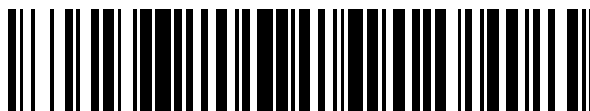


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 577 291**

51 Int. Cl.:

**H04L 9/32**

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **28.12.2006** **E 06832267 (6)**

97 Fecha y número de publicación de la concesión europea: **13.04.2016** **EP 2035948**

54 Título: **Enlaces unidireccionales seguros desde y hacia un motor de seguridad**

30 Prioridad:

**27.06.2006 US 816924 P**

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

**14.07.2016**

73 Titular/es:

**WATERFALL SECURITY SOLUTIONS LTD.  
(100.0%)**

**21 Hamelacha Street, Afek Industrial Park Idan  
Building no. 2  
48091 Rosh Ha'ayin, IL**

72 Inventor/es:

**FRENKEL, LIOR y  
ZILBERSTEIN, AMIR**

74 Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

ES 2 577 291 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Enlaces unidireccionales seguros desde y hacia un motor de seguridad

### Sector técnico de la invención

5 La presente invención se refiere, en general, a los sistemas de comunicación de datos, y específicamente a sistemas y procedimientos de seguridad informática.

### Antecedentes de la invención

10 En una red informática que maneja datos extremadamente confidenciales, tales como datos en entornos militares o financieros, partes de la red pueden estar conectadas mediante enlaces de datos unidireccionales. Por ejemplo, los datos confidenciales que se requiere no sean accesibles desde sitios externos se pueden almacenar en un ordenador que está configurado para recibir datos sobre un enlace unidireccional y que no tiene ningún enlace físico saliente sobre el que se puedan transmitir datos al sitio externo.

15 Los enlaces unidireccionales se pueden implementar, por ejemplo, utilizando sistemas Waterfall™, que están fabricados por la firma GITA Technologies, Ltd. (Rosh HaAyin, Israel). Las especificaciones de los sistemas Waterfall están disponibles en el sitio web GITA en [www.waterfall.co.il](http://www.waterfall.co.il). Cuando un ordenador transmisor está conectado mediante 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 ninguna comunicación de retorno al ordenador transmisor.

La patente de EE.UU. 6.049.611 describe la generación de datos de autenticación mediante un verificador que incluye un generador de números aleatorios.

20 La patente de EE.UU. 6.026.502 describe un mecanismo para impedir la invasión de un ordenador por virus informáticos, mediante un dispositivo de vigilancia de enlaces que comunica con un servidor por medio de lados de entrada y salida conmutados.

La publicación de patente de EE.UU. 2005/0122930 describe un controlador de tráfico no solicitado, que bloquea tráfico no solicitado en su camino desde una red de paquetes de datos hacia una red inalámbrica costosa.

### 25 Compendio de la invención

Las realizaciones de la presente invención dan a conocer procedimientos y dispositivos para filtrar datos entregados a un ordenador sobre un enlace unidireccional.

30 En las realizaciones de la presente invención, el camino físico entre un ordenador transmisor y un ordenador receptor se divide en partes que comprenden dos o más enlaces unidireccionales. Se sitúa entre los enlaces unidireccionales un dispositivo que sirve de motor de seguridad de los datos.

35 El ordenador transmisor está configurado para transmitir datos al motor de seguridad de los datos sobre un primer enlace unidireccional. El motor de seguridad de los datos puede estar configurado para validar datos llevando a cabo diversas verificaciones de seguridad, tal como verificar que los datos no incluyen virus u otro software malicioso. Las verificaciones de seguridad pueden incluir asimismo el filtrado de contenidos, que bloquea ciertos tipos de contenido, así como verificaciones asociadas con encapsulación de contenidos, tal como verificaciones para autenticar el origen de los datos.

40 Habitualmente, el motor de seguridad de los datos almacena los datos en memoria tampón mientras lleva a cabo las verificaciones de seguridad. Una vez que un conjunto de datos se ha validado, se transmite sobre un segundo enlace unidireccional al ordenador receptor. Los datos no válidos son rechazados. Las transmisiones sobre los enlaces unidireccionales se pueden configurar para que se produzcan en los tiempos designados, de tal modo que no se produzcan transmisiones al mismo tiempo sobre el primer y el segundo enlaces unidireccionales. Para una mayor seguridad, opcionalmente se pueden utilizar conmutadores, tal como relés, para conectar y desconectar físicamente cada enlace unidireccional, asegurando de ese modo que por lo menos una parte del camino físico está siempre desconectada. Un controlador de conmutadores puede estar configurado para controlar los conmutadores físicos. Los tiempos designados para transmisión sobre cada uno de los enlaces unidireccionales se pueden establecer mediante configuraciones predefinidas o, en otras realizaciones, mediante la transmisión de señales de control especiales al controlador de conmutadores desde el motor de seguridad de los datos o, alternativa o adicionalmente, desde el ordenador transmisor, el ordenador receptor o un origen externo. Conmutar físicamente cada enlace unidireccional impide además ataques contra el ordenador receptor mediante intrusos informáticos y mediante software malicioso.

