(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 362**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06100494 .1**
(96) Fecha de presentación : **18.01.2006**
(97) Número de publicación de la solicitud: **1686758**
(97) Fecha de publicación de la solicitud: **02.08.2006**

(54) Título: **Sistema asegurado de interconexión unidireccional.**

(30) Prioridad: **28.01.2005 FR 05 00893**

(45) Fecha de publicación de la mención BOPI:
04.07.2011

(45) Fecha de la publicación del folleto de la patente:
04.07.2011

(73) Titular/es: **THALES**
45 rue de Villiers
92200 Neuilly sur Seine, FR

(72) Inventor/es: **Alcouffe, Fabien**

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Sistema asegurado de interconexión unidireccional

El objeto de la presente invención se refiere a un sistema de interconexión unidireccional, por ejemplo desde un sistema A con un nivel de seguridad bajo a un sistema B con un nivel de seguridad alto. El sistema garantiza de este modo la no-transmisión (voluntaria o no) de información física y/o lógica desde B hacia A.

De manera más general, la invención se aplica en cualquier sistema que comprenda varios sistemas con niveles de seguridad diferentes o iguales, en los que se desea restringir la transmisión de información en un sentido, por ejemplo, desde un sistema de seguridad N-1 hacia un sistema con un nivel de seguridad N.

Esta se utiliza, por ejemplo, para la interconexión de dos entidades A y B, como ordenadores, redes, diferentes capas de redes, etc.

En el campo de intercambios de información unidireccionales entre sistemas, es necesario permitir la transferencia de información desde un sistema A hacia un sistema B, por ejemplo, garantizando al mismo tiempo la no transmisión voluntaria o inesperada de información desde un sistema B que tiene un nivel de seguridad alto hacia un sistema A que tiene un nivel de seguridad bajo, en comparación con el nivel de seguridad del sistema A.

Actualmente, el control de estos intercambios se puede realizar en el campo de las redes de protocolos de Internet IP mediante un cortafuegos. No obstante, existen numerosas amenazas ligadas a la utilización de una solución de este tipo. Se pueden citar: el secuestro del software del cortafuegos, la toma de control y la modificación de las criterios de filtrado del cortafuegos, el secuestro del material del cortafuegos, los errores de configuración de los criterios de filtrado, los errores de codificación, la explotación de los defectos del software, la explotación de las señales electromagnéticas por radiación o conducción.

La patente US-A-6 108 787 divulga un sistema que permite controlar los flujos de información que circulan entre dos sistemas informáticos. Para ello, el sistema utiliza un diodo que recibe la información desde una primera red y la transmite hacia una segunda red. El control de circulación del flujo se hace por medio de un conmutador que tiene dos estados.

El documento US 2002/112181 divulga un sistema de acceso asegurado multinivel. El sistema consta de una unidad de conmutación.

La invención se refiere a un sistema securizado de interconexión unidireccional de acuerdo con la reivindicaión1.

El medio de conexión es, por ejemplo, una fibra óptica equipada con uno o varios aisladores ópticos.

El aislador puede ser un aislador pasivo con un nivel de atenuación constante.

El sistema de acuerdo con la invención presenta en particular las siguientes ventajas:

- Permite transferir informaciones de forma unidireccional desde el sistema con el nivel más bajo A hacia el sistema con el nivel más alto B y prohíbe, en funcionamiento normal, la transferencia lógica y/o física de informaciones desde B hacia A, ya sea esa transferencia voluntaria o no (debido al secuestro del sistema B, por ejemplo);
- La solución que se propone es pasiva y no necesita, en funcionamiento normal, una fuente de energía, aplica unos materiales no conductores y tolerantes a las radiaciones electromagnéticas;
- La solución que se propone es independiente del tipo de protocolo de comunicación que se utilice para la transferencia desde A hacia B (IP (protocolo de Internet), RS232, ARINC, etc.);
- Esta ofrece simplicidad y facilidad de aplicación, un muy elevado nivel de seguridad, una ausencia de sensibilidad a los ataques informáticos y a los fallos de diseño, de fabricación o de codificación.

Se mostrarán más claramente otras características y ventajas de la presente invención con la lectura de la descripción que sigue de un ejemplo de realización dado a título ilustrativo no excluyente, a la que se anexan unas figuras que representan:

- La figura 1, un representación sinóptica del sistema de acuerdo con la invención;
- La figura 2, un ejemplo de diseño del sistema de la figura 1;
- La figura 3, un ejemplo de aplicación para unos intercambios unidireccionales entre dos redes con diferentes sensibilidades;
- La figura 4, una variante que comprende varios sistemas que comunican con un sistema con un nivel de seguridad elevado;
- La figura 5, una variante de realización para unos intercambios bidireccionales con separación de los flujos entrantes y salientes.

