(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 752 468**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/53 (2013.01)
G06F 21/79 (2013.01)
G06F 12/14 (2006.01)
G06F 15/173 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.01.2008 PCT/IL2008/000070**

(87) Fecha y número de publicación internacional: **24.07.2008 WO08087640**

(96) Fecha de presentación y número de la solicitud europea: **16.01.2008 E 08702651 (4)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2019 EP 2104892**

(54) Título: **Archivo seguro**

(30) Prioridad:

16.01.2007 IL 18074807

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.04.2020

(73) Titular/es:

WATERFALL SECURITY SOLUTIONS LTD. (100.0%)
14 Hamelacha Street, Afek Industrial Park, Gav Yam Building, 1st Floor
Rosh HaAyin 4809133, IL

(72) Inventor/es:

FRENKEL, LIOR y
ZILBERSTEIN, AMIR

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Archivo seguro

La presente invención se refiere en general a sistemas informáticos, y específicamente a sistemas y métodos para comunicación y almacenamiento de datos.

En una red informática que maneja datos confidenciales, tal como datos en entornos militares o financieros, porciones de la red pueden estar conectadas por enlaces de datos unidireccionales. Por ejemplo, datos confidenciales a los que no se debe acceder desde sitios externos se pueden almacenar en un ordenador que está configurado para recibir datos a través de un enlace unidireccional y no tiene un enlace saliente físico sobre el cual se puedan transmitir datos al sitio externo.

Se pueden implementar enlaces unidireccionales, por ejemplo, utilizando los sistemas Waterfall™, que son fabricados por Gita Technologies, Ltd. (Rosh HaAyin, Israel). Las especificaciones de los sistemas Waterfall están disponibles en www.waterfall.co.il. El sistema Waterfall proporciona una conexión unidireccional física basada en la comunicación por fibra óptica, utilizando un protocolo de transferencia propietario subyacente. Cuando un ordenador transmisor está conectado por un sistema Waterfall (u otro enlace unidireccional) a un ordenador receptor, el ordenador receptor puede recibir datos del ordenador transmisor, pero no tiene medios para enviar comunicaciones de retorno al ordenador transmisor.

El documento DE-A-10/2005/025169 describe un dispositivo de comunicación para transmitir datos a un dispositivo asociado de comunicación, el dispositivo de comunicación incluye un transmisor para transmitir datos de transmisión al dispositivo asociado de comunicación y un medio receptor configurado para recibir datos recibidos.

El documento US-A-2005/0033990 describe un sistema y un método para comunicación de datos que garantiza que la comunicación de datos sensibles o confidenciales a través de un límite de red permanezca segura.

El documento US-5946399 describe una unidad de dispositivo que proporciona una interfaz a prueba de fallos entre una pluralidad de aplicaciones cliente y una tarjeta criptográfica.

El documento US-A-2005/0015624 describe una técnica utilizada para monitorizar el rendimiento, la seguridad y el estado de un sistema utilizado en una aplicación industrial.

El documento US-A-2006/0259431 describe un aparato de almacenamiento que comprende: una memoria; un procesador de encriptación, que está configurado para recibir y encriptar datos transmitidos desde uno o más ordenadores para almacenamiento en la memoria; y un enlace unidireccional, que acopla el procesador de encriptado a la memoria.

Los sistemas informáticos en red, tales como redes informáticas empresariales, a menudo utilizan almacenamiento centralizado para archivar datos, tal como registros de transacciones, eventos del sistema de tecnología de la información (TI) y copias de seguridad. Mantener la integridad de dichos archivos es crucial para garantizar que funciones como el análisis de registros, auditorías, análisis forenses y recuperación de datos después de fallos del sistema puedan llevarse a cabo. También es necesario evitar que terceros no autorizados accedan a datos sensibles archivados.

Las realizaciones de la presente invención que se describen a continuación abordan estas necesidades proporcionando un sistema de almacenamiento seguro, en el que los ordenadores en una red pueden escribir datos en una memoria solo a través de un procesador de encriptado. (El término "memoria" se usa ampliamente en la presente solicitud de patente y en las reivindicaciones para referirse a cualquier tipo de medio de almacenamiento de datos). El procesador encripta los datos utilizando una clave de encriptado, que normalmente no está disponible para los ordenadores de origen, y transmite los datos encriptados a través de un enlace unidireccional a la memoria. Por lo tanto, el procesador de encriptado puede escribir datos encriptados en la memoria, pero no leerlos.

