la lista maestra, e y identifica los elementos en la sublista. Como se observó anteriormente, y es un elemento opcional en la estructura de solicitud. Esta solicitud puede ser hecha mediante el uso de cualquier mecanismo que incluya el uso de lenguajes como el lenguaje marcado extensible (XML) para comunicar los elementos de la lista y sublistas.

El ejemplo de XML mostrado a continuación para solicitar los valores de mediciones solicitados para las aplicaciones de Internet Explorer y Media Player.

1. <?xml versión="1.0" encoding="UTF-8" ?>
2. <SolicitudValoresPCR>
    i.<ListaMaestra>
    ii. <Id>Aplicaciones</Id>
        1. <SubLista>
    iii. <Id>Internet_Explorer</Id>
    iv. <Id>Media_Player</Id>
        1. <SubLista>
    v.</ListaMaestra>
3. </SolicitudValoresPCR>

Basado en los ejemplos descritos los números de PCR virtuales son asignados a las aplicaciones. Estos valores son preferiblemente cualquier identificador, (por ejemplo, identificador único global (GUID) o identificador único universal (UUID), y similares), y una tabla de correspondencia entre el TPM y las asignaciones del PCR real se almacena preferiblemente en la memoria del TPM. En este escenario, la aplicación que solicita los valores del PCR no conoce los valores del PCR asignados a la aplicación, y realiza una solicitud usando un identificador único que es válido a través de múltiples plataformas.

En relación a los métodos representados anteriormente, la Figura 8 muestra cómo un sistema de dispositivo de usuario que tiene un TPM y PCR virtuales puede ser usado para suministrar datos para verificación de la integridad de configuración de la plataforma a un retador. La Figura 8 muestra un procedimiento de TCG implementado en un sistema 800 que incluye un retador 805 y un dispositivo 810 de usuario que incluye un agente 815 de plataforma, un TPM 820 y un PCR 825 virtual. Observe que el sistema de dispositivo de usuario puede tener PCR virtuales, hasta el orden de 2^{32}.

Como se muestra en la Figura 8, el retador 805 solicita (paso 830) al agente 815 de plataforma que obtenga los datos de configuración de la plataforma que serán luego usados para la verificación de la integridad de la plataforma.

El agente 815 de plataforma emite un comando (paso 835) al TPM 820 para extender un PCR desde un estado base de referencia. El agente 815 de plataforma puede no necesariamente tener que especificar si el PCR del que quiere que el TPM 820 extienda es un PCR físico o un PCR virtual. El TPM 820 entonces extiende el valor del PCR virtual y encripta el PCR 825 virtual con su valor ahora extendido con una clave de encriptación que está almacenada en el TPM 820 mismo o una clave que está almacenada fuera del TPM pero que está protegida por una clave almacenada en el TPM 820 mismo (paso 840). El agente 815 de plataforma después ordena al TPM 820 que firme el valor del PCR y lo envíe al agente 815 de plataforma (paso 845). El TPM 820 entonces accede al PCR 825 virtual y obtiene el valor del PCR encriptado del PCR virtual 825 (pasos 850 y 855). El TPM entonces desencripta (paso 860) el valor del PCR virtual encriptado. El TPM 820 entonces firma el valor del PCR virtual desencriptado, lo vuelve a encriptar, (con una clave diferente que la usada por el retador 805), y lo envía (paso 865) al agente 815 de plataforma. El agente 815 de plataforma compone los datos de configuración de la plataforma, que incluye los datos del PCR 825 virtual, y lo envía al retador 805 (paso 870). El retador 805 entonces usa los datos de configuración de la plataforma recibidos para verificar el estado de integridad, (o estado de configuración de la plataforma), del dispositivo 805 de usuario (paso 875).

Ejemplos

1. En un sistema informático que incluye un dispositivo de usuario que tiene un módulo de plataforma de confianza (TPM), un agente de plataforma y un certificado de estado base de referencia (RBS), un método comprende:

un retador que emite un comando al agente de plataforma para obtener la configuración de la plataforma computada a partir de una configuración inicial especificada por un estado base aplicable a una aplicación cargada para la cual el retador está interesado en verificar la integridad.

2. El método del ejemplo 1 además comprende:

el agente de plataforma que emite un comando al TMP para comprobar el Certificado de RBS aplicable a la aplicación para la cual el retador está interesado en verificar la integridad;

el TPM que obtiene un Certificado de RBS firmado que indica un estado base; y

el agente de plataforma que emite un comando al TPM para realizar una operación de verificación y extensión pro la cual el TPM extiende un registro de configuración de plataforma (PCR) específico controlado por el TPM y específico para la aplicación a la que se le está verificando la integridad para el retador.

3. El método del ejemplo 2 además comprende:

verificar que el estado del sistema y el estado base son el mismo; y

el agente de plataforma verifica que un resumen de un extracto es el mismo que un valor resumen contenido en el certificado de RBS.