La solución se basa en particular en la utilización de un hilo de fibra óptica y de un aislador óptico.

Se puede utilizar cualquier otro medio que presente unas características funcionalmente idénticas o prácticamente idénticas a la fibra óptica y al aislador óptico.

La figura 1 representa un sistema A, por ejemplo un ordenador equipado con un emisor óptico 1, y un sistema B, otro ordenador equipado con un receptor óptico 2. El nivel de seguridad del sistema A es un nivel bajo con respecto al alto nivel de seguridad asociado al sistema B.

La figura 2 representa un ejemplo de sistema securizado de interconexión unidireccional de acuerdo con la invención, en el que los sistemas A y B se conectan por medio de una fibra óptica 3 equipada con un aislador óptico 4.

Las características del aislador se seleccionan, por ejemplo, para respetar la compatibilidad con el ordenador A y el ordenador B.

La luz que emite el sistema A con un nivel bajo de seguridad se transmite por la fibra óptica 3. El aislador 4 está adaptado para que, en funcionamiento normal, ninguna información emitida por el sistema B, tras un error de conexión o debido al secuestro del sistema B con un nivel de seguridad alto, pueda ser explotada por el sistema A. El aislador óptico 4 permite en particular la transmisión unidireccional de información entre dos redes.

Siendo la solución pasiva en funcionamiento normal, no necesita ninguna alimentación eléctrica ni otra fuente de energía.

La fibra óptica y el aislador óptico utilizados son eléctrica y electromagnéticamente no conductores y no radiantes.

Una eventual avería en el funcionamiento implica la pérdida de la función de transmisión desde A hacia B.

La emisión de fuerte intensidad de luz por el sistema B lleva, por ejemplo, a la destrucción del aislador, lo que bloquea cualquier transmisión.

El aislamiento que se consigue con estos aisladores comerciales es del orden de 40 dB y se puede aumentar mediante la instalación en serie de varios aisladores. La solución se puede realizar con unos aisladores totalmente pasivos con un nivel de atenuación fijo o con unos aisladores con un nivel de atenuación ajustable, en este último caso la solución necesita una alimentación eléctrica.

El sistema de acuerdo con la invención se utiliza, por ejemplo, en las siguientes aplicaciones: la transferencia de archivos, de mensajes, la duplicación de bases de datos, la reactivación de alarmas centralizada, el acceso concomitante a unas informaciones procedentes de diferentes sistemas cerrados, etc.

El ejemplo que se da en la figura 2 corresponde a una implementación en el campo de las tarjetas ópticas de red. Cada uno de los sistemas A y B están equipados con un tarjeta óptica de red, 5, 6. Estas últimas proponen por lo general una detección automática de rotura de las fibras ópticas en el conector Rx. Las tarjetas detectan la pérdida de recepción de la señal óptica y emiten una alarma. La parte Rx receptora de la tarjeta acciona una alarma si deja de recibir una información procedente del Tx de la tarjeta emisora. Esto permite detectar un problema en la cadena de transmisión emisor, fibra, receptor (la señal puede ser una onda portadora constante o un mensaje emitido a intervalos regulares). En el ejemplo que se da en la figura 2, una parte Si de la señal emitida se desvía para reinyectarla en la misma tarjeta 5, esto vuelve al sistema compatible con todas las categorías de tarjeta y permite verificar que el emisor funciona de forma correcta.

La solución propuesta utiliza una parte Si de la señal emitida T_1 por el sistema A y se la devuelve. El sistema A va por lo tanto a detectar la señal luminosa Si que le llega como si la hubiera emitido el sistema B. El resto de la señal S_2 pasa a través del aislador 4 antes de transmitirse al sistema B. Este montaje presenta en particular como ventaja que detecta una avería de emisión del sistema A, recibiendo este último una parte de la luz.

La figura 3 esquematiza otro ejemplo de aplicación en el campo de los intercambios unidireccionales entre dos redes con diferentes sensibilidades. La solución garantiza que ninguna información de la red más sensible, sistema B, sea accesible desde la red menos sensible, sistema A. Una configuración de este tipo se aplica, por ejemplo, para la copia de seguridad de información, la duplicación de bases de datos, las secuencias de video.

