(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 795 109**

(51) Int. CI.:

G06F 21/60 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.12.2017 PCT/EP2017/084232**

(87) Fecha y número de publicación internacional: **28.06.2018 WO18115359**

(96) Fecha de presentación y número de la solicitud europea: **21.12.2017 E 17822302 (0)**

(97) Fecha y número de publicación de la concesión europea: **11.03.2020 EP 3485418**

(54) Título: **Sistema y procedimiento de comunicación unidireccional**

(30) Prioridad:

22.12.2016 FR 1663262

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.11.2020

(73) Titular/es:

AIRBUS DEFENCE AND SPACE SAS (100.0%)
31 rue des Cosmonautes, ZI du Palays
31402 Toulouse Cedex 4, FR

(72) Inventor/es:

DUPONT, GÉRARD;
LAGARDE, OLIVIER y
MARTY, JEAN-LUC

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Sistema y procedimiento de comunicación unidireccional

Sector de la técnica

La presente invención se refiere a un sistema de comunicación desde una red segura hacia una red de menor confianza.

Estado de la técnica

La norma ISO 22301 define la continuidad de la actividad de un sistema de información en uso como su capacidad para proseguir el aprovisionamiento de productos o la prestación de servicios a niveles aceptables y previamente definidos después de un incidente perturbador. También conocida por el acrónimo MCO de mantenimiento en condiciones operativas, también conocida por las siglas MCO de mantenimiento en condiciones operativas, la continuidad de una actividad de un sistema de información en uso busca definir el conjunto de medios y procedimientos necesarios para que el sistema de información siga siendo apto, a lo largo de su vida útil, para el empleo que se le ha asignado. El documento XP002687973, divulga una pasarela unidireccional (diodo de datos) que se utiliza para permitir que los datos de supervisión sean comunicados a partir de un enclave crítico de alta seguridad a una zona desmilitarizada (DMZ), menos segura.

En los sistemas de información denominados críticos, el MCO representa un coste de explotación importante ya que con frecuencia precisa la presencia sobre el terreno de al menos un técnico de mantenimiento que debe mantenerse listo para intervenir en cualquier momento, en cuanto se detecta un incidente perturbador. Esta configuración viene dictada principalmente por la necesidad de confidencialidad de la información asociada al funcionamiento de estos sistemas.

Con el fin de reducir el coste de explotación del MCO, los operadores de sistemas de información críticos contemplan cada vez más la utilización de la televigilancia como a menudo es el caso para los sistemas de información no críticos. En la práctica, cuando se produce un acontecimiento perturbador, un mensaje de aviso se transmite automáticamente al técnico de mantenimiento que está de guardia, por ejemplo, a través de un SMS, correo electrónico o llamada oral por telefonía fija o móvil.

Sin embargo, la adopción de la televigilancia en los sistemas de información crítica a través de una red pública no inspira confianza a los operadores implicados. En efecto, los dispositivos utilizados actualmente para emitir las llamadas preceptivas no garantizan suficiente seguridad de la interconexión entre el sistema de información y la red pública, de manera que existen riesgos de intrusión informáticas y/o de pérdida de información sensible.

Es por tanto importante proponer una solución que permita resolver estos problemas ya que tales fallos de seguridad pueden permitir que se perpetren ataques informáticos que provoquen, por ejemplo, la modificación del comportamiento del sistema de información, su falta de disponibilidad por saturación de sus recursos o permitir, por ejemplo, recuperar información sensible del sistema de información.

Objeto de la invención

A este efecto, un primer objetivo de la invención se refiere a un sistema de comunicación para la transmisión de al menos un mensaje desde una primera red de un primer sistema de información hacia una segunda red de un segundo sistema de información, teniendo la primera red una clasificación de seguridad superior a la de la segunda red. En la práctica, el sistema comprende:

- una entrada del sistema adecuada para conectarse a la primera red y prevista para recibir el mensaje, comprendiendo el mensaje al menos un primer metadato asociado al funcionamiento del primer sistema de información;
- una salida del sistema adecuada para conectarse a la segunda red;
- una unidad de análisis y filtrado de información acoplada a la entrada del sistema y prevista para generar un mensaje filtrado filtrando el mensaje en función de una señal de filtrado de manera que al menos una información sensible asociada a dicho al menos un primer metadato esté enmascarada;
- una unidad de cifrado de información acoplada a la unidad de análisis y filtrado de información y prevista para generar un mensaje cifrado cifrando el mensaje filtrado en función de una señal de cifrado;
- un circuito de diodo de datos acoplado a la unidad de cifrado de información y que comprende una entrada del circuito y una salida del circuito, estando el circuito de diodo de datos previsto para transferir unidireccionalmente el mensaje cifrado entre la entrada del circuito y la salida del circuito, comprendiendo además el circuito de diodo de datos una entrada de control y unos medios de activación para impedir o permitir el paso del mensaje cifrado entre la entrada del circuito y la salida del circuito en función de una señal de control recibida al nivel de la entrada de control;
- una unidad de emisión de mensajes acoplada entre la salida del circuito y la salida del sistema y prevista para

emitir un mensaje de llamada que comprende el mensaje cifrado; y,

- un procesador acoplado a la unidad de análisis y filtrado de información, a la unidad de cifrado de información y al circuito y que está previsto para generar la señal de filtrado, la señal de cifrado y la señal de control.

En una primera implementación, el circuito de diodo de datos además comprende un elemento de diodo de datos que tiene una unidad de transmisión prevista para transmitir unidireccionalmente el mensaje cifrado, estando los medios de activación previstos para ser accionables entre una primera posición en la que los medios de activación están dispuestos para interrumpir la alimentación de la unidad de transmisión y una segunda posición en la que los medios de activación están dispuestos para activar la alimentación de la unidad de transmisión.