4. El método del ejemplo 3 además comprende:

el TPM que firma un valor del PCR con una clave de identificación de atestación (AIK);

el TPM que envía el valor del PCR firmado al agente de plataforma; y

el agente de plataforma que envía la información de configuración de plataforma, que incluye el valor del PCR firmado, al retador.

5. El método como en cualquiera de los ejemplos 1 a 4 además comprende:

el retador verifica si la aplicación ha sido cargada correctamente y sin comprometer la aplicación del estado del sistema base correcto como se indica en el certificado de RBS.

6. Un dispositivo de usuario que comprende:

al menos un certificado de estado base de referencia (RBS);

un agente de plataforma configurado para recibir un primer comando de un retador para obtener una configuración de plataforma computada a partir de una configuración de inicio especificada por un estado base aplicable a la aplicación cargada para la cual el restador está interesado en verificar la integridad; y

un módulo de plataforma de confianza (TPM) configurado para recibir un segundo comando para comprobar un Certificado de RBS aplicable a la aplicación en la cual el retador está interesado en verificar la integridad, para obtener un Certificado de RBS firmado que indica un estado base, donde el agente de plataforma emite un tercer comando al TPM para realizar una operación de verificación y extensión por la cual el TPM extiende un registro de

configuración de plataforma (PCR) específico controlado por el TPM y específico a la aplicación cuya integridad está siendo verificada para el retador.

7. El dispositivo de usuario del ejemplo 6 donde si el estado del sistema y el estado base se verifican que son el mismo, el agente de plataforma verifica que un resumen de un extracto es el mismo que un valor de resumen contenido en el certificado de RBS.

8. El dispositivo de usuario del ejemplo 7 donde el TPM firma un valor de PCR con una clave de identificación de atestación (AIK), y envía el valor de PCR firmado al agente de plataforma.

9. El dispositivo de usuario del ejemplo 8 donde el agente de plataforma envía información de configuración de plataforma, que incluye el valor de PCR firmado, al retador.

10. El dispositivo de usuario como en cualquiera de los ejemplos de 6 a 9 donde el retador verifica si la aplicación ha sido cargada correctamente y sin compromiso a la aplicación a partir del estado del sistema base correcto como se indica en el certificado de RBS.

11. Un módulo de plataforma de confianza (TPM) para verificar aplicaciones que comprende:

una memoria no volátil escudada que comprende:

ubicaciones de primera memoria para almacenar una pluralidad de registros de configuración de plataforma (PCR), donde el TPM establece de nuevo los valores de los PCR a valores por defecto durante un reinicio del sistema; y

ubicaciones de segunda memoria para almacenar una pluralidad de estados base que representan el estado de la plataforma cuando un proceso de inicio de sistema se completa con éxito, donde el estado de la menos una aplicación se calcula con respecto a un estado base.

12. El TPM del ejemplo 11 donde el sistema es seleccionado del grupo que incluye un ordenador personal (PC), un asistente de datos personal (PDA), un sistema incorporado, un teléfono móvil, periféricos con sistemas incorporados, elementos de red, y otras plataformas que estén equipadas con tecnologías de Grupo Informático de Confianza (TCG), específicamente funciones y servicios habilitados por o habilitados para el uso del TPM.

13. En un sistema informático que incluye un dispositivo de usuario que tiene un módulo de plataforma de confianza (TPM) y un agente de plataforma, el TPM tiene una memoria no volátil escudada que almacena una pluralidad de registros de configuración de la plataforma (PCR), un método que comprende:

un primer retador que envía una solicitud para una configuración de plataforma que está computada a partir de un estado base específico del agente de plataforma;

el agente de plataforma que extiende un registro de configuración de plataforma (PCR) del TPM a partir del estado base específico con un primer valor de medición;

el agente de plataforma que solicita el valor firmado del PCR particular del TPM;

el TPM que envía el valor de PCR firmado al agente de plataforma;

el primer retador que recibe una configuración de plataforma de agente de plataforma; y

el primer retador que compara los datos de configuración de plataforma con un valor que computa él mismo y verifica la configuración de la plataforma.

14. El método del ejemplo 13 que además comprende:

un segundo retador que solicita y recibe la configuración de plataforma computada otra vez a partir del estado base específico;

el agente de plataforma que extiende el PCR particular con un segundo valor de medición que es diferente del primer valor de medición;

el agente de plataforma que solicita y recibe valores firmados del PCR particular del TPM; y

el segundo retador que verifica la configuración de la plataforma que recibe.

15. El método del ejemplo 14 donde el primer y segundo retadores ambos reciben sus datos de configuración de plataforma como computados de manera independiente a partir del estado base pero con sus propios valores de mediciones.