Dado que todos los datos escritos en la memoria están encriptados, cualquier código de programa malicioso que un hacker pueda intentar introducir en el sistema de almacenamiento se codifica y, por lo tanto, se vuelve inofensivo hasta que se desencripta. El desencriptado puede tener lugar en un entorno controlado y "estéril", en el que se puede detectar y neutralizar el código malicioso antes de que afecte a los elementos vulnerables de la red. Por ejemplo, el contenido de almacenamiento puede duplicarse y luego desencriptarse en un entorno que está separado del sistema de almacenamiento, de modo que cualquier daño que pueda ser causado por un código malicioso no afectará los datos almacenados originales.

Se proporciona, de acuerdo con un aspecto de la presente invención, un aparato de almacenamiento, que comprende una memoria; un procesador de encriptación, que está configurado para recibir y encriptar datos transmitidos desde uno o más ordenadores para almacenamiento en la memoria; y un enlace unidireccional, que acopla el procesador de encriptado a la memoria; en el que el procesador de encriptado está conectado a uno o más ordenadores a través de una red informática; en el que la memoria comprende una memoria de archivo que archiva centralmente datos para una pluralidad de ordenadores; y en el que la memoria y el procesador de encriptado están

conectados directamente solo por el enlace unidireccional, y el enlace unidireccional está configurado físicamente para permitir la transmisión de datos entre el procesador de encriptado y la memoria solo en la dirección del procesador de encriptado a la memoria; caracterizado por que el aparato comprende además un procesador de monitorización conectado a la memoria de archivo, que tiene una conexión que permite la transmisión a la red, en el que el procesador de monitorización está preprogramado para monitorizar el estado de la memoria de archivo e informar sobre un estado de almacenamiento de datos de la memoria de archivo sin recibir comandos explícitos para hacerlo desde los ordenadores, y dicha conexión del procesador de monitorización a la red es a través de un segundo enlace unidireccional de tal manera que uno o más ordenadores no pueden enviar al procesador de monitorización datos o comandos que podrían hacer que el procesador de monitorización recupere y transmita a la red datos confidenciales desde la memoria de archivo.

En algunas realizaciones, el procesador de encriptado está configurado para encriptar los datos usando una clave de encriptado que no está disponible para uno o más ordenadores. En una realización, para cada transmisión de datos desde uno o más ordenadores, el procesador de encriptado está configurado para seleccionar la clave de encriptado entre una pluralidad de claves de encriptado posibles, y para transmitir una indicación de la clave de encriptado seleccionada a la memoria además de los datos encriptados. Por lo general, la memoria está configurada para almacenar los datos encriptados sin desencriptados antes del almacenamiento. En una realización divulgada, el procesador de encriptado está configurado para recibir los datos de uno o más ordenadores a través de una red privada y para aplicar una marca de tiempo a cada uno de al menos algunos elementos de los datos que se escriben en la memoria. En una realización divulgada, la memoria de archivo está configurada para recibir solo datos para archivar, encriptados por el procesador de encriptado. También se proporciona, de acuerdo con otro aspecto de la presente invención, un método para el almacenamiento de datos, que comprende: recibir datos transmitidos desde uno o más ordenadores para almacenarlos en una memoria; encriptar los datos recibidos utilizando un procesador de encriptado antes de pasar los datos a la memoria; transmitir los datos encriptados desde el procesador de encriptado a la memoria a través de un enlace unidireccional; y almacenar los datos encriptados en la memoria; en el que la memoria comprende una memoria de archivo que archiva centralmente datos para una pluralidad de ordenadores; y en el que la memoria y el procesador de encriptado están conectados directamente solo por el enlace unidireccional, que está configurado físicamente para permitir la transmisión de datos entre el procesador de encriptado y la memoria solo en la dirección del procesador de encriptado a la memoria; caracterizado por conectar un procesador de monitorización a la memoria de archivo, en el que el procesador de monitorización tiene una conexión que permite la transmisión a la red, en el que el procesador de monitorización está preprogramado para monitorizar el estado de la memoria de archivo e informar sobre un estado de almacenamiento de datos de la memoria de archivo sin recibir comandos explícitos para hacerlo desde los ordenadores, y dicha conexión del procesador de monitorización a la red es a través de un segundo enlace unidireccional, de tal manera que uno o más ordenadores no pueden enviar datos al procesador de monitorización datos o comandos que podrían hacer que el procesador de monitorización recupere y transmita a la red datos confidenciales desde la memoria de archivo.

La presente invención se entenderá más completamente a partir de la siguiente descripción detallada de las realizaciones de la misma, tomada junto con los dibujos en los que:

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema para la transmisión y el almacenamiento de datos, de acuerdo con una realización de la presente invención.

