(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 862**

(51) Int. CI.:

G06F 21/64 (2013.01)
G06F 21/79 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.07.2008 PCT/EP2008/058909**

(87) Fecha y número de publicación internacional: **29.01.2009 WO09013132**

(96) Fecha de presentación y número de la solicitud europea: **09.07.2008 E 08774915 (6)**

(97) Fecha y número de publicación de la concesión europea: **29.03.2017 EP 2171632**

(54) Título: **Procedimiento y equipo para comprobar la integridad de datos memorizados en una zona de memoria predeterminada perteneciente a una memoria**

(30) Prioridad:

24.07.2007 DE 102007034525

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.07.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
WITTELSBACHERPLATZ 2
80333 MÜNCHEN, DE

(72) Inventor/es:

BUSSER, JENS-UWE y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO Y EQUIPO PARA COMPROBAR LA INTEGRIDAD DE DATOS MEMORIZADOS EN UNA ZONA DE MEMORIA PREDETERMINADA PERTENECIENTE A UNA MEMORIA

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un equipo para comprobar la integridad de datos memorizados en una zona de memoria predeterminada perteneciente a una memoria.

El ámbito técnico de la invención se refiere a la comprobación de la integridad de datos memorizados, en particular de firmware o software. Un tal software o firmware es adecuado para controlar aparatos de campo, sensores, actuadores, unidades de DVD, discos duros o similares. Los mismos pueden ser además adecuados para comunicar mediante una red entre sí o con otros aparatos, como servidores u ordenadores personales. Desde luego si estos aparatos no están protegidos físicamente, tienen entonces los atacantes la posibilidad de acceder al software o firmware en particular para fines de ingeniería inversa (Reverse Engineering). También existe el peligro de que se devuelva al correspondiente aparato un software o firmware manipulado.

Puede lograrse una seguridad frente a manipulación del software o firmware del correspondiente aparato tomando medidas de hardware, como por ejemplo mediante un sellado el aparato. Tras el sellado del aparato no son posibles ya manipulaciones. Desde luego no sería posible entonces tampoco una posterior actualización (update) legal, consciente y deseada del firmware.

Otra posibilidad de protección puede lograrse mediante una prueba de integridad y autenticidad del firmware cargado al realizar la actualización del firmware basándose en firmas digitales. Pero esto presupone que en el proceso de carga puede realizarse un control y no se sustituye simplemente el módulo de memoria del firmware.

Como posibilidad adicional para la seguridad frente a manipulaciones, conoce la entidad solicitante internamente la realización de un control de integridad del software para un aparato mediante el cálculo de una suma de comprobación para el software actualmente existente y comparación de la suma de comprobación calculada con una suma de comprobación archivada. Entonces puede estar configurada la suma de comprobación como suma de prueba criptográfica y la suma de comprobación archivada puede estar archivada firmada. Entonces pueden consultar en un acoplamiento del correspondiente aparato mediante una red otros nodos de red o equipos a través de los canales de comunicación existentes esta suma de comprobación y compararla con el valor deseado. Desde luego si se sobreescribe el software del correspondiente aparato mediante una actualización con un firmware manipulado, entonces deja de tener validez esta posibilidad de control, ya que el aparato manipulado puede seguir contestando consultas relativas a su suma de comprobación con el valor deseado, siempre que la correspondiente suma de comprobación permanezca almacenada en el aparato manipulado. Entonces ciertamente no corresponde ya la suma de comprobación memorizada a la suma de comprobación real del software actualmente existente en el aparato correspondiente. Pero la misma está memorizada fijamente en el aparato manipulado para simular la integridad del software memorizado.

El documento US 6,954,861 B2 da a conocer un procedimiento para comprobar la autenticidad de un primer sistema de comunicación (client o cliente), que busca acceso a un segundo sistema de comunicación (host o anfitrión). Para ello explora a continuación el segundo sistema de comunicación (host) la zona de memoria en la que está memorizado un software determinado en el primer sistema de comunicación (client), para comprobar si puede asociarse a un sistema de comunicación registrado.

El documento EP 1 030 237 A1 da a conocer un sistema para un equipo de cálculo en el que un componente de vigilancia realiza comprobaciones de datos en una plataforma de cálculo.

El documento EP 1 056 010 A1 muestra la creación de un valor Hash para datos que se memorizan en una zona de memoria no segura, memorizándose el valor Hash en una zona de memoria asegurada.

En consecuencia es un objetivo de la presente invención vigilar la integridad de datos memorizados, en particular de firmware o software, de un primer equipo mediante un segundo equipo acoplado con el primer equipo. De acuerdo con la invención se logra el objetivo formulado mediante las reivindicaciones independientes.

En consecuencia se propone un procedimiento para comprobar la integridad de datos memorizados en una zona de memoria predeterminada de una memoria de un primer equipo, estando acoplado el primer equipo con al menos un segundo equipo mediante una red, que presenta las siguientes etapas:

a) proporcionar al menos un parámetro que es adecuado para influir sobre un valor Hash de al menos una función Hash predeterminada;

b) cálculo de al menos un valor Hash en función de los datos memorizados en la memoria predeterminada, de la función Hash predeterminada y de las que al menos hay una del parámetro, de los que al menos hay uno y

c) comprobación de la integridad de los datos memorizados en la zona de memoria predeterminada del primer equipo, en función del valor Hash calculado o de los valores Hash calculados mediante el segundo equipo,

incluyendo el parámetro, de los que al menos hay uno, un cierto número de indicadores de lugar de memoria, con lo que se definen al menos dos segmentos de memoria de la zona de memoria predeterminada, cubriendo los segmentos de memoria definidos al menos la zona de memoria predeterminada, calculándose en cada caso un valor Hash en función de los datos de uno de los segmentos de memoria y de una de las funciones Hash predeterminadas.