16. En un módulo de plataforma de confianza (TPM) que tiene una memoria no volátil escudada que almacena una pluralidad de registros de configuraciones de plataforma (PCR), un método comprende:

repartir los PCR en grupos; y

asignar por adelantado cada grupo de PCR para hacer seguimiento de mediciones de integridad para una aplicación, donde ninguna otra medición de aplicación puede ser registrada en cualquiera de los PCR que no pertenezca al grupo al cual la aplicación particular se ha asignado.

17. El método del ejemplo 16 donde cuando todos los PCR son establecidos de nuevo, usan un PCR de cada grupo como un espacio de tenencia de estados para después del inicio, 'estado inicial, limpio' de un sistema.

18. El método del ejemplo 17 que además comprende:

usar los otros PCR en los grupos para registrar capturas detalladas de las historias de los eventos de una forma predeterminada, secuencial.

19. El método del ejemplo 18 donde los eventos incluyen la carga de diferentes versiones de la misma aplicación.

20. El método del ejemplo 18 que además comprende:

registrar capturas de las extensiones del PCR en diferentes PCR sin realmente extender PCR individuales.

21. En un sistema informático que incluye un dispositivo de usuario que tiene un módulo de plataforma de confianza (TPM), un agente de plataforma y un registro de configuración de plataforma (PCR) virtual, un método para suministrar datos de configuración de plataforma para la verificación de la integridad de la configuración de la plataforma a un retador, el método comprende:

el retador que solicita al agente de plataforma que obtenga los datos de configuración de la plataforma que serán después usados para verificar la integridad de una plataforma;

el agente de plataforma que envía un comando al TPM para extender un PCR a partir de un estado base de referencia;

el TPM que extiende un valor del PCR virtual; y

el TPM que encripta el PCR virtual con su nuevo valor extendido con una clave de encriptación que está almacenada dentro del propio TPM o una clave que está almacenada fuera del TPM pero que está protegida por una clave almacenada dentro del TPM.

22. El método del ejemplo 21 que además comprende:

el agente de plataforma que ordena al TPM que firme el valor del PCR y envíe el valor del PCR firmado al agente de plataforma;

el TPM que accede al PCR virtual y obtiene el valor del PCR encriptado del PCR virtual; y

el TPM que desencripta el valor del PCR virtual encriptado.

23. El método del ejemplo 22 que además comprende:

el TPM que firma el valor del PCR virtual desencriptado;

el TPM que vuelve a encriptar el valor del PCR desencriptado con una clave diferente que la que tiene el retador; y

el TPM que envía el valor del PCR encriptado de nuevo al agente de plataforma.

24. El método del ejemplo 23 que además comprende:

el agente de plataforma que compone datos de configuración de plataforma, que incluye los datos del PCR virtual;

el agente de plataforma que envía los datos compuestos al retador; y

el retador que usa los datos compuestos para verificar el estado de integridad, o estado de configuración de la plataforma, del dispositivo de usuario.

Aunque las características y elementos de la presente invención son descritos en las realizaciones preferidas en combinaciones particulares, cada característica o elemento se puede usar solo sin las otras características y

elementos de las realizaciones preferidas o en varias combinaciones con o sin otras características y elementos de la presente invención. Los métodos o diagramas de flujo proporcionados en la presente invención pueden implementarse en un programa informático, software, o firmware realizado de manera tangible en un medio de almacenamiento legible por un ordenador para ser ejecutado por un ordenador o procesador de propósito general. Ejemplos de medios de almacenamiento legibles por un ordenador incluyen una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM), un registro, una memoria caché, dispositivos de memoria semiconductores, medios magnéticos tales como discos duros internos y discos extraíbles, medios magnetópticos, y medios ópticos tal como discos CD-ROM, y discos versátiles digitales (DVD).

Los procesadores adecuados incluye, a modo de ejemplo, un procesador de propósito general, un procesador de propósito específico, un procesador convencional, un procesador de señal digital (DSP), una pluralidad de microprocesadores, uno o más microprocesadores en asociación con un núcleo de DSP, un controlador, un microcontrolador, Circuitos Integrados Específicos de Aplicación (ASIC), circuitos de Matrices de Puertas Programables en Campo (FPGA), y otro tipo de circuito integrado (IC), y/o máquina de estado.

Un procesador en asociación con software puede usarse para implementar un transceptor de frecuencia de radio para usar en una unidad de recepción transmisión inalámbrica (WTRU), equipo de usuario (UE), terminal, estación base, controlador de red por radio (RNC), o cualquier equipo informático. La WTRU puede usarse junto con módulos, implementados en hardware y/o software, tal como una cámara, un módulo de cámara de video, un videoteléfono, un teléfono altavoz, un dispositivo de vibración, un altavoz, un micrófono, un transceptor de televisión, un auricular manos libres, un teclado, un módulo de Bluetooth®, una unidad de radio modulada en frecuencia (FM), una unidad de representación de cristal líquido (LCD), una unidad de representación de diodo emisor de luz orgánico (OLED), un reproductor de música digital, un reproductor de medios, un módulo reproductor de video juegos, un navegador de Internet, y/o cualquier módulo de red de área local inalámbrico (WLAN).