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema 20 para la transmisión y almacenamiento de datos, de acuerdo con una realización de la presente invención. Unos ordenadores 24 en un sistema 20 escriben datos en un archivo seguro 22 a través de una red informática 26. Estos datos pueden comprender, por ejemplo, registros de transacciones u otras entradas de registro de datos, actualizaciones de bases de datos, copias de seguridad de archivos o sustancialmente cualquier otro tipo de datos que puedan estar sujetos a archivo. La red 26 puede comprender sustancialmente cualquier tipo de red privada o pública. (En una realización alternativa, no mostrada en las figuras, el archivo 22 puede estar conectado por un solo enlace en lugar de a través de una red de múltiples ordenadores). Incluso cuando el acceso a la red 26 se controla cuidadosamente, sin embargo, usuarios no autorizados aún pueden obtener acceso a la red. Dichos usuarios pueden intentar introducir código de programa malicioso en el archivo 22 para leer los datos almacenados en el archivo o para corromper el contenido del archivo. Por ejemplo, un atacante que ha pirateado la red podría intentar borrar o alterar el registro del sistema de TI para cubrir sus huellas.

El archivo 22 comprende un procesador de encriptado 28, que escribe datos encriptados en una memoria 30 a través de un enlace unidireccional 32. Ordenadores en la red 26 pueden escribir datos en la memoria 30 solo a través del procesador de encriptado. Por lo tanto, cualquier código de programa malicioso que un usuario pueda intentar introducir en el archivo 22 será codificado y simplemente se almacenará en forma codificada en la memoria 30. En consecuencia, el usuario no podrá hacer que la unidad de control de la memoria 30 realice ninguna acción que no sea simplemente escribir datos en la memoria, ya que las instrucciones del programa enviadas por el usuario serán ininteligibles por el encriptado.

El procesador de encriptado 28 puede comprender hardware dedicado o un procesador informático de uso general, accionado por software, o una combinación de elementos de hardware y software. Para un encriptado rápido, así como una seguridad mejorada, por ejemplo, el procesador de encriptado puede comprender una o más

disposiciones de puerta con firmware adecuado y/o un circuito integrado específico de la aplicación (ASIC). Si se utiliza un procesador de ordenador de uso general, el software para llevar a cabo las funciones descritas en este documento puede descargarse al procesador a través de una red, o puede proporcionarse alternativamente en medios tangibles, tal como medios de memoria ópticos, magnéticos o electrónicos.

El procesador de encriptado puede usar cualquier tipo de encriptado adecuado que se conozca en la técnica, incluidos los métodos de encriptado asimétrico, como el algoritmo RSA (Rivest Shamir Adelman), y métodos simétricos, como algoritmos DES (Estándar de encriptado de datos) y AES (Estándar de encriptado avanzado), así como métodos más simples, que a veces se denominan "codificación". Al encriptar los datos entrantes, el procesador de encriptado generalmente usa claves diferentes en diferentes momentos, y puede usar una clave que no está disponible para ordenadores fuera del archivo 22. Debido al cambio de claves, los piratas informáticos no pueden usar una clave conocida para preparar sus transmisiones de manera que tengan un efecto malicioso después de la codificación. Por lo general, el procesador de encriptado elige la clave para cada elemento de datos o grupo de elementos de datos mediante un proceso pseudoaleatorio, ya sea mediante la selección de una lista preparada de antemano o mediante la generación pseudoaleatoria. (Alternativamente, la clave se puede elegir de manera determinista, siempre que no se conozca o no esté disponible para el ordenador que envía). La clave puede tener cualquier longitud adecuada, según el algoritmo de encriptado que se utilice.

El procesador de encriptado 28 transmite los datos encriptados a través del enlace unidireccional 32 a la memoria 30. Suponiendo que el procesador de encriptado usa diferentes claves de encriptado en diferentes momentos, el procesador de encriptado también puede transmitir a la memoria una indicación de la clave que se utilizará para descifrar cada transmisión. La indicación puede comprender la propia clave o un índice de una lista predeterminada de claves. Opcionalmente, el procesador de encriptado o el controlador de memoria (o ambos) pueden agregar una marca de tiempo a cada elemento de datos, para facilitar las funciones de auditoría. Alternativa o adicionalmente, la marca de tiempo puede ser aplicada por una unidad de hardware dedicada.

