(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 636 972**

(51) Int. CI.:

G06F 21/52 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.03.2012 E 12002063 (1)**

(97) Fecha y número de publicación de la concesión europea: **10.05.2017 EP 2503483**

(54) Título: **Sistema de comunicaciones con dispositivo de seguridad, así como método correspondiente**

(30) Prioridad:

25.03.2011 DE 102011015123

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.10.2017

(73) Titular/es:

G DATA SOFTWARE AG (100.0%)
Königsallee 178 b
44799 Bochum, DE

(72) Inventor/es:

BÜSCHER, ARMIN y
SIEBERT, THOMAS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema de comunicaciones con dispositivo de seguridad, así como método correspondiente

La presente invención hace referencia a un sistema de comunicaciones con un dispositivo de seguridad, a un dispositivo de seguridad, así como a un método correspondiente. Los sistemas de comunicaciones, en particular los sistemas de comunicaciones asistidos por procesadores específicos o por ordenadores, utilizan con frecuencia aplicaciones de navegadores web para comunicarse con otros sistemas de comunicaciones o unidades de procesamiento, en particular para intercambiar datos.

Las aplicaciones de navegadores web utilizadas emplean bibliotecas de sistema en las cuales se encuentra almacenada información sobre las interfaces del sistema. Con frecuencia, esas interfaces del sistema son manipuladas, por ejemplo a través de ataques con un objetivo determinado, utilizando un software malicioso. Los ataques de ese tipo pueden dañar el sistema de comunicaciones, afectándolo en particular en cuanto a la seguridad operativa o bloqueando de forma parcial o completa el sistema de comunicaciones. El software malicioso puede utilizarse también para espiar datos de funcionamiento del sistema de comunicaciones. Por el estado del arte son conocidos métodos para detectar rootkits (encubridores) y malware (software dañinos) a través de la comparación del estado real de bibliotecas de sistema con un estado objetivo, véase por ejemplo Joanna Rutkowska: "System Virginity Verifier", Hack In The Box Security Conference, 29 de septiembre de 2005 (2005-09-29) http://www.bandwidthco.com/whitepapers/compforensics/malware/rk/. Estos métodos, sin embargo, se refieren a la comparación de una biblioteca de sistema completa y no abordan sus propiedades particulares.

Por lo tanto, el objeto de la presente invención consiste en perfeccionar de manera ventajosa un sistema de comunicaciones con un dispositivo de seguridad, un dispositivo de seguridad, así como un método correspondiente, en particular de manera que daños del sistema de comunicaciones puedan ser detectados de forma sencilla, rápida y fiable.

De acuerdo con la invención, el objeto mencionado se alcanzará a través de un sistema de comunicaciones con las características de la reivindicación 1. Conforme a ello, se prevé un sistema de comunicaciones, con al menos un medio de comunicaciones, mediante el cual el sistema de comunicaciones puede ser conectado con al menos otra unidad de procesamiento y/o con otro sistema de comunicaciones, con al menos un primer medio de memoria, con al menos un segundo medio de memoria y con al menos un dispositivo de seguridad, donde en el primer y en el segundo medio de memoria está almacenada información idéntica, y donde mediante una comparación de esa información mediante el dispositivo de seguridad puede determinarse un daño del sistema de comunicaciones, donde el primer medio de memoria es una primera memoria con una biblioteca de sistema, en donde como información se encuentra almacenado al menos un directorio de las interfaces del sistema proporcionadas a través de la biblioteca de sistema y donde el segundo medio de memoria es una segunda memoria con una copia de la biblioteca de sistema de la primera memoria, en donde como información está almacenado al menos un directorio de las interfaces del sistema proporcionadas a través de la biblioteca de sistema, caracterizado porque se proporciona un tercer medio de memoria, porque interfaces del sistema individuales dañadas pueden identificarse a través de al menos una propiedad de las interfaces del sistema, la cual es independiente del sistema de comunicaciones y/o de las propiedades del sistema de comunicaciones, donde al menos una propiedad puede almacenarse o se encuentra almacenada en el tercer medio de memoria como información, y donde con esa información, mediante el dispositivo de seguridad, puede formarse una suma de comprobación, y porque mediante la suma de comprobación puede determinarse la clase de daño, en donde la suma de comprobación, mediante el dispositivo de seguridad, puede ser comparada con sumas de comprobación ya conocidas, almacenadas en el dispositivo de seguridad.