50 Por lo tanto se da a conocer, de acuerdo con una realización de la presente invención, un procedimiento para comunicaciones seguras entre un ordenador transmisor y un ordenador receptor, incluyendo el procedimiento:

transmitir datos desde el ordenador transmisor sobre un primer enlace unidireccional a un motor de seguridad de los datos;

recibir y validar los datos en el interior del motor de seguridad de los datos; y

5 después de validar los datos, transmitir los datos desde el motor de seguridad de los datos al ordenador receptor sobre un segundo enlace unidireccional.

Habitualmente, transmitir los datos sobre el primer enlace unidireccional se lleva a cabo durante un primer periodo de tiempo, y transmitir los datos sobre el segundo enlace unidireccional se lleva a cabo durante un segundo periodo de tiempo posterior al primer periodo de tiempo y no solapado con el mismo. El primer periodo de tiempo puede ser uno de una secuencia de intervalos de tiempo que se definen en el ordenador transmisor y el motor de seguridad de los datos antes de transmitir los datos desde el ordenador transmisor. Antes del primer periodo de tiempo, se puede hacer funcionar un primer conmutador para conectar el primer enlace unidireccional y se puede hacer funcionar un segundo conmutador para desconectar el segundo enlace unidireccional; después del primer periodo de tiempo, se puede hacer funcionar el primer conmutador para desconectar el primer enlace unidireccional; y antes del segundo periodo de tiempo, se puede hacer funcionar el segundo conmutador para conectar el segundo enlace unidireccional. El funcionamiento del primer y el segundo conmutadores puede incluir controlar automáticamente los conmutadores utilizando un controlador de conmutadores. El control automático puede incluir enviar una señal de control desde el motor de seguridad de los datos al controlador de conmutadores. Alternativa o adicionalmente, el control automático puede incluir definir el primer y el segundo periodos de tiempo en el controlador de conmutadores antes de transmitir los datos desde el ordenador transmisor.

20 Validar los datos puede incluir determinar que los datos incluyen contenido no válido y rechazar el contenido no válido. En tal caso, se puede asimismo emitir una alarma.

Los medios de validación de los datos pueden incluir verificar los datos contra software malicioso, verificar los datos contra contenido inapropiado y autenticar el origen de los datos.

25 Se da a conocer además, de acuerdo con una realización de la presente invención, un aparato para comunicaciones seguras entre un ordenador transmisor y un ordenador receptor, incluyendo el aparato:

un motor de seguridad de los datos que tiene un puerto de transmisión y un puerto de recepción, y es operativo para recibir datos en el puerto de recepción, validar los datos, y entregar los datos en el puerto de transmisión después de ser validados;

30 un primer enlace unidireccional operativo para transmitir los datos desde el ordenador transmisor al puerto de recepción del motor de seguridad de los datos; y

un segundo enlace unidireccional operativo para transmitir los datos desde el puerto de transmisión del motor de seguridad de los datos al ordenador receptor.

35 El ordenador transmisor puede ser operativo para transmitir los datos sobre el primer enlace unidireccional durante un primer periodo de tiempo, y el ordenador intermedio puede ser operativo para transmitir los datos sobre el segundo enlace unidireccional durante un segundo periodo de tiempo posterior al primer periodo de tiempo y que no solapa con el mismo. El primer periodo de tiempo puede ser uno de una secuencia de intervalos de tiempo, que se definen mediante configuraciones en el ordenador transmisor y el motor de seguridad de los datos. Un primer conmutador puede ser operativo para conectar el primer enlace unidireccional antes del primer periodo de tiempo y para desconectar el primer enlace unidireccional a continuación del primer periodo de tiempo, y un segundo conmutador puede ser operativo para desconectar el segundo enlace unidireccional antes del primer periodo de tiempo y para conectar el segundo enlace unidireccional después del segundo periodo de tiempo. Un controlador de conmutadores puede estar configurado para hacer funcionar automáticamente el primer y el segundo conmutadores. El controlador de conmutadores puede estar acoplado para recibir una señal de control procedente del motor de seguridad de los datos, que define el primer y el segundo periodos de tiempo. Alternativa o adicionalmente, el controlador de conmutadores puede estar configurado con ajustes predefinidos que definen el primer y el segundo periodos de tiempo.

40 El motor de seguridad de los datos puede ser operativo para determinar que los datos incluyen contenido no válido y para rechazar el contenido no válido. El motor de seguridad de los datos puede asimismo ser operativo para emitir una alarma si determina que los datos incluyen contenido no válido.

50 El motor de seguridad de los datos puede ser operativo para validar los datos por medios que incluyen verificar los datos contra software malicioso, verificar los datos contra contenido inapropiado y autenticar un origen de los datos.