Además se propone un sistema para comprobar la integridad de datos memorizados en una zona de memoria predeterminada de un primer equipo, estando acoplado el primer equipo con al menos un segundo equipo mediante una red y presentando el sistema:

- un medio para determinar o proporcionar al menos un parámetro que es adecuado para influir sobre un valor Hash de al menos una función Hash predeterminada;
- el primer equipo, que calcula al menos un valor Hash en función de los datos memorizados en la zona de memoria predeterminada, de la función Hash predeterminada, de las que al menos hay una y del parámetro, de los que al menos hay uno y
- el segundo equipo, que comprueba la integridad de los datos memorizados en la zona de memoria predeterminada del primer equipo en función del valor Hash calculado o de los valores Hash calculados, incluyendo el parámetro, de los que al menos hay uno, una cierta cantidad de indicadores de lugar de memoria, con lo que se definen al menos dos segmentos de memoria de la zona de memoria predeterminada y los segmentos de memoria definidos cubren al menos la zona de memoria predeterminada, calculándose en cada caso un valor Hash en función de los datos de uno de los segmentos de memoria y de una de las funciones Hash predeterminadas.

Una ventaja de la presente invención reside en que el primer equipo comprobado sólo puede calcular y generar el valor Hash correcto o los valores Hash correctos cuando el primer equipo dispone también realmente de todos los datos cuya integridad se ha de comprobar. En particular, debido a la utilización del parámetro que influye sobre el correspondiente valor Hash, no es suficiente calcular una vez el o los valores Hash de los datos y memorizarlos a continuación, con lo que los datos podrían ser borrados o sobreescritos. Con preferencia está configurada la memoria del primer equipo tal que el mismo presenta, además de la (primera) zona de memoria predeterminada para memorizar los datos, una segunda zona de memoria. La primera zona de memoria es adecuada para memorizar los datos, en particular el software o firmware, del primer equipo. La segunda zona de memoria está prevista en particular para memorizar contenidos que no tienen que protegerse. Si por ejemplo está configurado el primer equipo como sensor, entonces está prevista la segunda zona de memoria para memorizar los correspondientes datos de medida y/o el número de identificación del sensor.

En particular está configurada la primera zona de memoria más grande o mucho más grande que la segunda zona de memoria.

Ejemplos de funciones Hash que pueden utilizarse son MD5, SHA-1, SHA-2xx.

Ventajosas variantes y perfeccionamientos de la invención resultan de las reivindicaciones secundarias, así como de la descripción con referencia a los dibujos.

Según un perfeccionamiento preferente de la invención, incluye la etapa c) del procedimiento:

c1) transmisión del valor Hash calculado, de los que al menos hay uno, desde el primer equipo al segundo equipo mediante la red;

c2) cálculo de al menos un valor Hash de comparación en función de una copia de los datos memorizados en la zona de memoria predeterminada, que está memorizada en el segundo equipo, de la función Hash predeterminada, de las que al menos hay una y del parámetro predeterminado, de los que al menos hay uno y

c3) comparación del valor Hash transmitido con el valor Hash de comparación calculado mediante el segundo equipo, para proporcionar un resultado de la comprobación.

Según una variante preferida de la invención, incluye el parámetro, de los que al menos hay uno, una cierta cantidad de indicadores de lugar de memoria, definiendo en cada caso dos indicadores de lugar de memoria un segmento de memoria de la zona de memoria predeterminada y cubriendo los segmentos de memoria definidos al menos la zona de memoria predeterminada, calculándose en cada caso un valor Hash en función de los datos de uno de los segmentos de memoria y de una de las funciones Hash predeterminadas.

Según otra variante preferida, incluye el parámetro, de los que al menos hay uno, dos indicadores de lugar de memoria, definiendo un primer indicador de lugar de memoria y un extremo final de la zona de memoria

predeterminada un primer segmento de memoria, definiendo un segundo indicador de lugar de memoria y un comienzo de la zona de memoria predeterminada un segundo segmento de memoria y cubriendo los segmentos de memoria definidos al menos la zona de memoria predeterminada, calculándose en cada caso un valor Hash en función de los datos de uno de los segmentos de memoria y de una de las funciones Hash predeterminadas.

Según otra variante preferida, está configurado el parámetro, de los que al menos hay uno, como un único indicador de celda de memoria, que divide la zona de memoria predeterminada en dos segmentos de memoria, calculándose en cada caso un valor Hash en función de los datos de uno de los segmentos de memoria y de una de las funciones Hash predeterminadas.

Según otra variante preferida, se calcula el correspondiente valor Hash de comparación en función de una copia de los datos memorizados en el correspondiente segmento de memoria y de la correspondiente función Hash predeterminada mediante el segundo equipo.

Según otra variante preferida, está configurado el parámetro, de los que al menos hay uno, como número aleatorio, mediante el cual se inicializa la correspondiente función Hash. El correspondiente valor Hash se calcula en función de los datos memorizados en la zona de memoria predeterminada y de la correspondiente función Hash inicializada.

Según otra variante preferida, se calcula el correspondiente valor Hash de comparación en función de una copia de los datos memorizados en la zona de memoria predeterminada y de la correspondiente función Hash predeterminada inicializada mediante el segundo equipo.

Según otra variante preferida, se calcula el valor Hash, de los que al menos hay uno, en función de los datos memorizados en la zona de memoria predeterminada, de la función Hash predeterminada, de las que al menos hay una, del parámetro, de los que al menos hay uno y de un número de identificación del primer equipo. Lo correspondiente es válido también para el valor Hash de comparación.

Según otra variante preferida, incluye la etapa del procedimiento a) las siguientes etapas parciales del procedimiento:

a1) aportación del parámetro, de los que al menos hay uno, que es adecuado para influir sobre un valor Hash de al menos una función Hash predeterminada, mediante el segundo equipo y
a2) transmisión del parámetro proporcionado desde el segundo equipo al primer equipo.

Según otra variante preferida, deduce el primer equipo el parámetro, de los que al menos hay uno, del valor Hash calculado o de los valores Hash calculados de una comprobación de integridad precedente.

Según otra variante preferente, se proporciona en cada comprobación de los datos memorizados en la zona de memoria predeterminada un nuevo parámetro.

Además se propone un producto de programa de computadora que provoca sobre un equipo controlado por programa la ejecución de un procedimiento como el antes indicado para la comprobación de la identidad.