En una segunda implementación, la unidad de análisis y filtrado de información además está prevista para generar una primera señal de finalización de operación que indica que se han completado las operaciones de la unidad de análisis y filtrado de información. Además, la unidad de cifrado de información también está prevista para generar una segunda señal de finalización de operación que indica que se han completado las operaciones de la unidad de cifrado de información. Por último, el procesador además está previsto para generar la señal de control en respuesta a la generación sucesiva de la primera señal de finalización de operación y de la segunda señal de finalización de operación.

En una tercera implementación, el sistema además comprende,

- un puerto de memoria acoplado al procesador y previsto para recibir una memoria portátil; y,
- una memoria portátil adecuada para recibirse en el puerto de memoria y configurada para memorizar datos de filtrado y datos de cifrado.

En ese caso, el procesador además está previsto para configurar la señal de filtrado y la señal de cifrado, a partir de los datos de filtrado y de los datos de cifrado, respectivamente.

Según un ejemplo de la tercera implementación,

- la memoria portátil además está configurada para memorizar al menos una lista de contactos que comprende al menos un número de llamada de un dispositivo móvil con el que contactar, estando cada número de llamada asociado al menos a un segundo metadato relativo al funcionamiento del primer sistema de información,
- el procesador además está previsto para incluir la lista de contactos en la señal de filtrado,
- la unidad de análisis y filtrado de información además está prevista para generar un mensaje de asociación que asocia el mensaje filtrado al menos a un número de llamada del que dicho al menos un segundo metadato coincide con el primer metadato,
- la unidad de cifrado de información además está prevista para asociar el mensaje de asociación al mensaje cifrado; y,
- la unidad de emisión de mensajes además está prevista para emitir el mensaje de llamada en función del mensaje de asociación.

En ese caso, preferentemente, la unidad de emisión de mensajes además está prevista para generar y emitir un mensaje de pulsación periódica durante la espera de un mensaje de llamada.

Ventajosamente, la unidad de emisión de mensajes además está prevista para destruir el mensaje de llamada tras la emisión del mensaje de llamada.

En una distribución particular, la unidad de emisión de mensajes está configurada para emitir el mensaje de llamada utilizando un protocolo de mensajería elegido de entre al menos uno de los siguientes protocolos: SMS, MMS, XMPP y SMTP.

En otra distribución particular,

- la unidad de análisis y filtrado de información, la unidad de cifrado de información y el procesador están comprendidos en una primera caja,
- el circuito de diodo de datos está comprendido en una segunda caja; y,
- la unidad de emisión de mensajes está comprendida en una tercera caja.

En ese caso, la primera caja, la segunda caja y la tercera caja son geográficamente independientes entre sí de manera que ninguna radiación electromagnética pueda ser captada de una caja a otra.

De manera ventajosa,

- la unidad de análisis y filtrado de información, la unidad de cifrado de información, el procesador y la unidad de emisión de mensajes están comprendidos en una primera caja; y,
- el circuito de diodo de datos está comprendido en una segunda caja.

En ese caso, la primera caja y la segunda caja son geográficamente independientes entre sí de manera que ninguna radiación electromagnética pueda ser captada de una caja a otra.

Por último, un segundo objetivo de la invención se refiere a un procedimiento de transmisión de al menos un mensaje desde una primera red de un primer sistema de información hacia una segunda red de un segundo sistema de información, teniendo la primera red una clasificación de seguridad superior a la de la segunda red, comprendiendo el mensaje al menos un primer metadato asociado al funcionamiento del primer sistema de información. En la práctica, el procedimiento comprende las siguientes etapas:

- generar un mensaje filtrado filtrando el mensaje en función de una señal de filtrado de manera que al menos una información sensible asociada a dicho al menos un primer metadato está enmascarada;
- generar un mensaje cifrado cifrando el mensaje filtrado en función de una señal de cifrado;
- transferir el mensaje cifrado unidireccionalmente desde la red segura hacia la red no segura en función de una señal de control, solo cuando se han realizado el filtrado y el cifrado.

Descripción de las figuras

Las características y ventajas de la invención se entenderán mejor tras la lectura de la siguiente descripción y con referencia a los dibujos adjuntos, aportados a título ilustrativo y de ningún modo limitativo.

La figura 1 representa un ejemplo de implementación del sistema según la invención.
La figura 2 representa una implementación del circuito de diodo de datos según la invención.
La figura 3 representa un organigrama de un procedimiento según la invención.

Descripción detallada de la invención

En el marco de esta descripción, se entiende por sistema de información al conjunto de medios de hardware, de medios de software, de bases de datos y de redes de comunicación que pueden disponerse para suministrar productos o prestar servicios en un área denominada crítica.

Además, se entiende por área crítica los sistemas de información para los que una avería puede tener consecuencias dramáticas, como la muerte, lesiones graves, daños materiales/económicos importantes o consecuencias graves para el medioambiente. De este modo, esta definición cubre, por ejemplo, los sistemas de información de transporte (por ejemplo, para el pilotaje de un avión, un tren, un coche, un barco), los sistemas de información energéticos (por ejemplo, para el control de una central nuclear), los sistemas de información sanitaria (por ejemplo, un dispositivo médico) o bien los sistemas de información de telecomunicaciones (por ejemplo, un sistema de comunicación a tierra de un sistema de comunicaciones por satélite). No obstante, cualquier sistema de información conforme a la definición anterior también está contemplado en esta descripción.

En la descripción, se entiende asimismo por incidente perturbador, al conjunto de acontecimientos vinculados al estado operativo de un sistema de información tal como: el fallo de un componente de almacenamiento, defecto de alimentación de un motor de un dispositivo, la caída de tensión de control de una máquina, la caída de la potencia (hidráulica, eléctrica, etc.) recibida por una máquina, una avería mecánica. No obstante, cabe destacar que la invención no se refiere a la detección y diagnóstico de un incidente perturbador. En el resto de la descripción, se considerará que se ha detectado y diagnosticado un incidente como perturbador al nivel de un sistema de información. El incidente perturbador a continuación se incluye en un mensaje que se transmitirá a un técnico de mantenimiento o a un experto técnico.