La presente invención se comprenderá mejor a partir de la siguiente descripción detallada de la misma, considerada junto con los dibujos, en los cuales:

### Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que muestra esquemáticamente un sistema para proteger un ordenador que recibe transmisiones unidireccionales, de acuerdo con una realización de la presente invención;

5 las fibras 2A-2C son ilustraciones esquemáticas de un ordenador transmisor, un ordenador intermedio y un ordenador receptor, respectivamente, de acuerdo con una realización de la presente invención;

la figura 3 es un diagrama de bloques que muestra esquemáticamente un sistema para proteger un ordenador que recibe transmisiones unidireccionales, de acuerdo con otra realización de la presente invención;

la figura 4 es una ilustración esquemática de un tablero de relés utilizado en un sistema para transmisiones unidireccionales, de acuerdo con una realización de la presente invención; y

10 la figura 5 es un diagrama de flujo de un proceso para transmitir datos a un ordenador que recibe transmisiones unidireccionales, de acuerdo con una realización de la presente invención.

### Descripción detallada de realizaciones

La figura 1 es un diagrama de bloques que muestra esquemáticamente un sistema 20 para proteger un ordenador 22 que recibe información desde un ordenador transmisor 24, de acuerdo con una realización de la presente invención. Un ordenador transmisor 24 y un ordenador receptor 22 pueden ser ordenadores de propósito general, que ejecutan cualesquiera sistemas operativos y software de aplicación adecuados. Alternativamente, uno o ambos de los ordenadores transmisor y receptor pueden ser dispositivos de procesamiento especializados, tales como dispositivos de almacenamiento o controladores industriales. El ordenador transmisor 24 está configurado para enviar al ordenador receptor datos cuyo contenido puede comprender archivos, correo electrónico, actualizaciones de software, grabaciones de archivos, información de internet, información de monitorización, registros de procesos industriales o sustancialmente cualquier otra clase de datos informáticos.

El ordenador transmisor 24 no transmite estos datos directamente al ordenador receptor 22 sino que, por el contrario, los transmite a un ordenador intermedio 26, que comprende un motor de seguridad de los datos. El ordenador intermedio 26 puede ser un ordenador de propósito general o de aplicación específica, y está habitualmente configurado para ejecutar software de seguridad de los datos descrito a continuación. Este software se puede descargar al ordenador intermedio en formato electrónico, sobre un enlace de comunicación adecuado, o puede alternativamente proporcionarse en un medio tangible, tal como un medio de memoria óptico, magnético o electrónico. El ordenador intermedio 26 puede almacenar en memoria tampón los datos recibidos del ordenador transmisor 24 y a continuación puede procesar los datos utilizando software de seguridad para determinar la validez de los datos.

El procesamiento mediante software de seguridad de los datos puede incluir determinar que el contenido recibido no comprende software malicioso, tal como un virus informático. El procesamiento puede incluir asimismo verificar que los datos sean conformes a protocolos predeterminados, que se pueden referir a la forma de encapsulamiento y/o a la forma de cifrado. El software de seguridad puede asimismo autenticar el origen de los datos verificando, por ejemplo, una firma digital. El software de seguridad puede asimismo llevar a cabo un filtrado de contenidos, en el que ciertos tipos de contenido, tal como pornografía, se etiquetan como no válidos.

Después del procesamiento mediante software de seguridad, el ordenador intermedio 26 transmite los datos validados al ordenador receptor.

La transmisión de los datos desde el ordenador transmisor 24 al ordenador intermedio 26 se realiza sobre un enlace unidireccional 28 del lado anterior. De manera similar, la transmisión de los datos validados desde el ordenador intermedio 26 al ordenador receptor 22 se realiza sobre un enlace unidireccional 30 del lado posterior. Los enlaces unidireccionales 28 y 30 pueden comprender cualquier medio de transmisión unidireccional. Por ejemplo, un medio unidireccional puede ser una conexión en serie RS-232 de corte. La conexión en serie RS-232 de corte proporciona sólo un cable a tierra y un cable desde una clavija de transmisión en el lado de transmisión de la conexión hasta una clavija de recepción en el lado de recepción, sin ningún camino inverso.

En una configuración alternativa, el medio unidireccional para cualquiera o ambos de los enlaces unidireccionales puede ser un par de comunicaciones transmisor-receptor, tal como el sistema propietario Waterfall, descrito en los antecedentes.

En una realización a modo de ejemplo, un par de comunicaciones transmisor-receptor puede comprender un dispositivo de transmisión 32 y un dispositivo de recepción 34. Una conexión entre el ordenador transmisor 24 y un dispositivo de transmisión 32 puede ser una conexión Ethernet estándar. De manera similar, una conexión entre el dispositivo de recepción 34 y el ordenador intermedio 26 puede ser una conexión Ethernet estándar. Los datos para transmitir desde el dispositivo de transmisión 32 al dispositivo de recepción 34 se pueden transmitir sobre una conexión RS-232 de corte, tal como se ha descrito anteriormente, o se pueden comunicar desde un transmisor óptico en el dispositivo de transmisión hasta un sensor óptico en el dispositivo de recepción, asegurando de ese modo que no hay ningún camino de comunicaciones en la dirección de retorno.

Los dispositivos 32 y 34 están alimentados habitualmente por una fuente de alimentación independiente de la señal transmitida, tal como alimentación por cable o alimentación por baterías.