REIVINDICACIONES

1. Un dispositivo (615) de usuario que comprende:

una memoria en la cual se ha implementado un repositorio de certificados, el repositorio de certificados que tiene una pluralidad de estados base de referencia firmados, RBS, certificados, cada uno estando asociado con una aplicación y que comprende un estado base que es específico a una aplicación asociada y a un primer valor resumen de un extracto que indica si un estado de sistema real del dispositivo de usuario coincide con el estado base de la aplicación asociada;

un agente de plataforma (620) configurado para recibir un primer comando de un retador (605; 610) para obtener una configuración de plataforma computada a partir de una configuración inicial especificada por el estado base del certificado de RBS firmado para la aplicación cargada para la cual el retador está interesado en verificar la integridad; y

un módulo (625) de plataforma de confianza, TPM, configurado para recibir un segundo comando del agente de plataforma para comprobar el certificado de RBS aplicable a la aplicación cargada para la cual el retador está interesado en verificar la integridad, y obtener el certificado de RBS firmado del repositorio de certificados, donde:

el agente de plataforma además está configurado para construir un segundo valor resumen de un extracto que indica si un segundo estado de sistema real del dispositivo de usuario coincide con el estado base de la aplicación asociada contenida en el certificado de RBS, y emitir un tercer comando al TPM para realizar una operación de verificación y extensión; y

el TPM además está configurado para extender un registro de configuración de plataforma específico, PCR, controlado por el TPM y específico a la aplicación cuya integridad está siendo verificada para el retador, tras verificar que el primer valor resumen del certificado de RBS firmado es el mismo que el segundo valor resumen construido por el agente de plataforma, donde

el TPM está además configurado para firmar el valor de PCR con una clave de identificación de atestación y enviar el valor de PCR firmado al agente de plataforma.

2. El dispositivo de usuario de la reivindicación 1 donde el agente (620) de plataforma está además configurado para enviar información de configuración de plataforma, que incluye el valor de PCR firmado, al retador (605; 610).

3. El dispositivo de usuario de la reivindicación 2 donde el retador está configurado para verificar que la aplicación cargada asociada con el certificado de RBS firmado fue cargada a partir de un estado base correcto como se indica en el certificado de RBS firmado.