La figura 4 representa otra variante de realización aplicada en el campo de la concentración en un sistema B de información procedente de diferentes sistemas An, cada uno de estos sistemas presentando un nivel de seguridad más bajo que el nivel de seguridad del sistema B.

Para ello, cada fibra óptica Fi que garantiza la conexión entre un sistema Ai y el sistema B está equipada con un aislador óptico Ii que presenta unas características funcionales idénticas o prácticamente idénticas a las que se han descrito en la figura 2.

La solución garantiza que ninguna información del sistema B sea accesible desde los sistemas An y entre los diferentes sistemas An entre sí. La invención se aplica en particular para la copia de seguridad de información, la concentración de la información de conexión (o de forma abreviada log), la fusión de datos.

La figura 5 esquematiza una solución que puede aplicarse en el campo de intercambios bidireccionales con separación de los flujos de entrada y de salida.

Esta solución permite transmitir información desde B hacia A, por ejemplo, un corte funcional tras la transmisión de una información desde A hacia B por medio de un canal C_1 equipado con un aislador óptico como ya se ha descrito con anterioridad. La transmisión desde B hacia A se hace por medio de un canal diferente del de la transmisión desde A hacia B. Este otro canal unidireccional C_2 hace circular la información desde B hacia un dispositivo similar B' que reenvía la información hacia un dispositivo A' por ejemplo por medio de una fibra óptica, no representada, equipada con un aislador. La información se transmite a continuación hacia el dispositivo A.

Esta variante de realización permite tener en cuenta las amenazas de tipo análisis de la topología del sistema B desde el sistema A mediante exploración, los ataques de tipo protocolario. Esto permite aplicar unas soluciones de filtros independientes en los dos sentidos de flujos al ser diferentes las amenazas asociadas. En este ejemplo los cortes en el protocolo de comunicación no siempre son posibles ya que el canal de comunicación es unidireccional, por el contrario otro canal unidireccional permite un corte denominado « funcional » (por ejemplo, el envío de una información de recepción de mensaje).

REIVINDICACIONES

1. Sistema asegurado de interconexión unidireccional que comprende al menos un sistema A con un nivel de seguridad N_A y un sistema B con un nivel de seguridad N_B, los dos sistemas intercambiando información por medio de una conexión física (3), **que se caracteriza porque**:

- o el medio de conexión física está equipado con un dispositivo aislador óptico (4) adaptado para transmitir la información desde el sistema con el nivel de seguridad N_A hacia el sistema con el nivel de seguridad superior N_B;
- o cada sistema A y B está equipado con una tarjeta óptica de red, (5, 6), cada tarjeta óptica de red consta de una parte receptora Rx y de una parte emisora;
- o las tarjetas (5, 6) están adaptadas para detectar la pérdida de recepción de la señal óptica y la parte Rx receptora de la tarjeta para emitir una alarma si deja de recibir una información procedente del Tx de la tarjeta emisora.

2. Sistema de acuerdo con la reivindicación 1 **que se caracteriza porque**:

- o una parte S_1 de la señal T_1 es emitida por el sistema A y se la es devuelta para reinyectarla en la misma tarjeta (5);
- o el sistema A detecta la señal luminosa S_1 que le llega como si estuviera emitida por el sistema B;
- o el resto de la señal S_2 pasa a través del aislador óptico (4) antes de transmitirse al sistema B.

3. Sistema de acuerdo con la reivindicación 1 **caracterizado porque** el nivel de seguridad N_A es inferior al nivel de seguridad N_B.

4. Sistema de acuerdo con la reivindicación 1 **caracterizado porque** el medio de conexión es una fibra óptica equipada con uno o varios aisladores ópticos.

5. Sistema de acuerdo con la reivindicación 1 **caracterizado porque** el aislador es un aislador pasivo con un nivel de atenuación constante.

6. Sistema de acuerdo con la reivindicación 1 **caracterizado porque** el aislador presenta un nivel de atenuación regulable.

7. Sistema de acuerdo con la reivindicación 1 **caracterizado porque** cada sistema A y B está equipado con unos medios de detección automática de rotura de fibra.

8. Sistema de acuerdo con la reivindicación 1 **caracterizado porque** consta de varios sistemas An con unos niveles más bajos que el sistema B, cada sistema An comunicando con el sistema B por medio de una conexión física, Fi, y **porque** cada conexión física está equipada con un aislador, Ii.