También puede pensarse por ejemplo en aportar el producto de programa de computadora como medio de memoria, como tarjeta de memoria, lápiz USB, floppy, CD-ROM, DVD o también en forma de un fichero que puede descargarse desde un servidor en una red. Esto puede realizarse por ejemplo en una red de comunicación inalámbrica mediante la transmisión del correspondiente fichero con el producto de programa de computadora sobre el primer y/o segundo equipo.

La invención se describirá a continuación más en detalle en base a los ejemplos de realización indicados en las figuras esquemáticas. Se muestra en:

figura 1 un esquema de circuitos en bloques de un ejemplo de realización del sistema de acuerdo con la invención;
figura 2 un diagrama secuencial esquemático de un primer ejemplo de realización del procedimiento de acuerdo con la invención;
figura 3 un diagrama secuencial esquemático de un segundo ejemplo de realización del procedimiento de acuerdo con la invención;
figura 4 un diagrama secuencial esquemático de un tercer ejemplo de realización del procedimiento de acuerdo con la invención;
figura 5 un esquema de circuitos en bloques de la memoria del primer equipo sobre la cual se aplica una primera variante del procedimiento según la figura 2;
figura 6 un esquema de circuitos en bloques de la memoria del primer equipo sobre la cual se aplica una segunda variante del procedimiento según la figura 2;
figura 7 un esquema de circuitos en bloques de la memoria del primer equipo sobre la cual se aplica una tercera variante del procedimiento según la figura 2;

figura 8 un esquema de circuitos en bloques de la memoria del primer equipo sobre la cual se aplica una cuarta variante del procedimiento según la figura 2 y

figura 9 un esquema de circuitos en bloques de la memoria del primer equipo sobre la cual se aplica una quinta variante del procedimiento según la figura 2.

En todas las figuras están dotados los mismos elementos y equipos, o bien los que funcionan de la misma manera, de las mismas referencias, siempre que no se indique lo contrario.

La figura 1 muestra un esquema de circuitos en bloques de un ejemplo de realización del sistema 6 de acuerdo con la invención para comprobar la integridad de datos D memorizados en una zona de memoria SB1 predeterminada de una memoria 1 de un primer equipo 2. El primer equipo 2 está acoplado con al menos un segundo equipo 3 mediante una red 4.

El sistema 6 presenta un primer medio 7, el primer equipo 2 y el segundo equipo 3. Según el ejemplo de realización de la figura 1, está situado el primer medio 7 en el segundo equipo 3. Desde luego puede pensarse también en situar el primer medio 7 en el primer equipo 2 la integridad de cuyos datos ha de comprobarse. El primer medio 7 es adecuado para determinar o proporcionar al menos un parámetro P que es adecuado para influir sobre un valor Hash H1, H2 de al menos una función Hash predeterminada.

El primer equipo 2 calcula al menos un valor Hash H1, H2 en función de los datos D memorizados en una zona de memoria SB1 predeterminada, de la función Hash predeterminada, de las que al menos hay una y del parámetro P, de los que al menos hay uno.

Si se calcula por ejemplo sólo un valor Hash H1 para toda la zona de memoria SB1 predeterminada, entonces resulta el valor Hash H1 de la ecuación (1) siguiente:

$$(1) \quad H1 = f_{hash}(P, D(SB1)),$$

siendo P el parámetro, f_{hash} la función Hash utilizada y D(SB1) los datos que están memorizados en la zona de memoria SB1 predeterminada.

La referencia 8 designa un segundo medio, que está previsto en el primer equipo 2 y que realiza el cálculo de los valores Hash H1, H2.

El segundo equipo 3 es adecuado para comprobar la integridad de los datos D memorizados en la zona de memoria SB1 predeterminada del primer equipo, en función del valor Hash H1 calculado o de los valores Hash H1, H2 calculados. Para ello presenta el segundo equipo 3 un tercer medio 9, que realiza el cálculo en función de una copia K de los datos D memorizados en la zona de memoria SB1 predeterminada, que está memorizada en una segunda memoria 5 del segundo equipo 3 de la función Hash f_{hash} predeterminada, de las que al menos hay una y del parámetro P predeterminado, de los que al menos hay uno, Para el ejemplo antes descrito calcula el tercer medio 9 el único valor Hash de comparación H1' mediante la siguiente ecuación (2):

$$(2) \quad H1' = f_{hash}(P, K)$$

Con preferencia se proporciona en cada nueva comprobación de los datos D memorizados en la zona de memoria SB1 predeterminada de la memoria 1 del primer equipo 2 un nuevo parámetro P mediante el primer medio 7.

En particular la primera zona de memoria SB1 de la memoria 1 es mayor o claramente mayor que la segunda zona de memoria SB2 de la memoria 1, que memoriza contenidos cuya integridad no ha de comprobarse.

La figura 2 muestra un primer ejemplo de realización del procedimiento de acuerdo con la invención para comprobar la identidad de datos D memorizados en la zona de memoria SB1 predeterminada de la memoria 1 del primer equipo 2. A continuación se describirá el primer ejemplo de realización del procedimiento de acuerdo con la invención en base al esquema de circuitos de bloques de la figura 2 con referencia a la figura 1. El primer ejemplo de realización del procedimiento de acuerdo con la invención según la figura 2 presenta las siguientes etapas del procedimiento a) a c):

Etapa del procedimiento a):

Se proporciona al menos un parámetro P que es adecuado para influir sobre un valor Hash H1, H2 de al menos una función Hash predeterminada.

Con preferencia se proporciona en cada nueva comprobación de los datos D memorizados en una zona de memoria SB1 predeterminada un nuevo parámetro P.

Etapa del procedimiento b):

Se calcula el valor Hash H1, H2, de los que al menos hay uno, en función de los datos D memorizados en la zona de memoria SB1 predeterminada, de la función Hash, de las que al menos hay una y del parámetro P, de los que al menos hay uno.

Etapa del procedimiento c):

La integridad de los datos D memorizados en la zona de memoria SB1 predeterminada del primer equipo 2, se comprueba en función del valor Hash H1 calculado o de los valores Hash H1, H2 calculados mediante el segundo equipo 3.