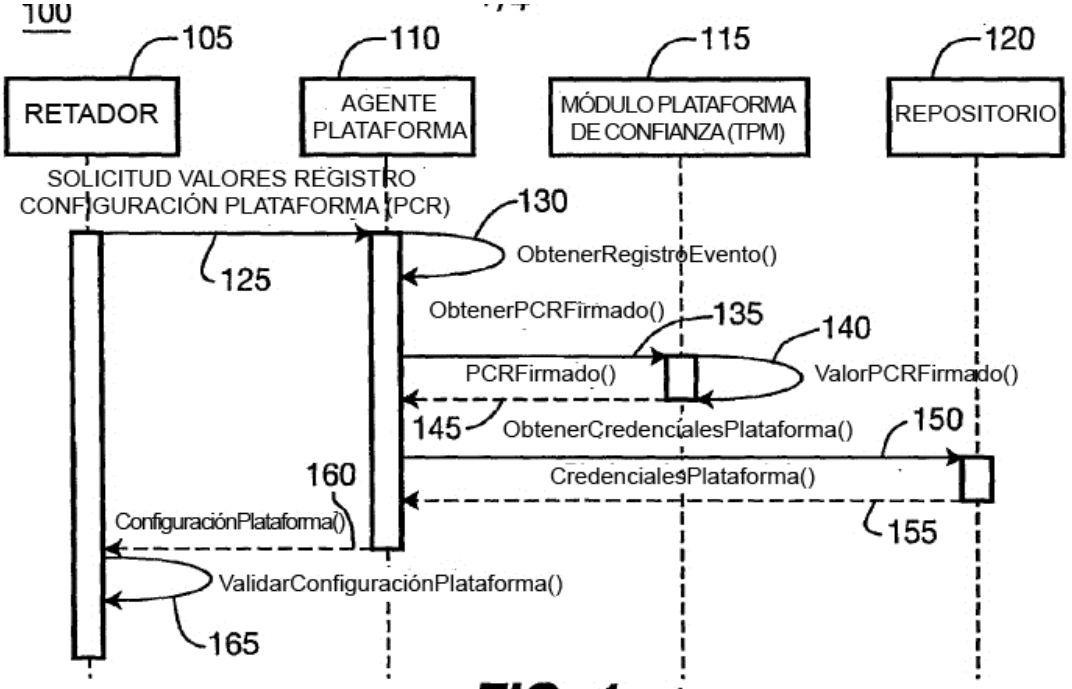

FIG. 1 TÉCNICA ANTERIOR

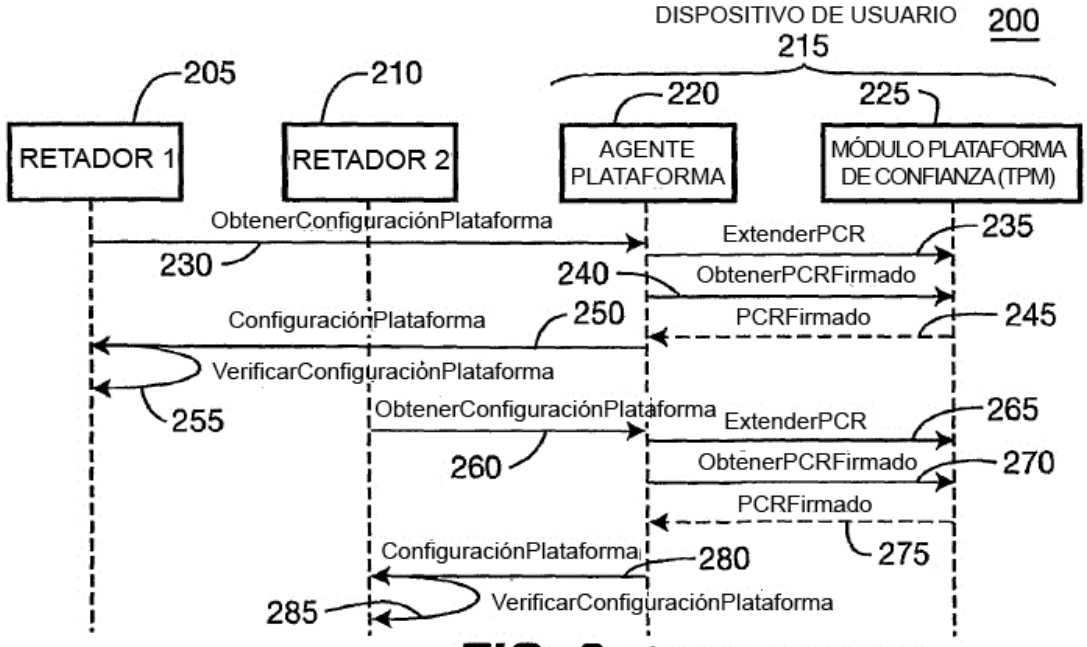

FIG. 2 TÉCNICA ANTERIOR

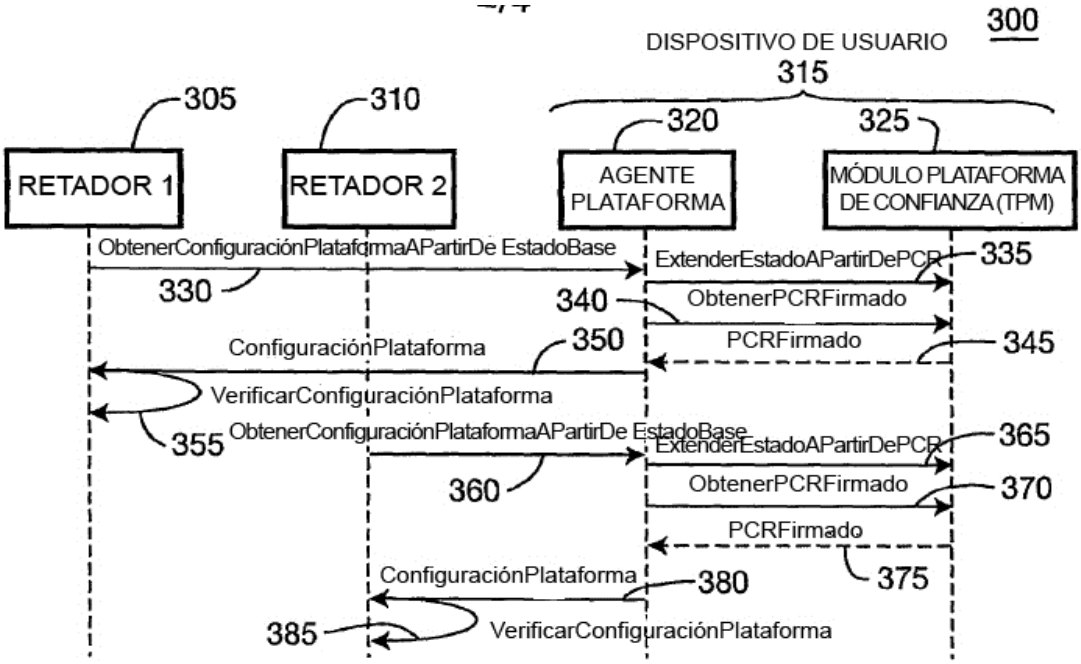
300
DISPOSITIVO DE USUARIO
315
305
310
320
325
RETADOR 1
RETADOR 2
AGENTE PLATAFORMA
MÓDULO PLATAFORMA DE CONFIANZA (TPM)
ObtenerConfiguraciónPlataformaAPartirDe EstadoBase
330
ExtenderEstadoAPartirDePCR
335
340
ObtenerPCRFirmado
PCRFirmado
345
ConfiguraciónPlataforma
350
VerificarConfiguraciónPlataforma
355
ObtenerConfiguraciónPlataformaAPartirDe EstadoBase
ExtenderEstadoAPartirDePCR
365
360
ObtenerPCRFirmado
370
PCRFirmado
375
ConfiguraciónPlataforma
380
385
VerificarConfiguraciónPlataforma