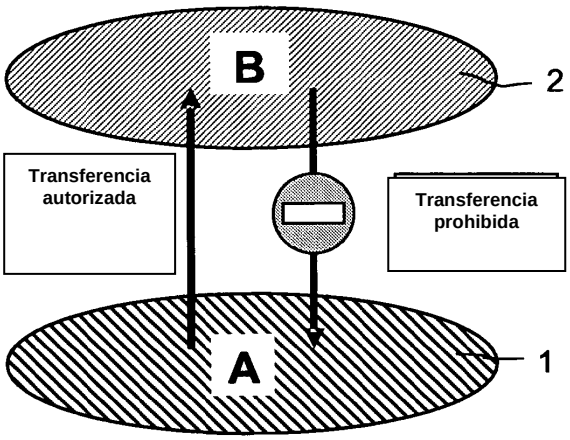
B
2
Transferencia autorizada
Transferencia prohibida
A
1

FIG.1

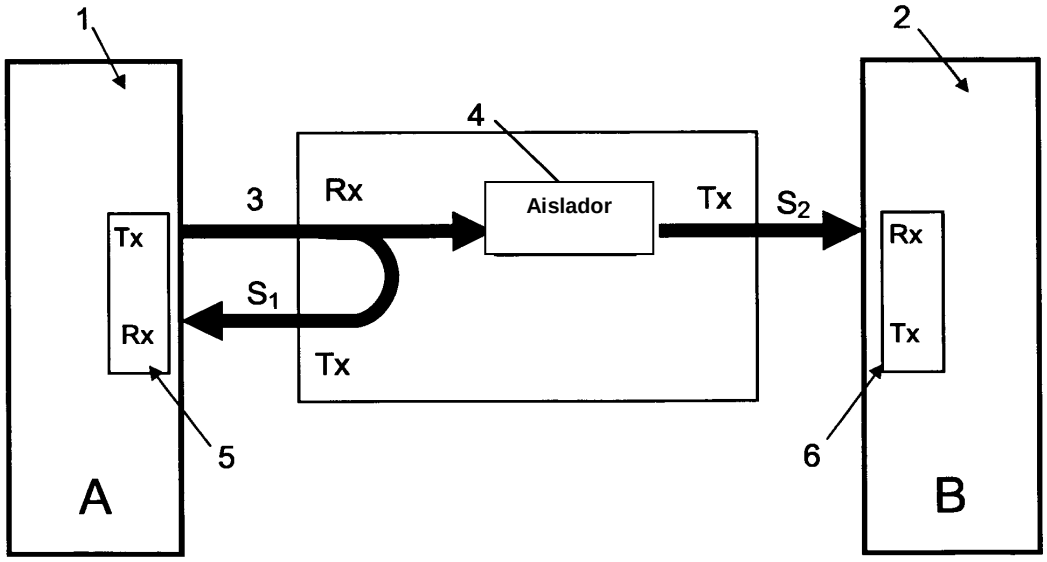
1
2
4
3
Rx
Aislador
Tx
S_2
Tx
Rx
Rx
Tx
S_1
Tx
5
6
A
B