Las figuras 2A-2C son diagramas de bloques que muestran esquemáticamente elementos del ordenador transmisor 24, el ordenador intermedio 26 y el ordenador receptor 22, de acuerdo con una realización de la presente invención. Tal como se indica en la figura 2A, el ordenador transmisor 24 incluye generalmente un procesador 40 que lleva a cabo funciones de acuerdo con instrucciones del software 42. Estas funciones pueden incluir recibir información en uno o varios puertos de entrada/salida (E/S) 44. Los puertos de E/S 44 pueden estar conectados a alimentadores de datos automatizados, de orígenes tales como procesos industriales o internet. Estos puertos pueden proporcionar medios para la introducción de datos locales de orígenes tales como medios de almacenamiento extraíble, un teclado o un escáner.

El procesador 40 transmite datos sobre el enlace unidireccional 28 del lado anterior desde un puerto de transmisión 46 al puerto de recepción 54 en el ordenador intermedio 26 (figura 2B). Tal como se describe a continuación haciendo referencia a la figura 3, el software 42 puede incluir configuraciones de tiempo que especifican periodos de tiempo designados para transmitir datos al ordenador intermedio 26. Los periodos de tiempo configurados para el ordenador transmisor 24 y para el ordenador intermedio 26 se pueden sincronizar utilizando procedimientos conocidos en la técnica, tal como internet o servicios radioeléctricos de configuración de señales horarias que están basados en relojes atómicos. Se proporciona un servicio de este tipo en [www.time.gov](http://www.time.gov) mediante el National Institute of Standards and Technology (NIST) de Estados Unidos.

Los periodos de tiempo designados se determinan generalmente especificando un intervalo de tiempo, tal como un período de segundos o minutos, durante el que se pueden transmitir datos, y especificando el subsiguiente intervalo durante el que no se deberían transmitir datos. Alternativamente, los periodos de tiempo designados se pueden especificar de otras formas, tal como proporcionando tiempos específicos con una periodicidad diaria o semanal, es decir, 10:00-11:00 a.m. diariamente, o proporcionando horas y fechas específicas. También alternativamente, el ordenador transmisor 24 y el ordenador intermedio 26 pueden transmitir de manera asíncrona, en cualquier momento deseado.

El ordenador intermedio 26, tal como se indica en la figura 2B, incluye habitualmente un procesador 50 que lleva a cabo funciones de acuerdo con las instrucciones de software 52. Estas funciones incluyen generalmente -recibir datos en- el puerto de recepción 54 y almacenar en memoria tampón estos datos en una memoria local 51. El software 52 incluye habitualmente software de seguridad de los datos, tal como se ha descrito anteriormente. El software 52 es ejecutado por un procesador 50 o por un procesador externo o complementario para determinar la validez de los datos recibidos. El ordenador intermedio 26 transmite datos que se ha determinado son válidos, sobre el enlace unidireccional 30 del lado posterior, desde un puerto de transmisión 56. Igual que el software 42 del ordenador transmisor 24, el software 52 se puede configurar con las mismas configuraciones temporales que especifican periodos de tiempo designados para transmitir datos. El software 52 se puede configurar asimismo con las mismas configuraciones temporales que designan los periodos de tiempo permitidos para recibir datos en el puerto de recepción 54. Alternativamente, tal como se ha indicado anteriormente, los ordenadores 24 y 26 pueden transmitir de manera asíncrona, en cuyo caso el ordenador intermedio puede transmitir datos inmediatamente después de validar los datos, incluso mientras recibe simultáneamente otros datos transmitidos por el ordenador transmisor.

El ordenador intermedio 26 puede estar configurado con un puerto de control 58, a través del cual el procesador 50 puede enviar señales sobre una línea de control 60, tal como se describe a continuación (figura 3). Pueden estar incluidos asimismo puertos E/S adicionales 62 en el ordenador intermedio 26, proporcionando de ese modo medios para gestionar, monitorizar y actualizar el software 52, incluyendo en el mismo aplicaciones de seguridad de los datos. Alternativa o adicionalmente, dichas actualizaciones se pueden transmitir al ordenador intermedio 26 a través del enlace unidireccional 28 del lado anterior.

El ordenador receptor 22, tal como se indica en la figura 2B, incluye generalmente un procesador 70 que lleva a cabo funciones de acuerdo con las instrucciones del software 72. Estas funciones incluyen recibir datos en el puerto de recepción 74 desde el enlace unidireccional 30 del lado posterior. El software 72 puede incluir asimismo funciones para procesar los datos recibidos y para almacenarlos en un almacenamiento de memoria 76. Habitualmente, los datos almacenados en el almacenamiento de memoria 76 son extremadamente confidenciales. Por consiguiente, los puertos E/S 78, que pueden estar incluidos en el ordenador receptor 22, pueden estar limitados al acceso de E/S local, tal como un acceso mediante una pantalla y un teclado de ordenador.