FIG. 3

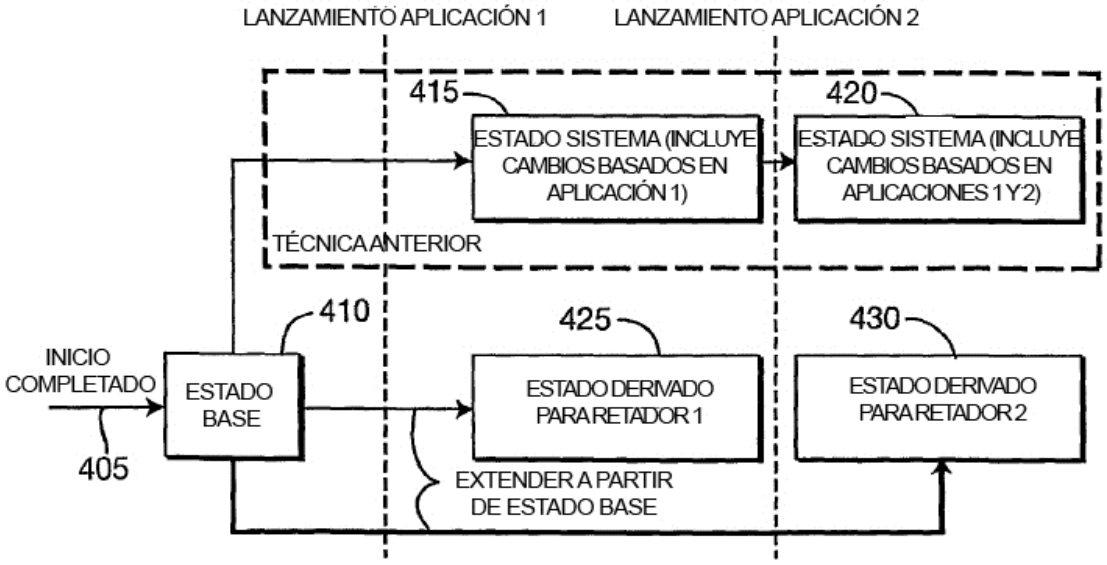
LANZAMIENTO APLICACIÓN 1
LANZAMIENTO APLICACIÓN 2
415
ESTADO SISTEMA (INCLUYE CAMBIOS BASADOS EN APLICACIÓN 1)
420
ESTADO SISTEMA (INCLUYE CAMBIOS BASADOS EN APLICACIONES 1 Y 2)
TÉCNICA ANTERIOR
410
425
430
INICIO COMPLETADO
ESTADO BASE
ESTADO DERIVADO PARA RETADOR 1
ESTADO DERIVADO PARA RETADOR 2
405
EXTENDER A PARTIR DE ESTADO BASE