El enlace unidireccional 32 puede comprender un enlace en cascada, como se describe en la sección de antecedentes anterior, o cualquier otro tipo adecuado de enlace unidireccional que se conoce en la técnica. Como se señaló anteriormente, este enlace está típicamente configurado físicamente para permitir la transmisión de datos en una sola dirección, desde el procesador 28 a la memoria 30. Opcionalmente, el enlace 32 puede comprender dos o más enlaces unidireccionales conectados en serie, con un motor de seguridad de datos colocado entre los enlaces unidireccionales. Esta configuración de enlace, que proporciona seguridad mejorada, se describe, por ejemplo, en la solicitud de patente PCT PCT/IL2006/001499.

La memoria 30 puede comprender cualquier tipo adecuado de dispositivo de almacenamiento, tal como memoria magnética, óptica o electrónica, o una combinación de estos tipos de memoria. El dispositivo de almacenamiento puede comprender una unidad de control (no mostrada), como se conoce en la técnica, que recibe los datos encriptados a través del enlace 32 y escribe los datos en ubicaciones apropiadas en la memoria. Sin embargo, como se señaló anteriormente, la unidad de control no intenta descifrar los datos antes de escribir. Por el contrario, los datos normalmente se desencriptan y se "esterilizan" fuera de línea, según sea necesario, por un procesador de desencriptado separado (no mostrado). Para descifrar los datos, este procesador utiliza la clave que indicó el procesador de encriptado, como se explicó anteriormente. Después del desencriptado, el procesador de desencriptado esteriliza los datos para detectar y neutralizar cualquier contenido malicioso, como virus, gusanos y spyware, por ejemplo. Los métodos que se pueden utilizar para el encriptado y desencriptado de transmisiones de datos potencialmente maliciosos se describen con mayor detalle en la solicitud de patente PCT PCT/IL2007/001070.

Algunas aplicaciones de archivo pueden requerir que el archivo 22 devuelva un acuse de recibo u otro indicador de estado a uno o más ordenadores 24 después de recibir datos del ordenador. El procesador de encriptado 28 puede devolver los reconocimientos de datos simples. Un procesador de monitorización 34 supervisa el estado de la memoria 30 e informa sobre el estado del almacenamiento de datos. Típicamente, el procesador de monitorización está preprogramado para llevar a cabo estas funciones y realiza las funciones sin recibir comandos explícitos para hacerlo de las computadoras en la red 26. El procesador de monitorización 34 transporta los informes a través de un enlace unidireccional 36 a una interfaz de salida 38, que luego transmite los informes al ordenador apropiado 24 en la red 26. En esta configuración, los ordenadores 24 no pueden enviar entradas, como datos o comandos, al procesador de monitorización, y por lo tanto se les impide introducir código de programa malicioso que podría hacer que este procesador recupere y transmita datos confidenciales de la memoria 30 o altere El contenido de la memoria.

Aunque la figura 1 muestra una cierta configuración del sistema 20 y particularmente de los elementos en el archivo 22, los principios de la presente invención pueden aplicarse de manera similar en otros tipos de configuraciones físicas. Por ejemplo, los enlaces 32 y 36 se pueden combinar en un solo paquete con conexiones y conmutación apropiadas para garantizar que los datos fluyan por los enlaces solo en las direcciones y modos operativos que se describen anteriormente. Las realizaciones de la presente invención se han descrito anteriormente a modo de ejemplos con referencias a las figuras. Sin embargo, se apreciará que pueden hacerse variaciones y modificaciones a los ejemplos descritos dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Aparato de almacenamiento, que comprende:

una memoria (30);

un procesador de encriptado (28), que está configurado para recibir y encriptar datos transmitidos desde uno o más ordenadores (24) para almacenamiento en la memoria (30); y

un enlace unidireccional (32), que acopla el procesador de encriptado (28) a la memoria (30);

en el que el procesador de encriptación (28) está conectado a una o más computadoras (24) a través de una red de computadoras (26);

en el que la memoria (30) comprende una memoria de archivo (30) que archiva centralmente datos para una pluralidad de ordenadores (24); y

en el que la memoria (30) y el procesador de encriptado (28) están conectados directamente solo por el enlace unidireccional (32), y el enlace unidireccional (32) está configurado físicamente para permitir la transmisión de datos entre el procesador de encriptado (28) y la memoria (30) solo en la dirección del procesador de encriptado (28) a la memoria (30);

caracterizado por que el aparato comprende además un procesador de monitorización (34) conectado a la memoria de archivo (30), que tiene una conexión que permite la transmisión a la red (26), en el que el procesador de monitorización (34) está preprogramado para monitorizar el estado de la memoria de archivo (30) e informar sobre el estado de almacenamiento de datos de la memoria de archivo (30) a un ordenador apropiado (24) sin recibir comandos explícitos para hacerlo desde los ordenadores (24), y dicha conexión del procesador de monitorización (34) a la red (26) es a través de un segundo enlace unidireccional (36) y en el que uno o más ordenadores (24) no pueden enviar al procesador de monitorización (34) datos o comandos que podrían causar que el procesador de monitorización (34) recuperara y transmitiera a la red (26) datos confidenciales desde la memoria de archivo (30).