La figura 3 es un diagrama de bloques que muestra esquemáticamente un sistema 80 para proteger un ordenador que recibe transmisiones unidireccionales, de acuerdo con otra realización de la presente invención. Además de los elementos del sistema 20 descrito anteriormente, el sistema 80 incluyen un controlador 82 de conmutadores, que controla la conexión y desconexión física de los enlaces unidireccionales 28 y 30. En algunas realizaciones, los conmutadores 90 y 92 están introducidos en respectivos enlaces unidireccionales 28 y 30, de tal modo que estos enlaces pueden ser conectados y desconectados físicamente. Tal como se ha descrito anteriormente, los enlaces unidireccionales pueden comprender varios tipos de medios físicos, que incluyen medios eléctricos tal como una conexión RS-232 de corte o una conexión a internet, que pueden a su vez estar conectados a un par de

comunicaciones transmisor-receptor unidireccionales. Para los medios eléctricos, los conmutadores 90 y 92 se pueden implementar como relés mecánicos, tal como un relé de bobina indicado mediante la vista a mayor escala del conmutador 92 mostrado en la figura 3. Los conmutadores 90 y 92 se pueden implementar como relés unipolares de una dirección (SPST, single-pole, single-throw) o relés unipolares de múltiples direcciones (SPMT, single-pole, multiple-throw), en función del número de cables utilizados en el medio físico. Para los enlaces unidireccionales que llevan transmisiones digitales, los conmutadores 90 y 92 se pueden implementar asimismo como puertas lógicas digitales. Alternativamente, cuando un enlace unidireccional comprende un par de comunicaciones transmisor-receptor, tal como los dispositivos 32 y 34 (figura 1), un conmutador que controle el enlace puede funcionar controlando la alimentación a los dispositivos. Cuando alguno de los dispositivos se apaga, el enlace unidireccional se desconecta de manera efectiva.

Alternativamente, para enlaces unidireccionales que comprenden conexiones ópticas, los conmutadores 90 y 92 se pueden implementar como conmutadores ópticos. Los conmutadores ópticos conocidos en la técnica incluyen conmutadores optomecánicos, termoópticos y electroópticos.

El controlador 82 de conmutadores utiliza líneas de control 84 y 86 para controlar la apertura y el cierre de los respectivos conmutadores 90 y 92. Abrir un conmutador desconecta el enlace respectivo; cerrar el conmutador conecta el enlace.

El controlador 82 de conmutadores se puede implementar como un controlador lógico programable (PLC, programmable logic controller), tal como un ordenador de propósito general, o como algún dispositivo informático configurado de manera similar.

En algunas realizaciones, el controlador 82 de conmutadores está programado con configuraciones de tiempo designado utilizadas por el ordenador transmisor 24 y por el ordenador intermedio 26, tal como se ha descrito anteriormente. Durante el periodo de tiempo designado para transmisión sobre el enlace unidireccional 28 del lado anterior, el controlador 82 de conmutadores cierra el conmutador 90 y abre el conmutador 92. Durante el periodo de tiempo designado para transmisión sobre el enlace unidireccional 30 del lado posterior, el controlador 82 de conmutadores cierra el conmutador 92 y abre el conmutador 90. Por consiguiente, se impide físicamente que se produzca la transmisión simultáneamente sobre ambos enlaces unidireccionales.

En otra realización, el controlador 82 de conmutadores puede recibir señales de control de conmutador desde un origen externo, tal como un ordenador intermedio 26, que transmite dichas señales sobre la línea de control 60. Las señales de control de conmutador se pueden recibir alternativamente desde el ordenador transmisor 24 o desde el ordenador receptor 22, o desde otro dispositivo independiente.

Cuando el controlador 82 de conmutadores está configurado para recibir señales de control de conmutador, están definidas en general tres señales: una primera señal para conectar el enlace 28 y desconectar el enlace 30, una segunda señal para conectar el enlace 30 y desconectar el enlace 28, y una tercera señal para desconectar ambos enlaces. La temporización de estas señales puede estar determinada por un mensaje de modo de conmutación originado en el ordenador transmisor 24 y que define el periodo de tiempo de transmisión para una transmisión determinada. Habitualmente, este mensaje se entrega al ordenador intermedio 26. El ordenador intermedio puede enviar a continuación mensajes de control de conmutadores al controlador 82 de conmutadores en base a periodos de tiempo de transmisión configurados en el mensaje de modo de conmutación. El ordenador intermedio puede enviar asimismo una versión del mensaje de control de conmutadores al ordenador receptor 22, notificando de ese modo al ordenador receptor 22 el periodo de tiempo previsto para una transmisión determinada.

Por lo tanto, el controlador 82 de conmutadores puede funcionar de dos modos: un modo temporizado, en el que el control de conmutadores se determina mediante configuraciones de tiempo preestablecidas; y un modo de control externo, en el que el control de conmutadores se determina mediante señales de control recibidas de un origen externo, tal como el ordenador intermedio. El controlador de conmutadores puede estar configurado asimismo para funcionar en modo temporizado con una anulación del modo de control externo. Se describe a continuación el funcionamiento de estos modos.