FIG. 4


PCR
PCR DEL SISTEMA OPERATIVO
PCR DEL SISTEMA
PCR DISPONIBLES
PCR PARA APLICACIÓN 1
PCR PARA APLICACIÓN 2

FIG. 5

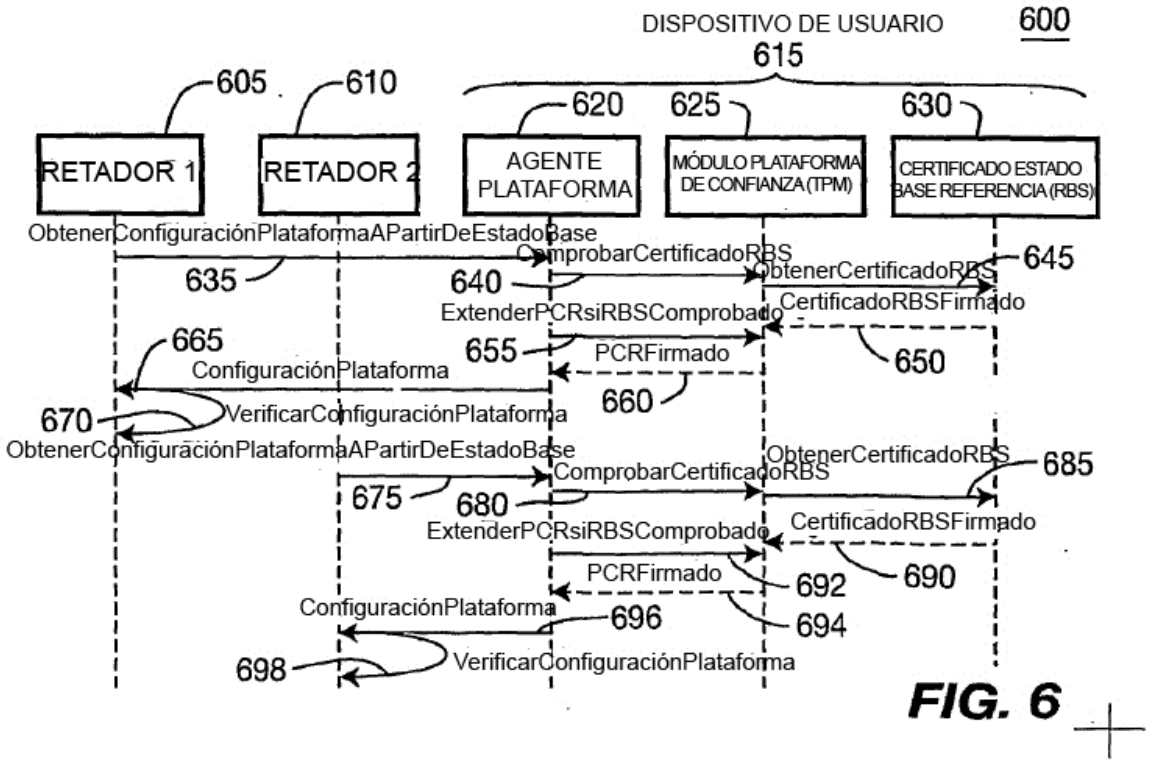
DISPOSITIVO DE USUARIO
600
615
605
610
620
625
630
RETADOR 1
RETADOR 2
AGENTE PLATAFORMA
MÓDULO PLATAFORMA DE CONFIANZA (TPM)
CERTIFICADO ESTADO BASE REFERENCIA (RBS)
ObtenerConfiguraciónPlataformaAPartirDeEstadoBase
635
ComprobarCertificadoRBS
640
ObtenerCertificadoRBS
645
CertificadoRBSFirmado
650
ExtenderPCRsiRBSComprobado
655
PCRFirmado
660
665
ConfiguraciónPlataforma
670
VerificarConfiguraciónPlataforma
ObtenerConfiguraciónPlataformaAPartirDeEstadoBase
675
ComprobarCertificadoRBS
680
ObtenerCertificadoRBS
685
CertificadoRBSFirmado
690
ExtenderPCRsiRBSComprobado
692
PCRFirmado
694
ConfiguraciónPlataforma
696
698
VerificarConfiguraciónPlataforma

FIG. 6

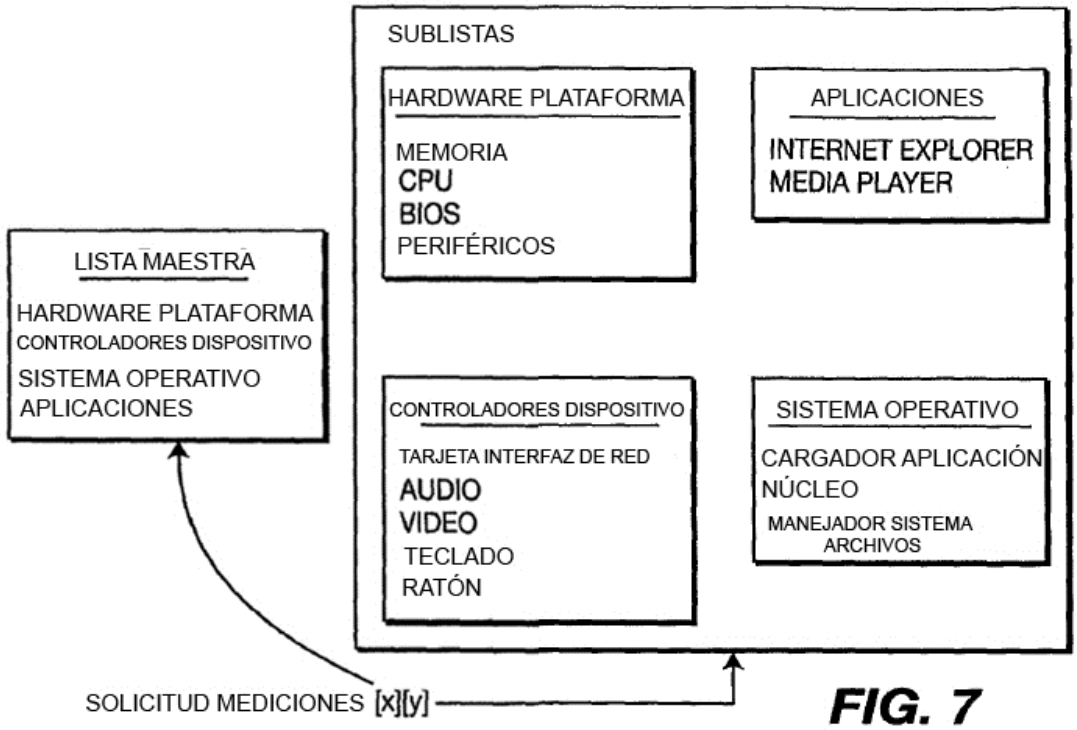
SUBLISTAS
HARDWARE PLATAFORMA
MEMORIA
CPU
BIOS
PERIFÉRICOS
APLICACIONES
INTERNET EXPLORER
MEDIA PLAYER
LISTA MAESTRA
HARDWARE PLATAFORMA
CONTROLADORES DISPOSITIVO
SISTEMA OPERATIVO
APLICACIONES
CONTROLADORES DISPOSITIVO
TARJETA INTERFAZ DE RED
AUDIO
VIDEO
TECLADO
RATÓN
SISTEMA OPERATIVO
CARGADOR APLICACIÓN
NÚCLEO
MANEJADOR SISTEMA ARCHIVOS
SOLICITUD MEDICIONES [x][y]