2. El aparato según la reivindicación 1, en el que el procesador de encriptado (28) está configurado para encriptar los datos usando una clave de encriptado que no está disponible para uno o más ordenadores (24).

3. El aparato según la reivindicación 2, en el que para cada transmisión de los datos desde uno o más ordenadores (24), estando el procesador de encriptado (28) configurado para seleccionar la clave de encriptado entre una pluralidad de posibles claves de encriptado, y para transmitir una indicación de la clave de encriptado seleccionada a la memoria (30) además de los datos encriptados.

4. El aparato según la reivindicación 1, en el que la memoria (30) está configurada para almacenar los datos encriptados sin desencriptado antes del almacenamiento.

5. El aparato según cualquiera de las reivindicaciones anteriores, en el que el procesador de encriptado (28) está configurado para recibir los datos de uno o más ordenadores (24) a través de una red privada (26).

6. El aparato según cualquiera de las reivindicaciones 1 a 5, en el que el procesador de encriptado (28) está configurado para aplicar una marca de tiempo a cada uno de al menos algunos elementos de los datos que se escriben en la memoria (30).

7. El aparato según cualquiera de las reivindicaciones anteriores, en el que la memoria de archivo (30) está configurada para recibir solo datos para archivar, encriptados por el procesador de encriptación (28).

8. Un método para almacenamiento de datos, que comprende:

recibir datos transmitidos desde uno o más ordenadores (24) para almacenamiento en una memoria (30);

encriptar los datos recibidos utilizando un procesador de encriptado (28) antes de pasar los datos a la memoria (30);

transportar los datos encriptados desde el procesador de encriptado (28) a la memoria (30) a través de un enlace unidireccional (32); y

almacenar los datos encriptados en la memoria (30);

en el que los datos se reciben desde uno o más ordenadores (24) a través de una red de ordenadores (26);

en el que la memoria (30) comprende una memoria de archivo (30) que archiva centralmente datos para una pluralidad de ordenadores (24); y

en el que la memoria (30) y el procesador de encriptado (28) están conectados directamente solo por el enlace unidireccional (32), que está configurado físicamente para permitir la transmisión de datos entre el procesador de

encriptado (28) y la memoria (30) solo en la dirección del procesador de encriptado (28) a la memoria (30);

caracterizado por conectar un procesador de monitorización (34) a la memoria de archivo (30), en el que el procesador de monitorización (34) tiene una conexión que permite la transmisión a la red (26), en el que el procesador de monitorización (34) está preprogramado para monitorizar el estado de la memoria de archivo (30) y para informar sobre el estado de almacenamiento de datos de la memoria de archivo (30) a un ordenador apropiado (24) sin recibir comandos explícitos para hacerlo desde los ordenadores (24), y dicha conexión del procesador de monitorización (34) a la red (26) es a través de un segundo enlace unidireccional (36) y en el que uno o más ordenadores (24) no pueden enviar al procesador de monitorización (34) datos o comandos que podrían hacer que el procesador de monitorización (34) recuperara y transmitiera a la red (26) datos confidenciales desde la memoria de archivo (30).

9. El método según la reivindicación 8, en el que el encriptado de los datos recibidos comprende encriptar los datos usando una clave de encriptado que no está disponible para uno o más ordenadores (24).

10. El método según la reivindicación 9, en el que el encriptado de los datos comprende, para cada transmisión de los datos desde uno o más ordenadores (24), seleccionar la clave de encriptado entre una pluralidad de posibles claves de encriptado, y transmitir una indicación de la clave de encriptado seleccionada de la memoria (30) además de los datos encriptados.

11. El método según cualquiera de las reivindicaciones 8-10, en el que almacenar los datos encriptados comprende escribir los datos encriptados en la memoria (30) sin desencriptar antes del almacenamiento.

12. El método según cualquiera de las reivindicaciones 8-11, en el que recibir los datos comprende recibir los datos desde uno o más ordenadores (24) a través de una red privada (26).

13. El método según cualquiera de las reivindicaciones 8-12, que comprende además aplicar una marca de tiempo a cada uno de al menos algunos elementos de los datos que se escriben en la memoria de archivo (30).

14. El método según cualquiera de las reivindicaciones 8-13, en el que los datos recibidos comprenden entradas de registro o copias de seguridad de archivos.

FIG. 1