La figura 4 es una ilustración esquemática de un tablero de relés 94 que comprende, como una sola unidad, un controlador 82 de conmutadores y conmutadores 90 y 92, de acuerdo con una realización de la presente invención. El tablero de relés 94 proporciona un medio cómodo de añadir elementos del sistema 80 a la configuración del sistema 20. Las líneas de control 84 y 86 son internas al tablero. El conmutador 90 está cableado a dos puertos en el tablero: un puerto de entrada 95, que puede estar conectado al enlace unidireccional 28 del lado anterior, y un puerto de salida 96, que puede estar conectado al puerto de recepción 54 del ordenador intermedio (figura 2B). De manera similar, el conmutador 92 está cableado a dos puertos, un puerto de entrada 97, que puede estar conectado al puerto de transmisión 56 del ordenador intermedio (figura 2B), y un puerto de salida 98, que puede estar conectado al enlace unidireccional 30 del lado posterior. La línea de control 60 desde el ordenador intermedio (figura 3) puede estar conectada a un puerto de entrada 99, que conecta con el controlador de conmutadores.

Los procedimientos para implementar las funciones del tablero de relés 94 en software en un ordenador de propósito general serán asimismo evidentes para los expertos en la materia.

La figura 5 es un diagrama de flujo de un proceso 100 para transmitir datos en el sistema 80 al ordenador receptor 22, de acuerdo con una realización de la presente invención. Cuando el controlador 82 de conmutadores funciona en modo temporizado, se inicia entonces una etapa 104 cuando se alcanza un tiempo designado inicial, que provoca que el controlador 82 de conmutadores cierre el conmutador 90, abriendo al mismo tiempo el conmutador 92.

5 Alternativamente, cuando el controlador de conmutadores funciona en modo de control externo, la etapa 104 se inicia cuando se recibe una señal de control mediante el controlador 82 de conmutadores desde el ordenador intermedio 26. El cierre del conmutador 90 conecta el enlace unidireccional del lado anterior entre el ordenador transmisor 24 y el ordenador intermedio 26.

10 El ordenador transmisor 24 está configurado habitualmente para comenzar la transmisión en un tiempo que está sincronizado con el cierre del conmutador 90. Esta transmisión se produce tal como se indica en la etapa 106. Durante la transmisión, el ordenador transmisor 24 puede enviar asimismo un mensaje de modo de conmutación al ordenador intermedio 26, que establece la duración temporal de la transmisión.

En paralelo o con posterioridad a la transmisión de la etapa 106, el ordenador intermedio 26 lleva a cabo, en la etapa 108, operaciones para validar el contenido de los datos transferidos. Estas operaciones, descritas anteriormente haciendo referencia a la figura 1, se pueden llevar a cabo mediante un procesador 50 o mediante un procesador auxiliar, interno o externo al ordenador intermedio. Si se determina que el contenido no es válido, al comprender, por ejemplo, software malicioso, entonces el ordenador intermedio no lleva a cabo operaciones subsiguientes asociadas con la transmisión de los datos al ordenador receptor 22 y, en lugar de esto, puede rechazar los datos no válidos o eliminar la parte no válida de los datos en la etapa 110. Alternativamente, el ordenador intermedio 26 puede archivar los datos no válidos para un análisis posterior. El ordenador intermedio 26 puede asimismo grabar en un registro la ocurrencia de datos no válidos y puede emitir una alarma.

15 20

Si el contenido de los datos es validado, entonces, en la etapa 114, el controlador 82 de conmutadores conecta el enlace unidireccional del lado posterior cerrando el conmutador 92, en la etapa 114. Para asegurar que la transmisión no se produce simultáneamente en ambos enlaces unidireccionales, el controlador de conmutadores abre asimismo el conmutador 90.

25

Si el controlador 82 de conmutadores funciona en modo temporizado, entonces la etapa 114 se inicia cuando se alcanza el tiempo designado. Alternativamente, cuando el controlador de conmutadores funciona en modo de control externo, la etapa 114 se inicia cuando se recibe una señal de control mediante el controlador 82 de conmutadores desde el ordenador intermedio 26.

30 A continuación, en la etapa 116, el ordenador intermedio 26 transmite los datos validados al ordenador receptor 22. Cuando ha transcurrido el periodo de tiempo designado para la transmisión (ya sea según un modo temporizado o un modo de control externo), el controlador de conmutadores abre el conmutador 92 en la etapa 118. En modo de control externo, la señal de control para abrir el conmutador 90 y el conmutador 92 se envía en la etapa 118. Alternativamente, se puede omitir la etapa 118, y el proceso 100 puede continuar en la etapa 104, con el cierre del conmutador 90 y la apertura simultánea del conmutador 92.

35

Aunque las realizaciones descritas anteriormente utilizan dos enlaces unidireccionales con un único ordenador intermedio, en realizaciones alternativas (no mostradas en las figuras), se pueden conectar en serie tres o más enlaces unidireccionales con múltiples ordenadores intermedios.

Además, aunque las realizaciones descritas anteriormente se refieren específicamente a ciertos tipos de funciones de seguridad que se aplican a contenido transmitido sobre un enlace unidireccional, se pueden llevar a cabo otros tipos de procesamiento de datos en un punto intermedio sobre un enlace unidireccional, de acuerdo con los principios de la presente invención. Los principios de la presente invención pueden ser aplicados análogamente en el contexto de otros entornos y otras tecnologías de comunicaciones.