FIG. 7

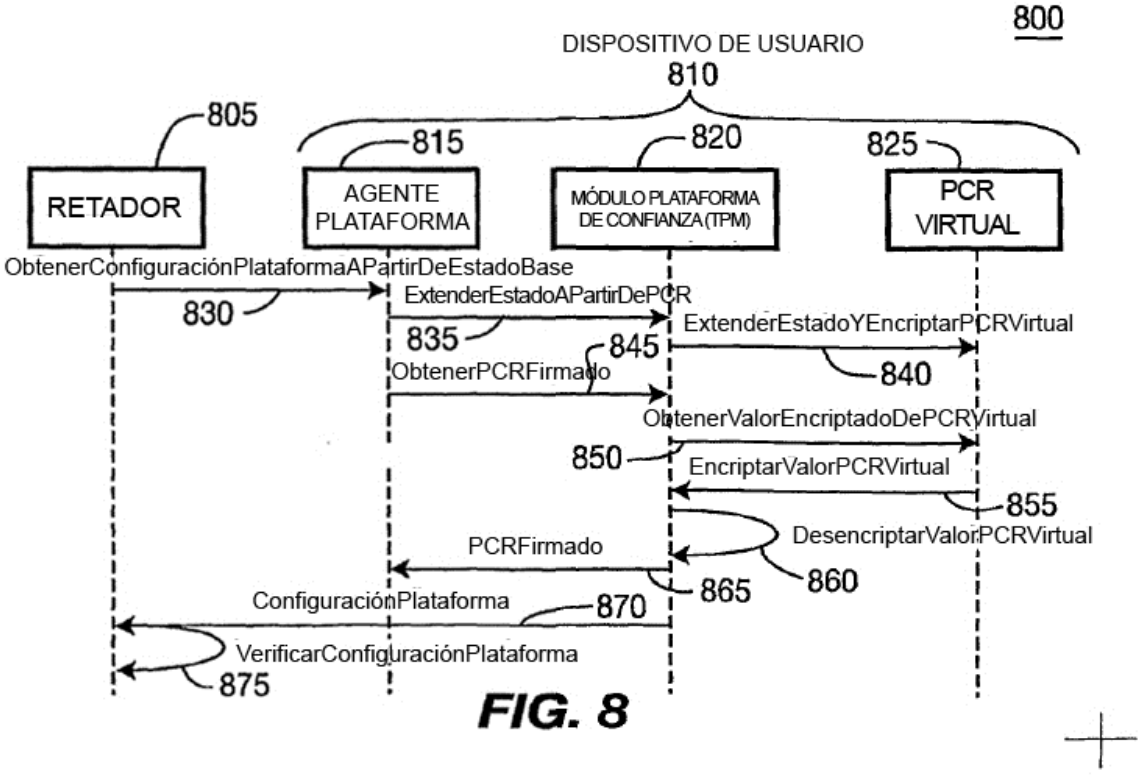
800
DISPOSITIVO DE USUARIO
810
805
815
820
825
RETADOR
AGENTE PLATAFORMA
MÓDULO PLATAFORMA DE CONFIANZA (TPM)
PCR VIRTUAL
ObtenerConfiguraciónPlataformaAPartirDeEstadoBase
830
ExtenderEstadoAPartirDePCR
835
ExtenderEstadoYEncriptarPCRVirtual
840
845
ObtenerPCRFirmado
ObtenerValorEncriptadoDePCRVirtual
850
EncriptarValorPCRVirtual
855
DesencriptarValorPCRVirtual
860
PCRFirmado
865
ConfiguraciónPlataforma
870
VerificarConfiguraciónPlataforma
875

FIG. 8