FIG.2

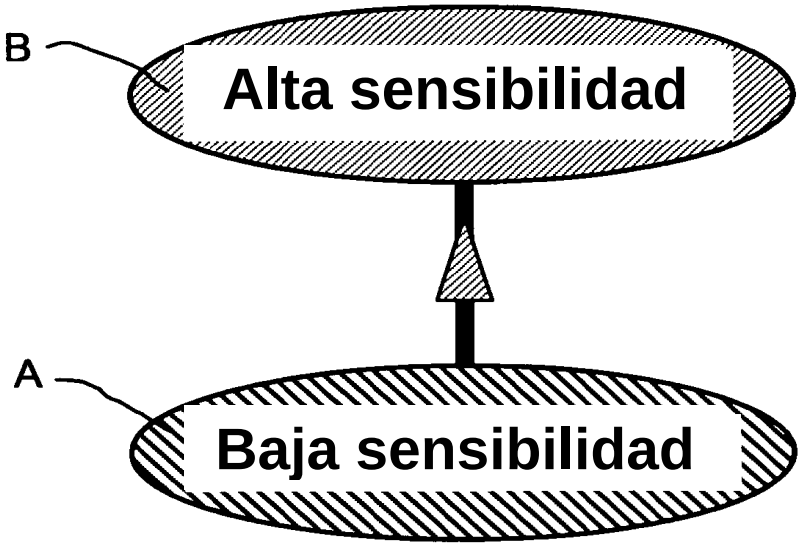
B
Alta sensibilidad
A
Baja sensibilidad

FIG.3

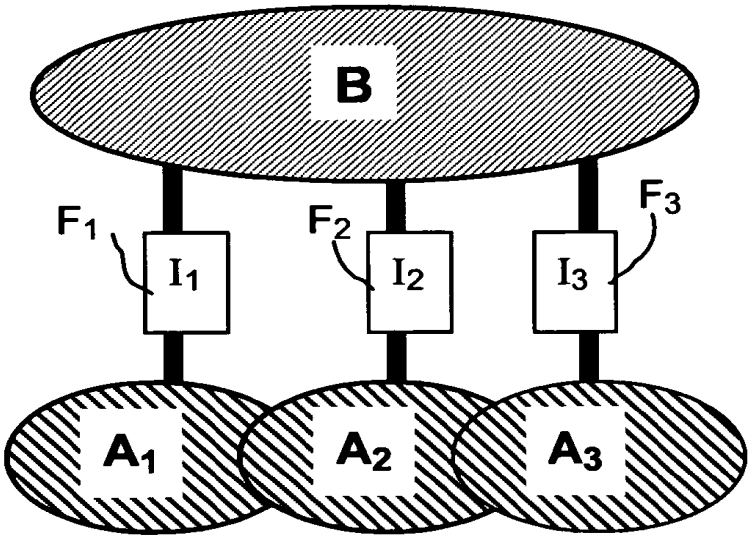
B
F1
F2
F3
I1
I2
I3
A1
A2
A3

FIG.4

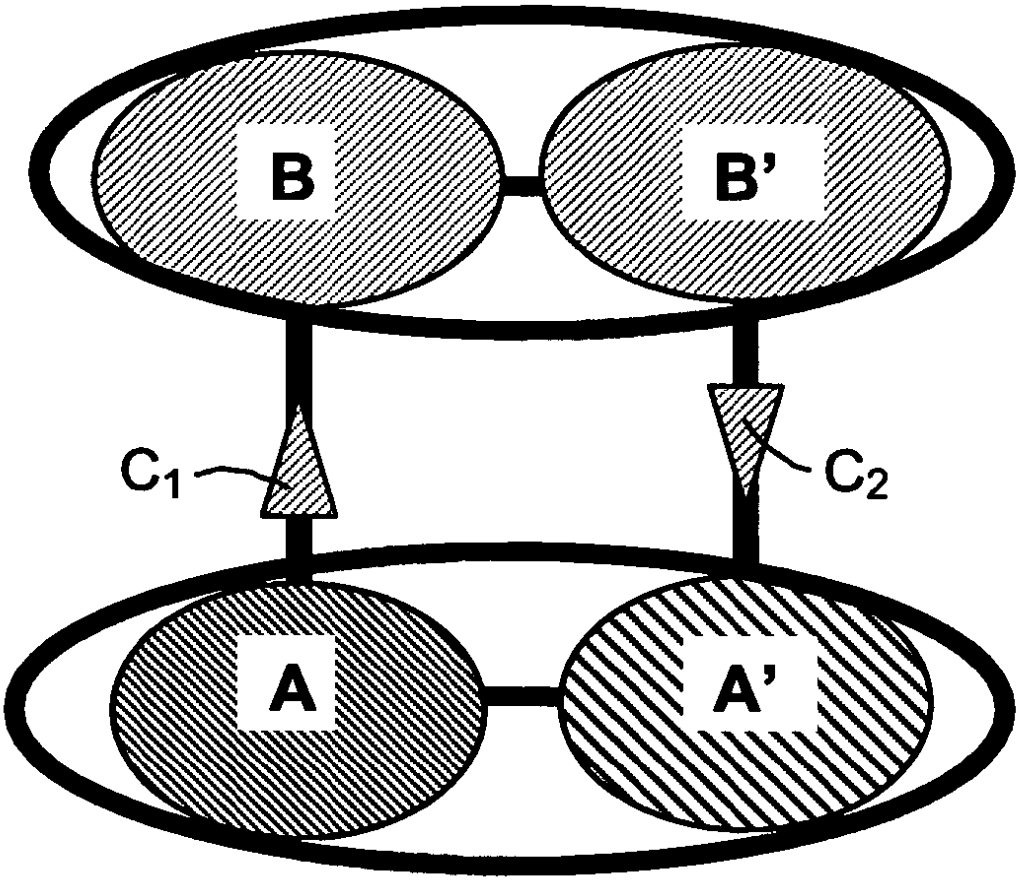

FIG.5