En la invención, se propone una solución al problema de la protección de una red segura contra ciberataques cuando la red segura tiene que comunicar informaciones desde la red segura hacia una red pública, por ejemplo, mediante la emisión de alertas y notificaciones a operadores remotos. En la práctica, la solución se basa en la utilización de diodo de datos (también conocido por el nombre de diodo de red o "data diode" en inglés) para permitir la transmisión unidireccional de información desde la red segura hacia una red pública. Esto tiene el efecto de volver imposible un ataque informático de la red segura desde la red pública. De este modo, esta disposición garantiza una separación física entre la red segura y la red pública.

La figura 1 representa un sistema 300 según la invención. En el ejemplo de la figura 1, el sistema 300 está situado entre una red segura 100 y una red no segura 200. La red segura 100 está asociada a un primer sistema de información mientras que la red no segura 200 está asociada a un segundo sistema de información diferente del primer sistema de información. De manera general, se considera que la red segura 100 es más segura que la red no segura 200 ya que cuenta con una clasificación de seguridad superior a la de la red no segura 200.

Estructuralmente, el sistema 300 comprende une entrada del sistema 301 y una salida del sistema 302. Además, el sistema 300 comprende una unidad de análisis y filtrado de información 310, una unidad de cifrado de información 320, un circuito de diodo de datos 330, una unidad de emisión de mensajes 340 y un procesador 350.

En el ejemplo de la figura 1, la entrada del sistema 301 está configurada para conectarse a la red segura 100 mientras que la salida del sistema 302 está configurada para conectarse a la red no segura 200. Cuando el sistema 300 está operativo, la entrada del sistema 301 está prevista para recibir un mensaje que comprenda al menos un metadato asociado al funcionamiento del primer sistema de información.

Se entiende por mensaje, un conjunto de señales digitales a las que se les ha dado una forma determinada. Por ejemplo, el mensaje recibido en la entrada del sistema 301 puede ser un mensaje de texto según la norma RFC5424 o cualquier otro estándar normalizado o no. El mensaje puede comprender elementos de identificación del mensaje, de marca de tiempo y fecha de generación del mensaje, de identificación de la fuente del mensaje o bien de identificación del acontecimiento que ha provocado la generación del mensaje. No obstante, se pueden añadir otros elementos al mensaje que se va a transmitir.

En el presente documento se entiende por metadato a cualquier información descriptiva del funcionamiento del primer sistema de información. Por ejemplo, en el sector del transporte, puede tratarse de datos relativos al fallo de un componente de almacenamiento, al estado de salud de los motores o bien a la temperatura de una pieza o de un componente.

De vuelta a la figura 1, la unidad de análisis y filtrado de información 310 está acoplada a la entrada del sistema 301. En operación, la unidad de análisis y filtrado de información 310 está configurada para generar un mensaje filtrado filtrando el mensaje recibido en función de una señal de filtrado. La señal de filtrado contiene toda la información que permite a la unidad de análisis y filtrado de información 310 determinar la extensión de la información que se debe filtrar. En la práctica, la unidad de análisis y filtrado de información 310 filtra el metadato del mensaje recibido en la entrada del sistema 301 de manera que al menos una información sensible asociada al metadato está enmascarada. Esto tiene el efecto de impedir la fuga de información sensible desde la red segura 100.

Se entiende por información sensible, una información o un conocimiento obtenido directa o indirectamente, que si se revelara al público, perjudicaría al sistema de información al que se refiere. En otras palabras, se trata de una información cuya divulgación, utilización con malas intenciones, modificación o acceso no autorizado pueden afectar desfavorablemente a la seguridad del sistema de información implicado. Por ejemplo, puede tratarse de una información asociada a la identificación de los servidores informáticos del sistema de información, tal como las direcciones IP, los nombres de los servidores o bien el tamaño de los servidores informáticos. En efecto, tal información puede, por ejemplo, informar sobre las capacidades de ataque o defensa del sistema de información. En ese caso, si la información sensible cae en malas manos, podría afectar negativamente a la seguridad de una organización.

En una primera implementación particular de la unidad de análisis y filtrado de información 310, el enmascaramiento se realiza mediante la supresión de información sensible del metadato. Por ejemplo, la dirección IP de un servidor que haya sufrido un incidente perturbador puede suprimirse del metadato.

En una segunda implementación de la unidad de análisis y filtrado de información 310, el enmascaramiento se realiza mediante la sustitución de la información sensible del metadato por una o varias informaciones no sensibles. Por ejemplo, el nombre de un servidor que haya sufrido un incidente perturbador puede ser sustituido por otro nombre o una sigla diferente del verdadero nombre del servidor. En ese caso, el operador que recibirá el mensaje debe conocer la o las palabras de sustitución. Otra posibilidad del mismo orden puede consistir en sustituir la información sensible mediante ofuscación para codificar la información sensible.

En una tercera implementación de la unidad de análisis y filtrado de información 310, el enmascaramiento se realiza mediante una combinación de supresión y sustitución de información sensible. De este modo, si un metadato comprende la dirección IP y el nombre de un servidor que haya sufrido un incidente perturbador, las soluciones de la primera implementación y de la segunda implementación se pueden utilizar conjuntamente. Por ejemplo, se puede sustituir la dirección IP por una sigla y suprimirse el nombre del metadato.

También en la figura 1, la unidad de cifrado de información 320 está acoplada a la unidad de análisis y filtrado de información 310. En operación, la unidad de cifrado de información 320 está configurada para generar un mensaje cifrado cifrando el mensaje filtrado en función de una señal de cifrado. La señal de filtrado contiene toda la información que permite a la unidad filtrado de información 320 cifrar la información filtrada. En la práctica, el cifrado puede hacerse con ayuda de todos los medios de cifrado conocidos por el experto en la materia, concretamente mediante la utilización de un algoritmo simétrico o asimétrico. Esto tiene el efecto de impedir que se intercepten los mensajes de notificación emitidos desde la red segura 100.