En particular puede deducirse en comprobaciones a realizar con regularidad de la integridad el parámetro P o los parámetros del valor Hash H1 o de los valores Hash H1, H2 de la comprobación precedente. Por ejemplo podría deducirse P como los 32 bits menos significativos del valor Hash H1 de la comprobación precedente.

Con ello puede comprobar el primer equipo 2 a comprobar la integridad de sus datos D o bien del software o firmware sin tener la necesidad de obtener cada vez antes de la comprobación el correspondiente parámetro P o los correspondientes parámetros P del segundo equipo 3. En consecuencia puede suprimirse un mensaje de solicitud del segundo equipo que realiza la comprobación 3 al primer equipo a comprobar 2. Esto es especialmente ventajoso cuando el segundo equipo 3 está configurado como un servidor (server) que realiza las comprobaciones, que ha de comprobar una pluralidad de primeros equipos 2 o nodos de red.

Esta variante es en particular ventajosa cuando queda asegurado que no se pierde ningún mensaje entre el primer equipo 2 y el segundo equipo 3. Pero si esto no puede asegurarse, debe implementarse adicionalmente un mecanismo de sincronización para la comprobación.

La figura 3 muestra un segundo ejemplo de realización del procedimiento de acuerdo con la invención. El segundo ejemplo de realización según la figura 3 se diferencia del primer ejemplo de realización según la figura 2 en que las etapas del procedimiento a1) y a2) correspondientes a la figura 3 sustituyen a la etapa del procedimiento a) según la figura 2. Por el contrario se corresponden entre sí las etapas del procedimiento b) y c) y por esta razón no se describirán. El segundo ejemplo de realización del procedimiento de acuerdo con la invención según la figura 3 presenta en consecuencia las etapas del procedimiento a1) y a2) que se describen más abajo y las etapas del procedimiento b) y c) descritas en relación con la figura 2:

Etapa del procedimiento a1):

El parámetro P, de los que al menos hay uno, que es adecuado para influir sobre un valor Hash H1, H2 de al menos una función Hash predeterminada, lo proporciona el segundo equipo 3.

Etapa del procedimiento a2):

El parámetro P proporcionado se transmite mediante el segundo equipo 3 al primer equipo 2 mediante la red 4.

La figura 4 muestra un tercer ejemplo de realización del procedimiento de acuerdo con la invención. El tercer ejemplo de realización del procedimiento de acuerdo con la invención según la figura 4 se diferencia del primer ejemplo de realización del procedimiento de acuerdo con la invención según la figura 2 en que las etapas del procedimiento c1) a c3) según la figura 4 sustituyen a la etapa del procedimiento c) según la figura 2. Las etapas del procedimiento a) y b) según la figura 4 corresponden a las etapas del procedimiento a) y b) según la figura 2. En consecuencia presenta el tercer ejemplo de realización del procedimiento de acuerdo con la invención según la figura 4 las etapas del procedimiento a) y b) descritas en relación con la figura 2, así como las etapas del procedimiento c1) a c3), que se describen a continuación:

Etapa del procedimiento c1):

El valor Hash H1, H2 calculado, de los que al menos hay uno, se transmite mediante el primer equipo 2 al segundo equipo 3 mediante la red 4.

Etapa del procedimiento c2):

Al menos un valor Hash de comparación H1', H2' se calcula en función de una copia K de los datos D memorizados en la zona de memoria SB1 predeterminada, que está memorizada en el segundo equipo 3, de la función Hash predeterminada, de las que al menos hay una y del parámetro P predeterminado, de los que al menos hay uno. Si calcula por ejemplo el primer equipo 2 dos valores Hash H1 y H2 según las ecuaciones (3) y (4) que van a continuación, entonces calcula el segundo equipo 3 los correspondientes valores Hash de comparación H1' y H2' mediante las ecuaciones (5) y (6) que se encuentran más abajo:

(3) $H1 = f_{hash}(P,D(SB1))$

(4) $H2 = f'_{hash}(P,D(SB1))$

(5) $H1' = fhash(P,K)$

(6) $H2' = f'hash(P,K)$

En particular tienen ambas funciones Hash f_{hash} y f'_{hash} una constitución diferente. Pero también pueden ser ambas idénticas.

Las figuras 5 a 9 muestran variantes de los tres ejemplos de realización del procedimiento de acuerdo con la invención según las figuras 2 a 4, en particular del procedimiento según la figura 2.

Según la figura 5 incluye el parámetro P, de los que al menos hay 1, cuatro indicadores de lugar de memoria S1-S4.

Los indicadores de lugar de memoria S1 y S4 definen un primer segmento de memoria SA1 de la zona de memoria SB1 predeterminada. Además definen los indicadores de lugar de memoria S2 y S3 un segundo segmento de memoria SA2 de la zona de memoria SB1 predeterminada. Ambos segmentos de memoria SA1 y SA2 cubren al menos la zona de memoria SB1 predeterminada. Según el ejemplo de realización de la figura 5, forman los mismos también un solape entre los indicadores de lugar de memoria S1 y S2, así como entre S3 y S4.

El primer valor Hash H1 se calcula en función de los datos D(SA1) del primer segmento de memoria SA1 y de una de las funciones Hash predeterminadas f_{hash} (véase la ecuación 7):

(7) $H1 = f_{hash}(D(SA1))$

El segundo valor Hash H2 se calcula en función de los datos D(SA2) del segundo segmento de memoria SA2 y de una de las funciones Hash f'_{hash} predeterminadas (véase la ecuación 8):

(8) $H2 = f'_{hash}(D(SA2))$

Las funciones f_{hash} y f'_{hash} pueden estar configuradas diferentes, pero también pueden ser idénticas.

En particular proporciona los indicadores de lugar de memoria S1 a S4 el segundo equipo a comprobar 3 al primer equipo 2, con lo que el equipo 2 comprobado no tiene ninguna posibilidad de calcular previamente, total o parcialmente, los valores Hash H1 y H2 de las funciones Hash f_{hash}, f'_{hash} y con ello de sustraer a la comprobación partes de los datos D o bien del software.