40

Por lo tanto, se apreciará que las realizaciones descritas anteriormente se indican a modo de ejemplo, y que la presente invención no se limita a lo que se ha mostrado y descrito particularmente en lo anterior.

45

## REIVINDICACIONES

1. Un procedimiento para comunicaciones seguras entre un ordenador transmisor (24) y un ordenador receptor (22), comprendiendo el procedimiento:  
5 transmitir datos desde el ordenador transmisor (24) sobre un primer enlace (28) a un motor (26) de seguridad de los datos;  
recibir y validar los datos en el interior del motor (26) de seguridad de los datos; y  
después de validar los datos, transmitir los datos del motor (24) de seguridad de los datos al ordenador receptor (22) sobre un segundo enlace (30),  
estando el procedimiento **caracterizado por que**  
10 tanto la transmisión desde el ordenador transmisor (24) al motor de seguridad (26) por medio del primer enlace (28) como desde el motor de seguridad (26) al ordenador receptor (22) por medio del segundo enlace (30) se llevan a cabo sobre enlaces unidireccionales de un medio de transmisión unidireccional, que no tienen ningún camino inverso.  
15 2. El procedimiento según la reivindicación 1, en el que transmitir los datos sobre el primer enlace unidireccional (28) se lleva a cabo durante un primer periodo de tiempo y transmitir los datos sobre el segundo enlace unidireccional (30) se lleva a cabo durante un segundo periodo de tiempo posterior al primer periodo de tiempo y no solapado con el mismo.  
3. El procedimiento según la reivindicación 2, en el que el primer periodo de tiempo es uno de una secuencia de intervalos de tiempo, y que comprende definir las secuencias de intervalos de tiempo en el ordenador transmisor (24) y el motor de seguridad de los datos (26) antes de transmitir los datos al ordenador transmisor (24).  
20 4. El procedimiento según la reivindicación 2, y que comprende:  
antes del primer periodo de tiempo, hacer funcionar un primer conmutador para conectar el primer enlace unidireccional (28) y hacer funcionar un segundo conmutador para desconectar un segundo enlace unidireccional (30);  
25 a continuación del primer periodo de tiempo, hacer funcionar el primer conmutador para desconectar el primer enlace unidireccional (28); y  
antes del segundo periodo de tiempo, hacer funcionar el segundo conmutador para conectar el segundo enlace unidireccional (30).  
30 5. El procedimiento según la reivindicación 4, en el que hacer funcionar el primer y el segundo conmutadores comprende controlar automáticamente los conmutadores utilizando un controlador de conmutadores.  
6. El procedimiento según la reivindicación 5, en el que controlar los conmutadores comprende enviar una señal de control desde el motor (26) de seguridad de los datos al controlador de conmutadores.  
7. El procedimiento según la reivindicación 5, en el que controlar los conmutadores comprende definir el primer y el segundo periodos de tiempo en el controlador de conmutadores antes de transmitir los datos desde el ordenador transmisor (24).  
35 8. El procedimiento según cualquiera de las reivindicaciones 1 a 7, en el que validar los datos comprende determinar que los datos comprenden contenido no válido y rechazar el contenido no válido.  
9. El procedimiento según cualquiera de las reivindicaciones anteriores, en el que el motor (26) de seguridad de los datos no tiene medios para enviar comunicaciones de retorno al ordenador transmisor (24) y el ordenador receptor (22) no tiene medios para enviar comunicaciones de retorno al motor (26) de seguridad de los datos.  
40 10. El procedimiento según cualquiera de las reivindicaciones 1 a 7, en el que validar los datos comprende verificar los datos contra software malicioso.  
11. El procedimiento según cualquiera de las reivindicaciones 1 a 7, en el que el enlace unidireccional (28, 30) comprende enlaces cableados u ópticos.  
45 12. El procedimiento según cualquiera de las reivindicaciones 1 a 7, en el que validar los datos comprende autenticar un origen de los datos.  
13. Sistema (20) para comunicaciones seguras entre un ordenador transmisor (24) y un ordenador receptor (22), comprendiendo el sistema:



un motor (26) de seguridad de los datos que tiene un puerto de transmisión (56) y un puerto de recepción (54), y es operativo para recibir datos en el puerto de recepción, validar los datos, y entregar los datos en el puerto de transmisión después de ser validados;

5 un primer enlace (28) operativo para transmitir los datos desde el ordenador transmisor (24) al puerto de recepción del motor (26) de seguridad de los datos; y

un segundo enlace (30) operativo para transmitir los datos desde el puerto de transmisión del motor (26) de seguridad de los datos al ordenador receptor (22),

**caracterizado por que**

10 el primer y el segundo enlaces (28, 30) son enlaces unidireccionales de un medio de transmisión unidireccional, que no tienen ningún camino inverso.