A través de un sistema de comunicaciones de esa clase, de manera ventajosa, puede solucionarse el problema técnico de la evasión de un daño del sistema de comunicaciones, a saber, a través del medio técnico de un dispositivo de seguridad, mediante el cual se posibilita una comparación de información correspondiente, en particular información almacenada de forma redundante, posibilitando gracias a ello una detección de un daño, de forma sencilla y fiable. Una modificación y/o manipulación de la información permite una detección segura y fiable de un daño del sistema de comunicaciones.

La posibilidad de determinar un daño mediante el dispositivo de seguridad se da también en principio cuando el sistema de comunicaciones no se encuentra conectado a otro sistema de comunicaciones y/o no se encuentra conectado sólo de forma provisional con al menos otra unidad de procesamiento y/o con otro sistema de comunicaciones. Una conexión permanente del sistema de comunicaciones con al menos otra unidad de procesamiento y/u otro sistema de comunicaciones no es necesaria de forma forzosa.

El término "daño" puede entenderse e interpretarse de forma amplia. Por ejemplo, un daño puede consistir en el hecho de que un software malicioso fue instalado en el sistema de comunicaciones y/o en el hecho de que una o varias funciones del sistema de comunicaciones han sido perjudicadas. Un perjuicio de esa clase puede consistir

también en el hecho de que información puede ser leída de forma no autorizada, por ejemplo debido a la instalación de un software malicioso.

De este modo, mediante el dispositivo de seguridad puede ser detectado un daño del sistema de comunicaciones cuando en el resultado de la comparación de la información se observa que la misma no coincide. En tanto el resultado de la comparación indique que existe una coincidencia de la información, de manera preferente, mediante el dispositivo de seguridad no puede determinarse ningún daño. Preferentemente, se puede mostrar al usuario del sistema de comunicaciones el estado de funcionamiento actual, por ejemplo en el caso de que no se encuentre presente un daño, en forma de un mensaje y/o de una señal que pueden ser insertados, y en el caso de un daño, en forma de un mensaje de advertencia.

Una detección segura y fiable de un daño del sistema de comunicaciones, de manera ventajosa, permite a su vez reparar el daño por ejemplo de forma inmediata. Por ejemplo, lo mencionado puede suceder de manera que, en el caso de un daño a través de una instalación no deseada de un software malicioso, esto pueda ser detectado automáticamente mediante el dispositivo de seguridad, impidiéndose automáticamente la ejecución del software malicioso, donde por ejemplo se realiza o puede realizarse una eliminación del software malicioso.

El sistema de comunicaciones puede ser una unidad de procesamiento y/o puede comprender una unidad de procesamiento. A modo de ejemplo, una unidad de procesamiento de esa clase puede ser un ordenador, un ordenador portátil, etc., el cual sin embargo también puede estar incorporado en un sistema de comunicaciones superordinado.

El medio de comunicaciones puede comprender una aplicación de navegador web o puede estar realizado como una aplicación de navegador web. La aplicación de navegador web presenta generalmente bibliotecas de sistema que presentan información sobre el funcionamiento del sistema de comunicaciones. Por ejemplo, la aplicación de navegador web puede ser un navegador web tradicional, como Microsoft Internet Explorer, Mozilla Firefox y/o Google Chrome.

Es posible además que el medio de comunicaciones presente otros medios de intercambio de datos correspondientes, como interfaces de transmisión de datos. Las interfaces de transmisión de datos de esa clase pueden posibilitar un intercambio de datos mediante cables y/o de forma inalámbrica.