Según la figura 6 incluye el parámetro P, de los que al menos hay uno, dos indicadores de lugar de memoria S1, S2. El primer indicador de lugar de memoria S1 y un extremo final S5 de la zona de memoria SB1 predeterminada definen el primer segmento de memoria SA1. El segundo indicador de lugar de memoria S2 y el comienzo S0 de la zona de memoria SB1 predeterminada definen el segundo segmento de memoria SA2. También ambos segmentos de memoria SA1 y SA2 según la figura 6 no sólo cubren la zona de memoria SB1 predeterminada - al igual que la figura 5 - por completo, sino que forman un solape, según la figura 6, entre S1 y S2. El cálculo de los valores Hash H1, H2 resulta análogamente de las ecuaciones anteriores (7) y (8).

Según la figura 7 está configurado el parámetro P, de los que al menos hay uno, como un único indicador de lugar de memoria S1, que divide la zona de memoria SB1 predeterminada en los dos segmentos de memoria SA1, SA2. El cálculo de los valores Hash H1, H2 resulta análogamente de ambas ecuaciones anteriores (7) y (8).

Evidentemente puede dividirse la zona de memoria SB1 predeterminada según las figuras 5 a 7 no sólo en dos segmentos de memoria SA1, SA2, sino en cualquier cantidad de segmentos de memoria, bien calculándose entonces para cada segmento de memoria un valor Hash propio o bien calculándose un valor Hash común para varios segmentos de memoria, que se combinan en una secuencia arbitraria, pero fijamente definida.

Según las figuras 8 y 9 está configurado el parámetro P, de los que al menos hay uno, como al menos un numero aleatorio R, mediante el cual se inicializa la correspondiente función Hash. El correspondiente valor Hash H1 se calcula entonces en función de los datos D(SB1) memorizados en la zona de memoria SB1 predeterminada y de la correspondiente función Hash f_{hash} inicializada. Por ejemplo se calcula el valor Hash H1 entonces a partir de la siguiente ecuación (9):

(9) $H1 = f_{hash}(R,D)$

(10) $H1' = f'_{hash}(R,K)$

En consecuencia se calcula el correspondiente valor Hash de comparación H1' en función de una copia K de los datos D memorizados en la zona de memoria SB1 predeterminada y de la correspondiente función Hash predeterminada inicializada mediante el segundo equipo 3 (véase la ecuación (10)). Ambas variantes según las figuras 8 y 9 se diferencian en el sentido de que el cálculo del valor Hash H1 se realiza en un caso desde el comienzo S0 de la zona de memoria SB1 predeterminada hasta su final S5 (véase al respecto la figura 8) y en el otro caso en sentido inverso de S5 hacia S0 (véase al respecto la figura 9).

Aun cuando la presente invención se ha descrito en el presente caso en base a ejemplos de realización preferentes, no queda limitada la misma a éstos, sino que puede modificarse de diversas formas. Por ejemplo puede pensarse en configurar el parámetro P, de los que al menos hay uno, tal que el mismo contenga tanto indicadores de lugar de memoria como también al menos un número aleatorio.

REIVINDICACIONES

1. Procedimiento para comprobar la integridad de datos (D) memorizados en una zona de memoria (SB1) predeterminada de una memoria (1) de un primer equipo (2), estando acoplado el primer equipo (2) con al menos un segundo equipo (3) mediante una red (4), con las etapas:
   a) proporcionar al menos un parámetro (P) que es adecuado para influir sobre un valor Hash (H1, H2) de al menos una función Hash predeterminada;
   b) cálculo de al menos un valor Hash (H1, H2) en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, de la función Hash predeterminada, de las que al menos hay una y del parámetro (P), de los que al menos hay uno y
   c) comprobación de la integridad de los datos (D) memorizados en la zona de memoria (SB1) predeterminada del primer equipo (2), en función del valor Hash calculado (H1) o de los valores Hash calculados (H1, H2) mediante el segundo equipo (3),

   incluyendo el parámetro (P), de los que al menos hay uno, un cierto número de indicadores de lugar de memoria (S1-S4), con lo que se definen al menos dos segmentos de memoria (SA1, SA2) de la zona de memoria (SB1) predeterminada, cubriendo los segmentos de memoria (SA1, SA2) definidos al menos la zona de memoria (SB1) predeterminada, calculándose en cada caso un valor Hash (H1, H2) en función de los datos de uno de los segmentos de memoria (SA1, SA2) y de una de las funciones Hash predeterminadas.

2. Procedimiento de acuerdo con la reivindicación 1,
   caracterizado porque la etapa c) del procedimiento incluye:
   c1) transmisión del valor Hash (H1, H2) calculado, de los que al menos hay uno, desde el primer equipo (2) al segundo equipo (3) mediante la red (4);
   c2) cálculo de al menos un valor Hash de comparación (H1', H2') en función de una copia (K) de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, que está memorizada en el segundo equipo (3), de la función Hash predeterminada, de las que al menos hay una y del parámetro (P) predeterminado, de los que al menos hay uno y
   c3) comparación del valor Hash (H1, H2) transmitido con el valor Hash de comparación (H1', H2') calculado mediante el segundo equipo (3), para proporcionar un resultado de la comprobación.

3. Procedimiento de acuerdo con la reivindicación 1 y 2,
   caracterizado porque el parámetro (P), de los que al menos hay uno, incluye una cierta cantidad de indicadores de lugar de memoria (S1-S4), definiendo en cada caso dos indicadores de lugar de memoria (S1, S4; S3, S2) un segmento de memoria (SA1, SA2) de la zona de memoria (SB1) predeterminada y cubriendo los segmentos de memoria (SA1, SA2) definidos al menos la zona de memoria (SB1) predeterminada, calculándose en cada caso un valor Hash (H1, H2) en función de los datos de uno de los segmentos de memoria (SA1, SA2) y de una de las funciones Hash predeterminadas.