De nuevo en la figura 1, el circuito de diodo de datos 330 está acoplado a la unidad de cifrado de información 320. Le circuito de diodo de datos 330 comprende una entrada del circuito 331, una salida del circuito 332 y un elemento del diodo de datos 333. En operación, el elemento del diodo de datos 333 está configurado para transferir unidireccionalmente el mensaje cifrado entre la entrada del circuito 331 y la salida del circuito 332. En efecto, el elemento del diodo de datos 333 que es asimismo conocido por el nombre de diodo de red es un sistema que permite interconectar dos redes informáticas permitiendo la transferencia de datos en un único sentido. Este tipo de sistema

generalmente se emplea para unir una red que precisa un nivel de seguridad elevado a una red de menor confianza (por ejemplo, Internet). En ese caso, solo está autorizada la subida de información de la red de menor confianza con el fin de garantizar la confidencialidad de la red segura evitando fugas de información sensible. No obstante, en el marco de la invención se ha contemplado la utilización del elemento del diodo de datos 333 en sentido inverso de manera que solo sea posible subir información desde la red segura. Esto tiene por efecto que sea imposible implementar ataques informáticos desde el exterior de la red segura, ya que solo hay un único canal de comunicación desde la red segura hacia la red de menor confianza y no en el otro sentido.

Además, en la figura 1, el circuito de diodo de datos 330 comprende una entrada de control 335 y unos medios de activación 334 para impedir o permitir el paso del mensaje cifrado entre la entrada del circuito 331 y la salida del circuito 332 en función de una señal de control recibida al nivel de la entrada de control 335. Los medios de activación 334 están previstos para ser accionables entre una primera posición en la que los medios de activación 334 impiden el paso del mensaje cifrado, y una segunda posición en la que los medios de activación 334 permiten el paso de información. Por último, los medios de activación 334 normalmente están accionados en la primera posición.

En la figura 2, se ha representado una implementación particular del circuito de diodo de datos 330 según la invención. En el ejemplo de la figura 2, el elemento de diodo de datos 333 del circuito de diodo de datos 330 comprende un elemento de transmisión TX y un elemento de recepción RX, ambos previstos en combinación para transmitir unidireccionalmente el mensaje cifrado entre el elemento de transmisión TX y el elemento de recepción RX. En un ejemplo, el elemento de diodo de datos 333 está realizado basándose en una fibra óptica que sólo comprende un único hilo. En ese caso, el elemento de transmisión TX puede ser una fuente de luz prevista para emitir un flujo de luz por la fibra óptica y el elemento de recepción RX puede ser un fotoreceptor previsto para recibir el flujo de luz. No obstante, también se pueden utilizar otras implementaciones de enlace de red unidireccional con la invención. Por ejemplo, también se ha contemplado la utilización de un enlace en serie RS-232 parcial o bien un enlace Ethernet RJ45 parcial con los elementos de transmisión y recepción correspondientes.

En una implementación particular de la figura 2, los medios de activación 334 se accionan en la primera posición controlando la interrupción de la alimentación del elemento de transmisión TX mientras que los medios de activación 334 se accionan en la segunda posición controlando la activación de la alimentación del elemento de transmisión TX. Para ello, los medios de activación 334 pueden estar directamente conectados a la alimentación del elemento de transmisión TX.

De vuelta a la figura 1, la unidad de emisión de mensajes 340 está acoplada entre la salida del circuito 332 y la salida del sistema 302. En operación, la unidad de emisión de mensajes 340 está configurada para emitir un mensaje de llamada que comprende el mensaje cifrado. En una implementación particular, la unidad de emisión de mensajes 340 está configurada para emitir el mensaje de llamada utilizando un protocolo de mensajería elegido de entre al menos uno de los siguientes protocolos: SMS, correo electrónico, MMS, XMPP,... De este modo, para una mayor seguridad, no se conserva ninguna copia del mensaje emitido al nivel del sistema 300.

En una implementación particular, la unidad de emisión de mensajes 340 está prevista para destruir el mensaje de llamada tras la emisión del mensaje de llamada.

En un ejemplo de la implementación anterior, la unidad de emisión de mensajes 340 está prevista para recibir un mensaje de acuse de recibo en respuesta a la emisión del mensaje de llamada y para destruir el mensaje de llamada en respuesta a la recepción del mensaje de acuse de recibo.

En otra implementación particular, la unidad de emisión de mensajes 340 además está prevista para generar y emitir un mensaje de pulsación periódica (en inglés, "heartbeat mensaje" o "keep alive mensaje") mientras está a la espera de un mensaje de llamada. El mensaje de pulsación está previsto para indicar al destinatario del mensaje que el sistema 300 todavía está en vía de ejecución. En otras palabras, el mensaje de pulsación periódica permite indicar al destinatario del mensaje que el sistema 300 todavía está en activo. En un ejemplo, el periodo de generación y emisión del mensaje de pulsación puede fijarse para que sea cada minuto, cada media hora o cada hora. En una implementación particular, el mensaje de pulsación periódica está cifrado y dispuesto de manera que no sea posible interceptarlo y poder simular así la presencia del sistema 300 reproduciendo de nuevo una secuencia de transmisión del mensaje de pulsación periódica ya utilizada.

Por último, en la figura 1, el procesador 350 está acoplado a la unidad de análisis y filtrado de información 310, a la unidad de cifrado de información 320 y al circuito de diodo de datos 330. En operación, el procesador 350 está configurado para generar la señal de filtrado, la señal de cifrado y la señal de control.

En una primera implementación del procesador 350, el conjunto de informaciones que permite configurar la señal de filtrado, la señal de cifrado y la señal de control está comprendido en una memoria del procesador 350. En ese caso, es el procesador 350 el que ordena la generación de las señales de filtrado, de cifrado y de control. En el marco de esta implementación particular, se debe entender que la señal de filtrado se ha generado antes que la señal de cifrado, de manera que la señal de control se genere accionando los medios de activación 334 en la segunda posición solo cuando se han realizado las operaciones de enmascaramiento y filtrado. Por ejemplo, el procesador 350 puede generar

la señal de cifrado, por un lado, y la señal de control, por otro lado, después de una temporización predeterminada tras la generación de la señal de filtrado, por un lado, y de la señal de cifrado, por el otro. De esta manera, se puede garantizar que se ha filtrado previamente cualquier información sensible de la información transmitida y que esta se ha cifrado.