El dispositivo de seguridad puede ser una ampliación del medio de comunicaciones. Por ejemplo, de manera ventajosa, puede preverse que el dispositivo de seguridad esté realizado como una ampliación del navegador web.

La información almacenada en las memorias puede ser una información referida a las características del sistema de comunicaciones o puede contener otra información.

Es posible que el primer medio de memoria sea una memoria de trabajo y que el segundo medio de memoria sea una memoria de datos. Por ejemplo, la memoria de trabajo puede ser una memoria RAM y la memoria de datos puede ser una memoria en un disco duro. En ese caso puede tratarse de un disco duro local. No obstante, también es posible que el segundo medio de memoria sea una memoria en una memoria no local. En particular puede preverse que un almacenamiento de la información en la primera memoria tenga lugar al poner en funcionamiento el sistema de comunicaciones y que la información se encuentre presente siempre en la memoria del disco duro.

Es posible también que el medio de memoria, la memoria RAM y/o la memoria del disco duro sea o sean sólo una parte del espacio de almacenamiento en un elemento de memoria RAM o en un disco duro del sistema de comunicaciones que se encuentra a disposición del sistema de comunicaciones o que pertenece al sistema de comunicaciones.

Puede preverse además que el primer medio de memoria sea una primera memoria con una biblioteca de sistema, en donde como información se encuentra almacenado al menos un directorio de las interfaces del sistema proporcionadas a través de la biblioteca de sistema y que el segundo medio de memoria sea una segunda memoria con una copia de la biblioteca de sistema de la primera memoria, en donde como información esté almacenado al menos un directorio de las interfaces del sistema proporcionadas a través de la biblioteca de sistema.

Es posible además que un daño de la interfaz del sistema, en particular una manipulación de la interfaz del sistema, pueda ser detectada mediante el dispositivo de seguridad, a través de al menos una comparación parcial de la primera memoria con la segunda memoria. De este modo, mediante el dispositivo de seguridad puede tener lugar un monitoreo de las bibliotecas de sistema utilizadas en el navegador web, en particular una protección frente a la manipulación de las bibliotecas de sistema utilizadas para la comunicación, así como de las interfaces del sistema almacenadas en las bibliotecas de sistema. Por lo tanto, lo mencionado se considera en especial ventajoso porque las interfaces del sistema de esas bibliotecas con frecuencia son manipuladas por software maliciosos o mediante la

utilización de software maliciosos, para interceptar entradas del usuario, como por ejemplo nombres de usuario y contraseñas en formularios de páginas web antes del encriptado a través del sistema de comunicaciones.

Puede preverse además que las interfaces del sistema presenten puntos de entrada y que la información relativa a los puntos de entrada pueda ser procesada de forma independiente mediante el dispositivo de seguridad y pueda ser comparada mediante los puntos de entrada procesados por el sistema de comunicaciones, donde en particular un daño puede ser determinado o se determina mediante el dispositivo de seguridad cuando a través del dispositivo de seguridad se determina una desviación de los puntos de entrada procesados a través del dispositivo de seguridad con los puntos de entrada procesados a través del sistema de comunicaciones. Sin embargo, en principio también es posible que en lugar de puntos de entrada se empleen otras estructuras de datos comparables o predefinidas de forma adecuada. La comparación y la detección de desviaciones de esas estructuras de datos y, con ello, de daños del sistema de comunicaciones, pueden ser detectadas de este modo en correspondencia con el procedimiento antes mencionado, a través de la comparación de los puntos de entrada.