4. Procedimiento de acuerdo con la reivindicación 1 ó 2,
   caracterizado porque el parámetro (P), de los que al menos hay uno, incluye dos indicadores de lugar de memoria (S1, S2), definiendo un primer indicador de lugar de memoria (S1) y un extremo final (S5) de la zona de memoria (SB1) predeterminada un primer segmento de memoria (SA1), definiendo un segundo indicador de lugar de memoria (S2) y un comienzo (S0) de la zona de memoria (SB1) predeterminada un segundo segmento de memoria (SA2) y cubriendo los segmentos de memoria (SA1, SA2) definidos al menos la zona de memoria (SB1) predeterminada, calculándose en cada caso un valor Hash (H1, H2) en función de los datos de uno de los segmentos de memoria (SA1, SA2) y de una de las funciones Hash predeterminadas.

5. Procedimiento de acuerdo con la reivindicación 3 ó 4,
   caracterizado porque el correspondiente valor Hash de comparación (H1', H2') se calcula en función de una copia (K) de los datos memorizados en el correspondiente segmento de memoria (SA1, SA2) y de la correspondiente función Hash predeterminada mediante el segundo equipo (3)

6. Procedimiento de acuerdo con la reivindicación 1 o una de las reivindicaciones 2 a 5,
   caracterizado porque el valor Hash (H1, H2), de los que al menos hay uno, se calcula en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, de la función Hash predeterminada, de las que al menos hay una, del parámetro (P), de los que al menos hay uno y de un número de identificación del primer equipo (2).

7. Procedimiento de acuerdo con la reivindicación 1 o una de las reivindicaciones 2 a 6,
   caracterizado porque la etapa del procedimiento a) incluye:
   a1) aportación del parámetro (P), de los que al menos hay uno, que es adecuado para influir sobre un valor Hash (H1, H2) de al menos una función Hash predeterminada, mediante el segundo equipo (3) y
   a2) transmisión del parámetro (P) proporcionado desde el segundo equipo (3) al primer equipo (2).

8. Procedimiento de acuerdo con la reivindicación 1 o una de las reivindicaciones 2 a 7,

caracterizado porque el primer equipo (2) deduce el parámetro (P), de los que al menos hay uno, del valor Hash (H1) calculado o de los valores Hash (H1, H2) calculados de una comprobación de integridad precedente.

9. Procedimiento de acuerdo con la reivindicación 1 o una de las reivindicaciones 2 a 8,
caracterizado porque en cada comprobación de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, se proporciona un nuevo parámetro.

10. Producto de programa de computadora,
que provoca sobre un equipo controlado por programa la ejecución de un procedimiento de acuerdo con una de las reivindicaciones 1 a 9.

11. Sistema (6) para comprobar la integridad de datos (D) memorizados en una zona de memoria (SB1) predeterminada correspondiente a una memoria (1) de un primer equipo (2), estando acoplado el primer equipo (2) con al menos un segundo equipo (3) mediante una red (4), con:
- un medio (7) para proporcionar al menos un parámetro (P), que es adecuado para influir sobre un valor Hash (H1, H2) de al menos una función Hash predeterminada;
- el primer equipo (2), que calcula al menos un valor Hash (H1, H2) en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, de la función Hash predeterminada, de las que al menos hay una y del parámetro (P), de los que al menos hay uno y
- el segundo equipo (3), que comprueba la integridad de los datos (D) memorizados en la zona de memoria (SB1) predeterminada del primer equipo (2) en función del valor Hash (H1) calculado o de los valores Hash (H1, H2) calculados,

incluyendo el parámetro (P), de los que al menos hay uno, una cierta cantidad de indicadores de lugar de memoria (S1-S4), con lo que se definen al menos dos segmentos de memoria (SA1, SA2) de la zona de memoria (SB1) predeterminada y los segmentos de memoria (SA1, SA2) definidos cubren al menos la zona de memoria (SB1) predeterminada, calculándose en cada caso un valor Hash (H1, H2) en función de los datos de uno de los segmentos de memoria (SA1, SA2) y de una de las funciones Hash predeterminadas.

12. Procedimiento para comprobar la integridad de datos (D) memorizados en una zona de memoria (SB1) predeterminada de una memoria (1) de un primer equipo (2), estando acoplado el primer equipo (2) con al menos un segundo equipo (3) mediante una red (4), con las etapas:
a) proporcionar al menos un parámetro (P), que es adecuado para influir sobre un valor Hash (H1, H2) de al menos una función Hash predeterminada;
b) cálculo de al menos un valor Hash (H1, H2) en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, de la función Hash predeterminada, de las que al menos hay una y del parámetro (P), de los que al menos hay uno y
c) comprobación de la integridad de los datos (D) memorizados en la zona de memoria (SB1) predeterminada del primer equipo (2), en función del valor Hash calculado (H1) o de los valores Hash calculados (H1, H2) mediante el segundo equipo (3),

en el que el parámetro (P), de los que al menos hay uno, está configurado como al menos un número aleatorio (R), mediante el cual se inicializa la correspondiente función Hash,
calculándose el correspondiente valor Hash (H1) en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada y de la correspondiente función Hash inicializada.

13. Procedimiento de acuerdo con la reivindicación 12,
caracterizado porque la etapa c) del procedimiento incluye:
c1) transmisión del valor Hash (H1, H2) calculado, de los que al menos hay uno, desde el primer equipo (2) al segundo equipo (3) mediante la red (4);
c2) cálculo de al menos un valor Hash de comparación (H1', H2') en función de una copia (K) de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, que está memorizada en el segundo equipo (3), de la función Hash predeterminada, de las que al menos hay una y del parámetro (P) predeterminado, de los que al menos hay uno y
c3) comparación del valor Hash (H1, H2) transmitido con el valor Hash de comparación (H1', H2') calculado mediante el segundo equipo (3), para proporcionar un resultado de la comprobación.

14. Procedimiento de acuerdo con la reivindicación 12,
caracterizado porque el correspondiente valor Hash de comparación (H1') se calcula en función de una copia (K) de los datos (D) memorizados en la zona de memoria (SB1) predeterminada y de la correspondiente función Hash predeterminada inicializada mediante el segundo equipo (3)

15. Procedimiento de acuerdo con la reivindicación 12, 13 ó 14,
caracterizado porque el valor Hash (H1, H2), de los que al menos hay uno, se calcula en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, de la función Hash predeterminada, de las que al menos hay una, del parámetro (P), de los que al menos hay uno y de un número de identificación del primer equipo (2).