En una segunda implementación del procesador 350, la generación de la señal de control está condicionada por la ejecución de las operaciones de la unidad de análisis y filtrado de información 310 y luego de la unidad de cifrado de información 320. En la práctica, la unidad de análisis y filtrado de información 310 además está prevista para generar una primera señal de finalización de operación que indica que se han completado las operaciones de la unidad de análisis y filtrado de información 310. Lo mismo ocurre para la unidad de cifrado de información 320 que también está prevista para generar una segunda señal de finalización de operación que indica que se han completado las operaciones de la unidad de cifrado de información 320. Por último, el procesador 350 además está previsto para generar la señal de control en respuesta a la generación de la primera señal de finalización de operación y de la segunda señal de finalización de operación. En el marco de esta implementación particular, se debe entender que la primera señal de finalización de operación se ha generado antes de la segunda señal de finalización de operación, de manera que la señal de control se genere accionando los medios de activación 334 en la segunda posición solo cuando se han realizado las operaciones de enmascaramiento y filtrado. De esta manera, se puede garantizar que se ha filtrado previamente cualquier información sensible de la información transmitida y que esta se ha cifrado.

En otra implementación particular del sistema 300, se incorpora un puerto de memoria y una memoria portátil. En esta implementación, el puerto de memoria está acoplado al procesador 350 y configurado para recibir memoria portátil. Además, la memoria portátil está configurada para memorizar datos de filtrado y datos de cifrado. Por último, el procesador 350 está adaptado para configurar, respectivamente, la señal de filtrado y la señal de cifrado a partir de los datos de filtrado y de los datos de cifrado. De este modo, en esta implementación particular, los datos que permiten configurar la señal de filtrado y la señal de cifrado se obtienen a partir de la memoria portátil. Esto ofrece la posibilidad a los propietarios del sistema de información seguro 100 determinar la manera en la que se deben realizar el filtrado y el cifrado.

En un ejemplo de esta implementación particular del sistema 300, la memoria portátil también se puede configurar para memorizar datos de control que el procesador 350 puede utilizar para configurar la señal de control.

En un ejemplo de la implementación anterior, la memoria portátil además está configurada para memorizar al menos una lista de contactos que comprenda al menos un número de llamada de un dispositivo móvil o fijo con el que contactar. En este ejemplo, cada número de llamada está asociado al menos a un segundo metadato relativo al funcionamiento de la red segura 100. Además, también se ha previsto que el procesador 350 incluya la lista de contactos en la señal de filtrado. Por otra parte, la unidad de análisis y filtrado de información 310 también está configurada para generar un mensaje de asociación que asocia el mensaje filtrado al menos a un número de llamada cuyo segundo metadato coincide con el primer metadato. Esta disposición tiene el efecto de permitir la notificación de la aparición de un incidente a uno o más de los técnicos más adecuados para resolver el incidente.

Se dirá que el primer metadato y el segundo metadato coinciden cuando ambos comprendan una información relativa al mismo incidente perturbador de la red segura 100. Por ejemplo, si el primer metadato puede comprender una información que indique que se ha producido un fallo en un componente de almacenamiento, entonces un segundo metadato que coincide con el primer metadato también comprende una información relativa al fallo de un componente de almacenamiento. En la práctica, como cada número de llamada está asociado a un técnico especialista en uno o más incidentes perturbadores de la red segura 100, entonces, la correlación de coincidencias según la invención tiene por objetivo limitar la lista de llamadas solo a los números asociados a los técnicos especialistas en el incidente perturbador que se ha producido.

En una implementación particular, se podrá contemplar la instauración de una tabla de conciencias que permita asociar una especialidad técnica a un incidente perturbador. Por ejemplo, todos los fallos del primer sistema de información que estén vinculados a la mecánica pueden correlacionarse con la especialidad técnica de un mecánico. De este modo, gracias a la tabla de coincidencias y a la lista de contactos, la unidad de análisis y filtrado de información 310 es capaz de determinar el o los números de llamada pertinentes que están asociados con la aparición de un incidente perturbador particular correlacionando el incidente perturbador con una especialidad técnica particular. En la práctica, se puede contemplar el almacenar la tabla de coincidencias en una memoria de la unidad de análisis y filtrado de información 310 o bien en el procesador 350.

En otro ejemplo de la implementación anterior, se puede contemplar el externalizar la funcionalidad que permite determinar el o los números de llamada pertinentes que están asociados con la aparición de un incidente perturbador particular, en una unidad independiente de la unidad de análisis y filtrado de información 310. Por ejemplo, se puede utilizar una unidad de enrutamiento acoplada a la unidad de análisis. En ese caso, la unidad de enrutamiento puede comprender una memoria así, como un procesador. La memoria puede entonces comprender la inclusión de la lista de contactos y de la tabla de coincidencias, ambas mencionadas anteriormente. En este ejemplo particular, la unidad de análisis y filtrado de información 310 está configurada para suministrar el segundo metadato relativo al funcionamiento de la red segura 100 a la unidad de enrutamiento. A continuación, la unidad de enrutamiento está

configurada para determinar y devolver a la unidad de análisis y filtrado de información 310, al menos un número de llamada cuyo segundo metadato coincide con el primer metadato. Además, la unidad de enrutamiento también está configurada para determinar y devolver a la unidad de análisis y filtrado de información 310 el o los números de llamada pertinentes que están asociados con la aparición de un incidente perturbador particular correlacionando el incidente perturbador con una especialidad técnica particular.