Es posible también que se proporcione un tercer medio de memoria y que una interfaz del sistema dañada pueda identificarse a través de al menos una propiedad de las interfaces del sistema, la cual es independiente del sistema de comunicaciones y/o de las propiedades del sistema de comunicaciones, donde al menos una propiedad puede almacenarse o se encuentra almacenada en el tercer medio de memoria como información, y donde con esa información, mediante el dispositivo de seguridad, puede formarse una suma de comprobación. De manera ventajosa, al menos una propiedad puede ser almacenada en una estructura de datos en un orden determinado, por ejemplo en orden alfabético. A continuación, mediante esa estructura de datos, puede formarse una suma de comprobación (valor hash). Esa propiedad de la interfaz del sistema puede ser por ejemplo el nombre de la interfaz del sistema, el cual, de manera ventajosa, siempre es el mismo, independientemente del sistema. De este modo, por tanto, una interfaz manipulada puede ser identificada a través de propiedades como por ejemplo el nombre de la interfaz del sistema, las cuales son independientes del sistema en concreto. De manera ventajosa, esto permite poder efectuar una detección mediante el dispositivo de seguridad, independientemente del sistema. También es posible que el tercer medio de memoria sea sólo una parte del espacio de almacenamiento en un elemento de memoria que se encuentra a disposición del sistema de comunicaciones o que pertenece al sistema de comunicaciones, donde no es necesario forzosamente que el tercer elemento de memoria se trate de un espacio de almacenamiento local. En una ejecución ventajosa, el tercer medio de memoria puede también formar parte del segundo medio de memoria o puede ser idéntico al segundo medio de memoria.

Puede preverse además que mediante la suma de comprobación pueda determinarse el tipo de daño, donde la suma de comprobación, mediante el dispositivo de seguridad, puede ser comparada con sumas de comprobación ya conocidas, almacenadas en el dispositivo de seguridad. Sin embargo, en principio también es posible no almacenar la suma de comprobación en el dispositivo de seguridad, sino en un medio de memoria separado.

[0022] En particular, a través del sistema de comunicaciones resulta la ventaja de que con el dispositivo de seguridad, así como mediante el dispositivo de seguridad a través del sistema de comunicaciones, durante el funcionamiento del sistema de comunicaciones puede detectarse el daño causado por ejemplo por un software malicioso. En particular, los daños mencionados pueden tratarse de manipulaciones de bibliotecas de sistema del medio de comunicaciones, en particular de la aplicación del navegador web. A través del dispositivo de seguridad puede cancelarse el daño, en particular la manipulación, durante el período de la ejecución, y el usuario del sistema de comunicaciones puede ser avisado de forma correspondiente. Además, es posible que el usuario, mediante el dispositivo de seguridad, en el caso de una identificación exitosa del software malicioso, mediante una suma de comprobación, en tanto se encuentren a disposición, se remita a herramientas proporcionadas para la eliminación permanente del software malicioso o de los productos generados por el software malicioso, desde el sistema de comunicaciones.

Además, la presente invención hace referencia a un dispositivo de seguridad con las características de la reivindicación 8. Conforme a ello se prevé que un dispositivo de seguridad esté realizado con las características del dispositivo de seguridad según una de las reivindicaciones precedentes.

El dispositivo de seguridad puede tratarse de un elemento de memoria en el cual están almacenadas en particular las características de funcionamiento del dispositivo de seguridad. Puede preverse además que el dispositivo de seguridad sea un programa de producto informático. Preferentemente, el dispositivo de seguridad es un dispositivo de seguridad que se proporciona para ser usado en un sistema de comunicaciones según una de las reivindicaciones 1 a 7.

Además, la presente invención hace referencia a un método para determinar un daño de un sistema de comunicaciones. De acuerdo con ello se prevé un método para determinar un daño de un sistema de comunicaciones con al menos un medio de comunicaciones, mediante el cual el sistema de comunicaciones puede ser conectado con al menos otra unidad de procesamiento y/o con otro sistema de comunicaciones, con al menos un primer medio de memoria, con al menos un segundo medio de memoria y con al menos un dispositivo de

seguridad, donde en el primer y en el segundo medio de memoria está almacenada información idéntica, y donde mediante una comparación de esa información mediante el dispositivo de seguridad puede determinarse un daño del sistema de comunicaciones.