16. Procedimiento de acuerdo con la reivindicación 12 o una de las reivindicaciones 13 a 15, **caracterizado porque** la etapa del procedimiento a) incluye:
a1) aportación del parámetro (P), de los que al menos hay uno, que es adecuado para influir sobre un valor Hash (H1, H2) de al menos una función Hash predeterminada, mediante el segundo equipo (3) y
a2) transmisión del parámetro (P) proporcionado desde el segundo equipo (3) al primer equipo (2).

17. Procedimiento de acuerdo con la reivindicación 12 o una de las reivindicaciones 13 a 16, **caracterizado porque** el primer equipo (2) deduce el parámetro (P), de los que al menos hay uno, del valor Hash (H1) calculado o de los valores Hash (H1, H2) calculados de una comprobación de integridad precedente.

18. Procedimiento de acuerdo con la reivindicación 12 o una de las reivindicaciones 13 a 17, **caracterizado porque** en cada comprobación de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, se proporciona un nuevo parámetro.

19. Producto de programa de computadora, **que** provoca sobre un equipo controlado por programa la ejecución de un procedimiento de acuerdo con una de las reivindicaciones 12 a 18.

20. Sistema (6) para comprobar la integridad de datos (D) memorizados en una zona de memoria (SB1) predeterminada correspondiente a una memoria (1) de un primer equipo (2), estando acoplado el primer equipo (2) con al menos un segundo equipo (3) mediante una red (4), con:
- un medio (7) para proporcionar al menos un parámetro (P), que es adecuado para influir sobre un valor Hash (H1, H2) de al menos una función Hash predeterminada;
- el primer equipo (2), que calcula al menos un valor Hash (H1, H2) en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada, de la función Hash predeterminada, de las que al menos hay una y del parámetro (P), de los que al menos hay uno y
- el segundo equipo (3), que comprueba la integridad de los datos (D) memorizados en la zona de memoria (SB1) predeterminada del primer equipo (2) en función del valor Hash (H1) calculado o de los valores Hash (H1, H2) calculados,

en el que el parámetro (P), de los que al menos hay uno, está configurado como al menos un número aleatorio (R), mediante el cual se inicializa la correspondiente función Hash,
calculándose el correspondiente valor Hash (H1) en función de los datos (D) memorizados en la zona de memoria (SB1) predeterminada y de la correspondiente función Hash inicializada.