A continuación, la unidad de cifrado de información 320 también está configurada para asociar el mensaje de asociación al mensaje cifrado. Por último, la unidad de emisión de mensajes 340 también está configurada para emitir el mensaje de llamada en función del mensaje de asociación. En otro ejemplo de esta implementación, se puede contemplar la inclusión de la lista de contactos en una memoria del procesador 350.

En una implementación de la invención, se puede contemplar el disponer físicamente los diferentes elementos del sistema 300 de acuerdo con varias distribuciones.

Por ejemplo, en una primera distribución, en una primera caja se agrupan la unidad de análisis y filtrado de información 310, la unidad de cifrado de información 320 y el procesador 350. Seguidamente, se incluye el circuito de diodo de datos en una segunda caja independiente de la primera caja. Por último, se coloca la unidad de emisión de mensajes 340 en una tercera caja independiente de la primera caja y de la segunda caja. Con esta distribución, la primera caja, la segunda caja y la tercera caja pueden ser geográficamente independientes entre sí de manera que ninguna radiación electromagnética pueda ser captada de una caja a otra.

En una segunda distribución, en una primera caja se agrupan la unidad de análisis y filtrado de información 310, la unidad de cifrado de información 320, el procesador 350 y la unidad de emisión de mensajes 340. Seguidamente, se coloca el circuito de diodo de datos 330 en una segunda caja independiente de la primera caja. Con esta distribución, la primera caja y la segunda caja son geográficamente independientes entre sí de manera que ninguna radiación electromagnética pueda ser captada de una caja a otra.

En la descripción, se ha considerado que la información transmitida desde la red segura 100 hacia la red segura 200 estaba vinculada a una disfunción del primer sistema de información. Esto tiene el efecto de permitir la instauración remota del mantenimiento correctivo preceptivo del primer sistema de información a través de una red pública. No obstante, gracias a la invención, la información que no está necesariamente vinculada a una disfunción del primer sistema de información también puede transmitirse hacia el exterior de este sistema. En ese caso, la unidad de análisis y filtrado de información 310 deberá configurarse para dejar pasar la información correspondiente. Esto tendrá el efecto de permitir la instauración de una supervisión remota del primer sistema de información.

La invención también se refiere a un emisor (no representado) de un sistema de comunicación de tipo alámbrico o inalámbrico que comprende el sistema 300 tal como se ha descrito antes. Tal emisor permite el establecimiento de una comunicación unidireccional encriptada a través de una red de comunicación cualquiera y concretamente una red pública.

La invención también se refiere a un procedimiento 400 para la transmisión de al menos un primer metadato desde la red segura 100 hacia la red no segura 200 según los aspectos técnicos descritos anteriormente. En la figura 3, el procedimiento 400 comprende las siguientes etapas, que consisten en:

- generar un mensaje filtrado 410 filtrando el primer metadato en función de la señal de filtrado, como se ha descrito antes, de manera que al menos una información sensible asociada al primer metadato esté enmascarada;
- generar un mensaje cifrado 420 cifrando el mensaje filtrado en función de la señal de cifrado, como se ha descrito antes;
- transferir unidireccionalmente 430 el mensaje cifrado desde la red segura 100 hacia la red no segura 200, condicionalmente, controlando el paso del mensaje cifrado en función de la señal de control como se ha descrito antes.

La invención descrita aporta una solución al problema de la protección de una red segura contra ciberataques cuando la red segura se ve forzada a comunicar informaciones desde la red segura hacia una red pública. En efecto, en conjunto, el sistema según la invención difícilmente se verá comprometido por un ciberataque. Más concretamente, solo la unidad de emisión de mensajes es susceptible de quedar comprometida o de ser dañada por un ataque de este tipo. No obstante, como esta unidad se encuentra situada aguas abajo del límite de seguridad física del sistema (c-a-d después del circuito de diodo de datos), su pérdida no afecta entonces a la seguridad global de la red segura. De este modo, la adición de un sistema según la invención a un sistema de información existente no supone ninguna oportunidad para la implementación de un ciberataque contra la red de este sistema de información. Además, gracias a la utilización de un circuito de diodo de datos controlado, también se garantiza que no haya fugas de ninguna información sensible desde la red segura a través del sistema según la invención. También se puede utilizar la noción de "tiristor de datos". En efecto, como un tiristor permite la conducción unidireccional de la corriente gracias al control de una puerta, el "tiristor de datos" permite la transmisión unidireccional de un mensaje después de que se haya limpiado de información sensible el mensaje que se va a emitir y después de que haya cifrado. En ese caso, el mensaje ejerce las funciones de corriente, mientras que la información de confirmación de la limpieza y el cifrado del mensaje

ejercen la función de puerta del tiristor.

REIVINDICACIONES

1. Sistema de comunicación (300) para la transmisión de al menos un mensaje desde una primera red (100) de un primer sistema de información hacia una segunda red (200) de un segundo sistema de información, teniendo la primera red (100) una clasificación de seguridad superior a la de la segunda red, comprendiendo el sistema (300)

- una entrada del sistema (301) adecuada para conectarse a la primera red, y prevista para recibir el mensaje, comprendiendo el mensaje al menos un primer metadato asociado al funcionamiento del primer sistema de información;
- una salida del sistema (302) adecuada para conectarse a la segunda red;
- una unidad de análisis y filtrado de información (310) acoplada a la entrada del sistema, y prevista para generar un mensaje filtrado filtrando el mensaje en función de una señal de filtrado de manera que al menos una información sensible asociada a dicho al menos un primer metadato esté enmascarada;
- una unidad de cifrado de información (320) acoplada a la unidad de análisis y filtrado de información, y prevista para generar un mensaje cifrado cifrando el mensaje filtrado en función de una señal de cifrado;
- un circuito de diodo de datos (330) acoplado a la unidad de cifrado de información (320), y que comprende una entrada del circuito (331) y una salida del circuito (332), estando el circuito de diodo de datos (330) previsto para transferir unidireccionalmente el mensaje cifrado entre la entrada del circuito (331) y la salida del circuito (332), comprendiendo además el circuito de diodo de datos una entrada de control (335) y unos medios de activación (334) para impedir o permitir el paso del mensaje cifrado entre la entrada del circuito (331) y la salida del circuito (332) en función de una señal de control recibida al nivel de la entrada de control (335);
- una unidad de emisión de mensajes (340) acoplada entre la salida del circuito (332) y la salida del sistema (302), y prevista para emitir un mensaje de llamada que comprende el mensaje cifrado; y,
- un procesador (350) acoplado a la unidad de análisis y filtrado de información (310), a la unidad de cifrado de información (320) y al circuito (330), y previsto para generar la señal de filtrado, la señal de cifrado y la señal de control.