Asimismo, de manera ventajosa puede preverse que el método sea ejecutado con un sistema de comunicaciones según una de las reivindicaciones 1 a 7.

Otras particularidades y ventajas de la invención se explican en detalle a través de un ejemplo de ejecución que se describe a continuación.

Una forma de ejecución ventajosa de un sistema de comunicaciones de acuerdo con la invención, en una ejecución sencilla, puede ser por ejemplo un ordenador privado, como un PC, una tableta, un ordenador portátil o una Notebook, los cuales están conectados o pueden conectarse a Internet. El medio de comunicaciones del sistema de comunicaciones comprende una aplicación de navegador web, así como una o varias interfaces, mediante las cuales el sistema de comunicaciones puede conectarse a Internet y/o a otra red.

En principio también es posible que la presente invención pueda ejecutarse con relación a un teléfono inteligente, a una consola de juegos o a un aparato comparable. Preferentemente, en este caso, el sistema de comunicaciones es el teléfono inteligente, la consola de juegos o el aparato comparable.

El dispositivo de seguridad está realizado como un objeto de ampliación de la aplicación de navegador web y se encuentra almacenado de forma permanente o instalado en una memoria del sistema de comunicaciones.

Un software malicioso manipula con frecuencia los puntos de entrada hacia las interfaces del sistema (APIs) proporcionadas a través del sistema operativo. El objeto del presente concepto consiste en detectar las manipulaciones de esa clase y en identificar el software malicioso mediante el tipo de manipulaciones.

Una biblioteca de programa es cargada en un proceso-objetivo que debe ser analizado y verifica si han sido modificados puntos de entrada en las interfaces del sistema de determinadas bibliotecas del sistema. Debe prestarse atención a las siguientes modificaciones:

(1) Las bibliotecas de sistema contienen un directorio de las interfaces del sistema proporcionadas. Dicho directorio puede ser manipulado por virus, después de que la biblioteca de sistema fue cargada en la memoria. Las manipulaciones de ese tipo pueden detectarse comparando el directorio en la memoria con el directorio en la copia del disco duro de la biblioteca de sistema.

(2) Las manipulaciones del código de las interfaces del sistema ("Inline-Hooking") son detectadas a través de la comparación con los fragmentos del código correspondientes de la copia del disco duro de la biblioteca del sistema.

(3) Otras manipulaciones (por ejemplo a través del procedimiento de carga del sistema operativo) son detectadas comparando los puntos de entrada de las interfaces del sistema, procesados a través del sistema operativo, con puntos de entrada procesados de forma independiente.

Las interfaces del sistema individuales manipuladas son identificadas a través de propiedades que son independientes del sistema en concreto (por ejemplo el nombre de las interfaces). Dichas propiedades son almacenadas en una estructura de datos, en un orden determinado (por ejemplo alfabéticamente). A continuación, mediante esa estructura de datos, se forma una suma de comprobación (valor hash).

La suma de comprobación producida puede utilizarse para identificar el virus, donde la suma de comprobación es comparada con sumas de comprobación ya conocidas.

En una variante ventajosa, el dispositivo de seguridad puede ser una ampliación de la aplicación de navegador web Microsoft Internet Explorer en el sistema operativo Microsoft Windows. Una implementación como ampliación para navegadores web de otros productores, como por ejemplo Mozilla Firefox y Google Chrome, es posible con una estructura muy similar en cuanto al aspecto técnico.

El objetivo de la ampliación de navegador web es el monitoreo de las bibliotecas de sistema utilizadas en el navegador web, en particular la protección frente a manipulaciones de las bibliotecas utilizadas para la comunicación. Lo mencionado es necesario, ya que las interfaces del sistema de las bibliotecas de esa clase con frecuencia son manipuladas por software maliciosos, para interceptar entradas del usuario, como por ejemplo nombres de usuario y contraseñas en formularios de páginas web, antes del encriptado a través del sistema.