FIG 1

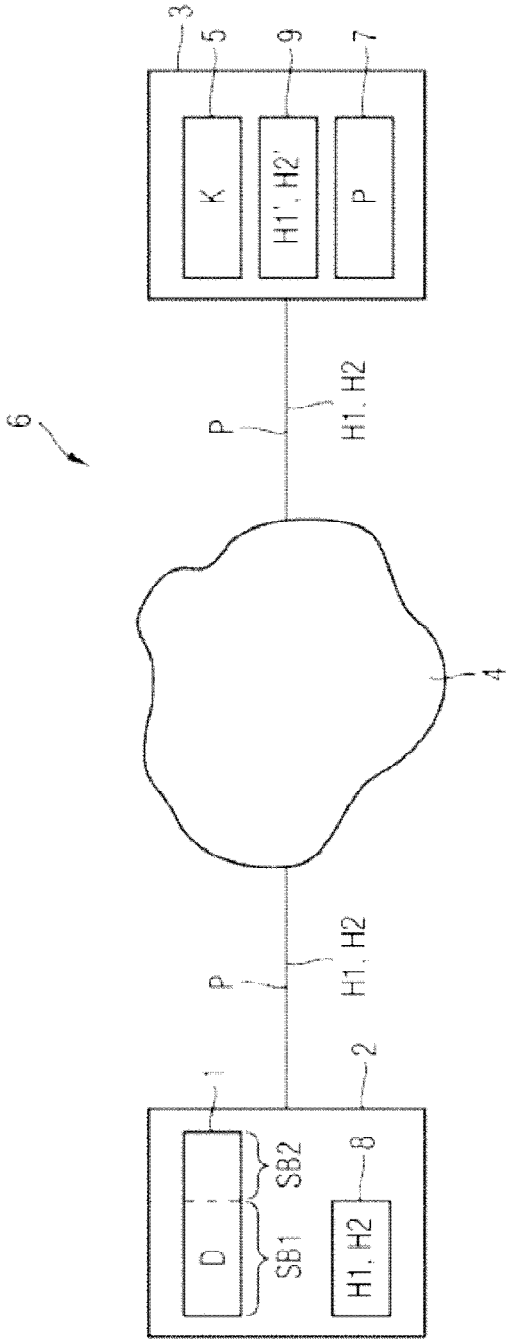

FIG 2

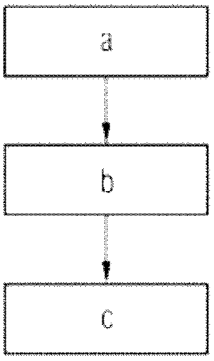

FIG 3

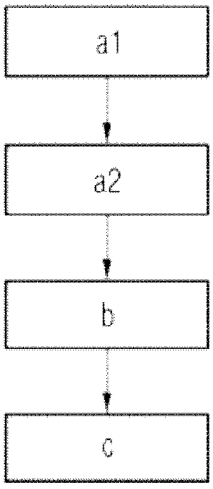

FIG 4

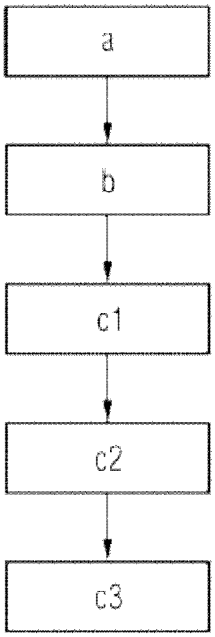

FIG 5

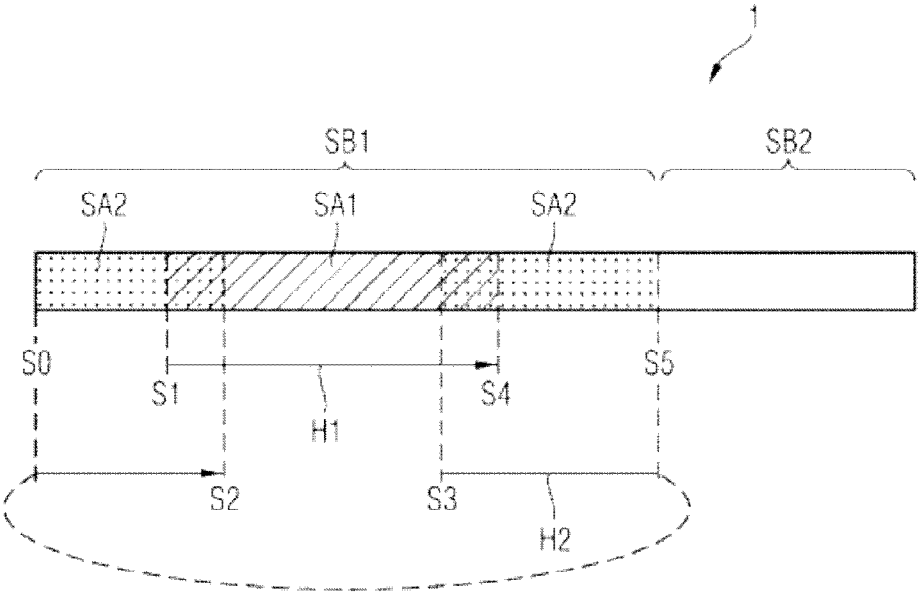
1
SB1
SB2
SA2
SA1
SA2
S0
S1
S4
S5
H1
S2
S3
H2

FIG 6

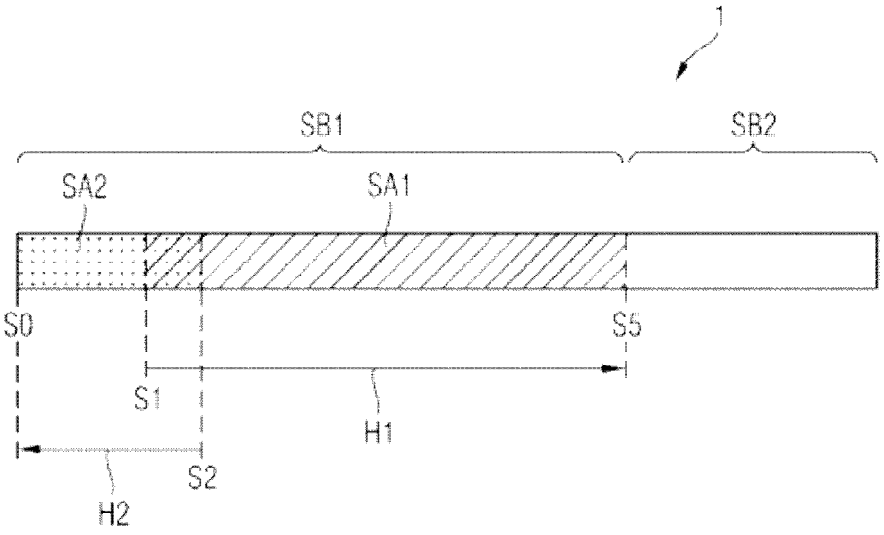
1
SB1
SB2
SA2
SA1
S0
S5
S1
H1
S2
H2

FIG 7

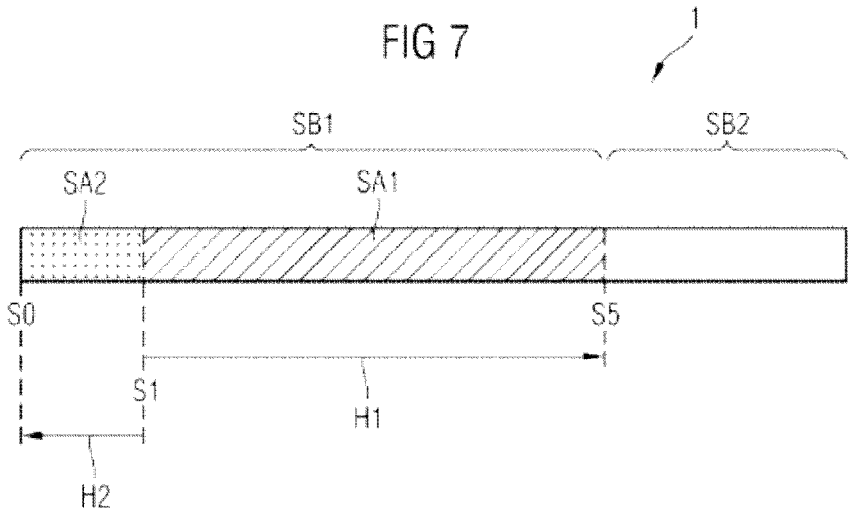

FIG 8

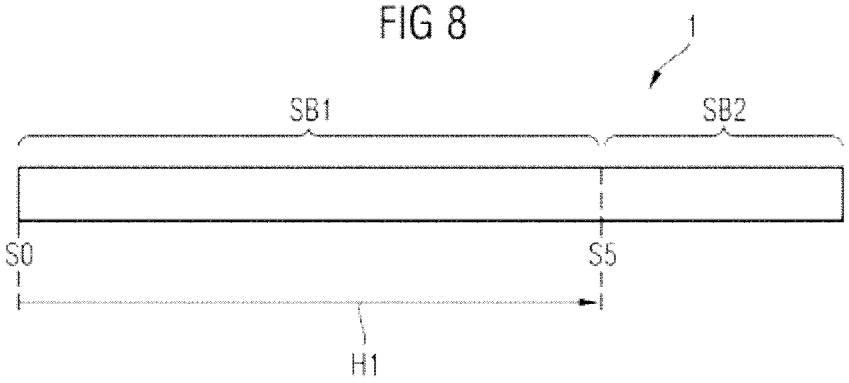

FIG 9