2. Sistema según la reivindicación 1 en donde, el circuito de diodo de datos además comprende un elemento de diodo de datos (333) que tiene una unidad de transmisión prevista para transmitir unidireccionalmente el mensaje cifrado, estando los medios de activación (334) previstos para ser accionables entre una primera posición en la que los medios de activación (334) están dispuestos para interrumpir la alimentación de la unidad de transmisión y una segunda posición en la que los medios de activación (334) están dispuestos para activar la alimentación de la unidad de transmisión.

3. Sistema según una cualquiera de las reivindicaciones 1 o 2 en donde,

- la unidad de análisis y filtrado de información (310) además está prevista para generar una primera señal de finalización de operación que indica que se han completado las operaciones de la unidad de análisis y filtrado de información (310);
- la unidad de cifrado de información (320) además está prevista para generar una segunda señal de finalización de operación que indica que se han completado las operaciones de la unidad de cifrado de información (320); y,
- el procesador (350) además está previsto para generar la señal de control en respuesta a la generación sucesiva de la primera señal de finalización de operación y de la segunda señal de finalización de operación.

4. Sistema según una cualquiera de las reivindicaciones 1, 2 o 3 que además comprende,

- un puerto de memoria acoplado al procesador y previsto para recibir una memoria portátil; y,
- una memoria portátil adecuada para recibirse en el puerto de memoria y configurada para memorizar datos de filtrado y datos de cifrado;

en donde el procesador además está previsto para configurar la señal de filtrado y la señal de cifrado, a partir de los datos de filtrado y de los datos de cifrado, respectivamente.

5. Sistema según la reivindicación 4 en donde,

- la memoria portátil además está configurada para memorizar al menos una lista de contactos que comprende al menos un número de llamada de un dispositivo móvil con el que contactar, estando cada número de llamada asociado al menos a un segundo metadato relativo al funcionamiento del primer sistema de información,
- el procesador además está previsto para incluir la lista de contactos en la señal de filtrado,
- la unidad de análisis y filtrado de información además está prevista para generar un mensaje de asociación que asocia el mensaje filtrado al menos a un número de llamada del que dicho al menos un segundo metadato coincide con el primer metadato,
- la unidad de cifrado de información además está prevista para asociar el mensaje de asociación al mensaje cifrado; y,
- la unidad de emisión de mensajes además está prevista para emitir el mensaje de llamada en función del mensaje de asociación.

6. Sistema según la reivindicación 5 en donde la unidad de emisión de mensajes además está prevista para generar y emitir un mensaje de pulsación periódica mientras se espera un mensaje de llamada.

7. Sistema según una cualquiera de las reivindicaciones 1, 2, 3, 4, 5 o 6 en donde la unidad de emisión de mensajes además está prevista para destruir el mensaje de llamada tras la emisión del mensaje de llamada.

8. Sistema según una cualquiera de las reivindicaciones 1, 2, 3, 4, 5, 6 o 7 en donde la unidad de emisión de mensajes está configurada para emitir el mensaje de llamada utilizando un protocolo de mensajería elegido de entre al menos uno de los siguientes protocolos: SMS, MMS, XMPP y SMTP.

9. Sistema según una cualquiera de las reivindicaciones 1, 2, 3, 4, 5, 6, 7 u 8 en donde,

- la unidad de análisis y filtrado de información, la unidad de cifrado de información y el procesador están comprendidos en una primera caja,
- el circuito de diodo de datos está comprendido en una segunda caja; y,
- la unidad de emisión de mensajes está comprendida en una tercera caja;

en donde, la primera caja, la segunda caja y la tercera caja son geográficamente independientes entre sí de manera que ninguna radiación electromagnética pueda ser captada de una caja a otra.

10. Sistema según una cualquiera de las reivindicaciones 1, 2, 3, 4, 5, 6, 7, 8 o 9 en donde,

- la unidad de análisis y filtrado de información, la unidad de cifrado de información, el procesador y la unidad de emisión de mensajes están comprendidos en una primera caja; y,
- el circuito de diodo de datos está comprendido en una segunda caja;

en donde, la primera caja y la segunda caja son geográficamente independientes entre sí de manera que ninguna radiación electromagnética pueda ser captada de una caja a otra.

11. Procedimiento (400) de transmisión de al menos un mensaje desde una primera red (100) de un primer sistema de información hacia una segunda red (200) de un segundo sistema de información, teniendo la primera red (100) una clasificación de seguridad superior a la de la segunda red, comprendiendo el mensaje al menos un primer metadato asociado al funcionamiento del primer sistema de información, comprendiendo el procedimiento las siguientes etapas:

- generar (410) un mensaje filtrado filtrando el mensaje en función de una señal de filtrado de manera que al menos una información sensible asociada a dicho al menos un primer metadato esté enmascarada;
- generar (420) un mensaje cifrado cifrando el mensaje filtrado en función de una señal de cifrado;
- transferir unidireccionalmente (430), por un circuito de diodo de datos, el mensaje cifrado desde la red segura (100) hacia la red no segura (200) en función de una señal de control, solo cuando se han realizado el filtrado y el cifrado.