La ampliación detecta las manipulaciones en bibliotecas del sistema en el navegador web realizadas durante el funcionamiento por software maliciosos y las cancela durante el período de ejecución, avisa al usuario y, en el caso de una identificación exitosa del software malicioso, mediante una suma de comprobación, en tanto se encuentren a disposición, lo remite a herramientas proporcionadas para la eliminación permanente de los archivos maliciosos correspondientes, desde el sistema.

REIVINDICACIONES

1. Sistema de comunicaciones con al menos un medio de comunicaciones, mediante el cual el sistema de comunicaciones puede ser conectado con al menos otra unidad de procesamiento y/o con otro sistema de comunicaciones, con al menos un primer medio de memoria, con al menos un segundo medio de memoria y con al menos un dispositivo de seguridad, donde en el primer y en el segundo medio de memoria está almacenada información idéntica, y donde mediante una comparación de esa información mediante el dispositivo de seguridad puede determinarse un daño del sistema de comunicaciones, donde el primer medio de memoria es una primera memoria con una biblioteca de sistema, en donde como información se encuentra almacenado al menos un directorio de las interfaces del sistema proporcionadas a través de la biblioteca de sistema y donde el segundo medio de memoria es una segunda memoria con una copia de la biblioteca de sistema de la primera memoria, en donde como información está almacenado al menos un directorio de las interfaces del sistema proporcionadas a través de la biblioteca de sistema, caracterizado porque se proporciona un tercer medio de memoria, porque interfaces del sistema individuales dañadas pueden identificarse a través de al menos una propiedad de las interfaces del sistema, la cual es independiente del sistema de comunicaciones y/o de las propiedades del sistema de comunicaciones, donde al menos una propiedad puede almacenarse o se encuentra almacenada en el tercer medio de memoria como información, y donde con esa información, mediante el dispositivo de seguridad, puede formarse una suma de comprobación, y porque mediante la suma de comprobación puede determinarse la clase de daño, en donde la suma de comprobación, mediante el dispositivo de seguridad, puede ser comparada con sumas de comprobación ya conocidas, almacenadas en el dispositivo de seguridad.

2. Sistema de comunicaciones según la reivindicación 1, caracterizado porque el primer medio de memoria es una memoria de trabajo y el segundo medio de memoria es una memoria de datos.

3. Sistema de comunicaciones según la reivindicación 1, caracterizado porque un daño de la interfaz del sistema, en particular una manipulación de la interfaz del sistema, puede ser detectada mediante el dispositivo de seguridad, a través de al menos una comparación parcial de la primera memoria con la segunda memoria.

4. Sistema de comunicaciones según la reivindicación 1 ó 3, caracterizado porque las interfaces del sistema presentan puntos de entrada y porque la información relativa a los puntos de entrada puede ser procesada de forma independiente mediante el dispositivo de seguridad y puede ser comparada mediante los puntos de entrada procesados por el sistema de comunicaciones, donde en particular un daño puede ser determinado o se determina mediante el dispositivo de seguridad cuando a través del dispositivo de seguridad se determina una desviación de los puntos de entrada procesados a través del dispositivo de seguridad con los puntos de entrada procesados a través del sistema de comunicaciones.

5. Dispositivo de seguridad con las características del dispositivo de seguridad según una de las reivindicaciones precedentes.

6. Método para determinar un daño de un sistema de comunicaciones con al menos un medio de comunicaciones, mediante el cual el sistema de comunicaciones puede ser conectado con al menos otra unidad de procesamiento y/o con otro sistema de comunicaciones, con al menos un primer medio de memoria, con al menos un segundo medio de memoria y con al menos un dispositivo de seguridad, donde en el primer y en el segundo medio de memoria está almacenada información idéntica, y donde mediante una comparación de esa información mediante el dispositivo de seguridad puede determinarse un daño del sistema de comunicaciones, donde el método se realiza con un sistema de comunicaciones según una de las reivindicaciones 1 a 5.