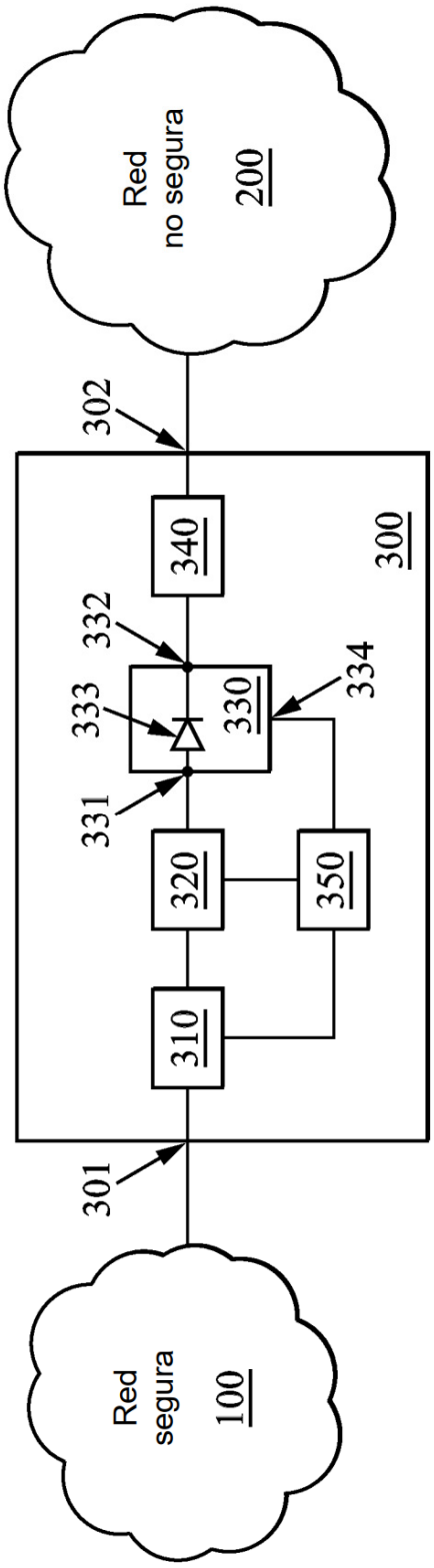
Red
no segura
200
302
340
300
332
333
330
334
331
320
350
310
301
Red
segura
100

FIG. 1

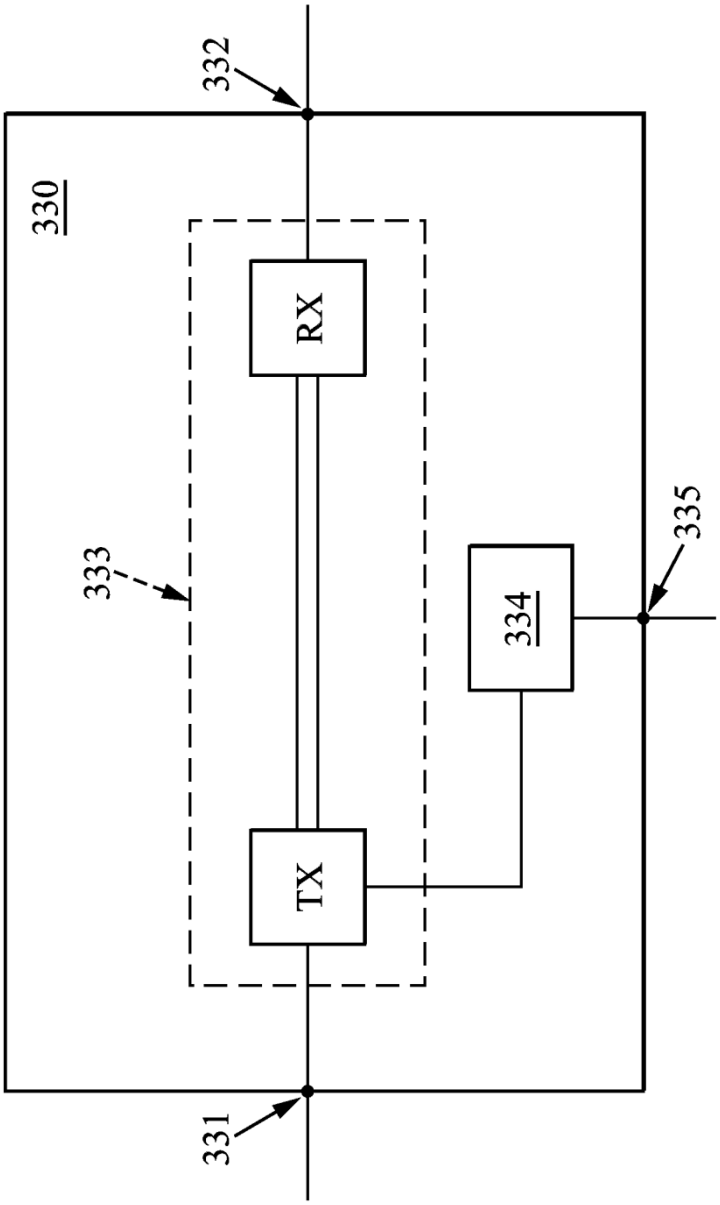

FIG. 2

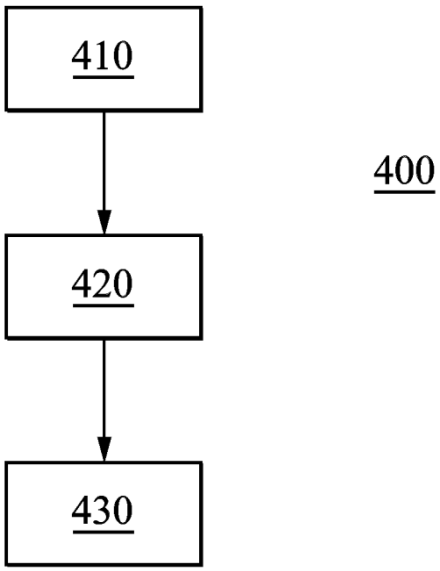

FIG. 3