14. El sistema según la reivindicación 13, en el que el ordenador transmisor (24) es operativo para transmitir los datos sobre el primer enlace unidireccional (28) durante un primer periodo de tiempo, y en el que el motor de seguridad (26) es operativo para transmitir los datos sobre el segundo enlace unidireccional durante un segundo periodo de tiempo subsiguiente al primer periodo de tiempo y que no solapa con el mismo.

15 15. El sistema según la reivindicación 13 ó 14, en el que el motor (26) de seguridad de los datos es operativo para determinar que los datos comprenden contenido no válido y para rechazar el contenido no válido.

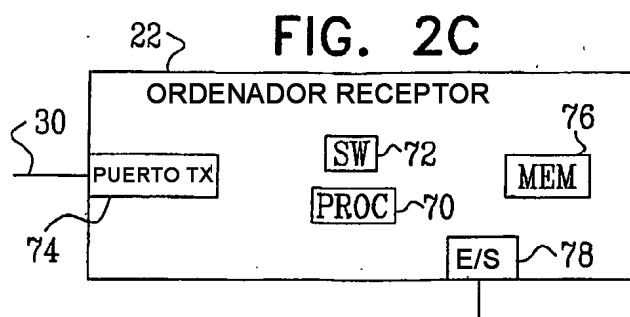
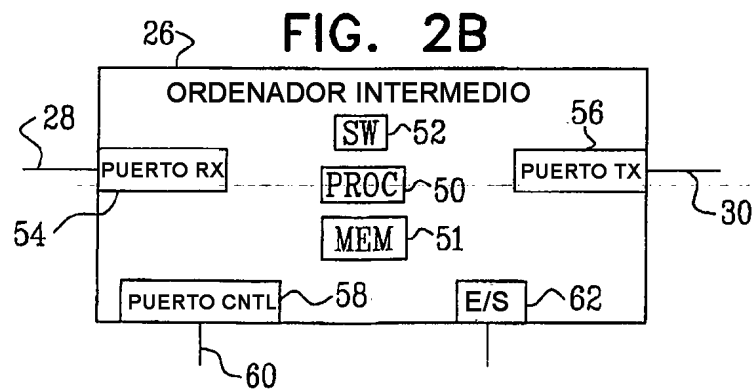
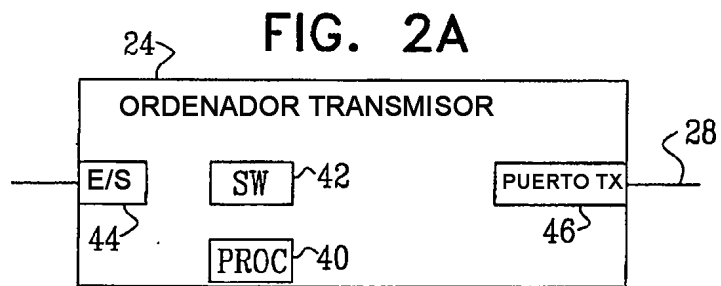
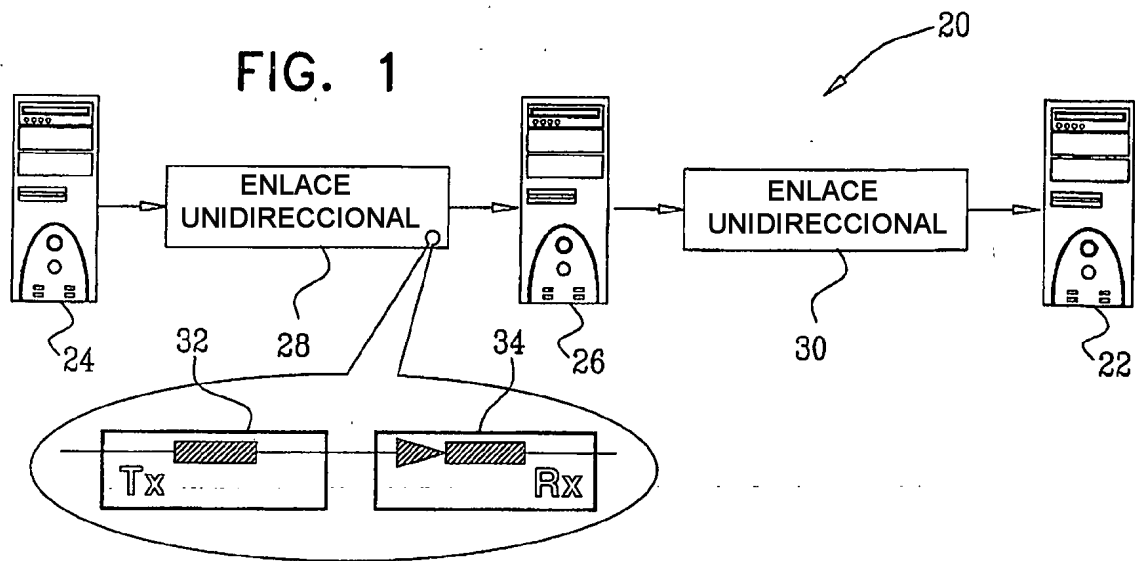


FIG. 3

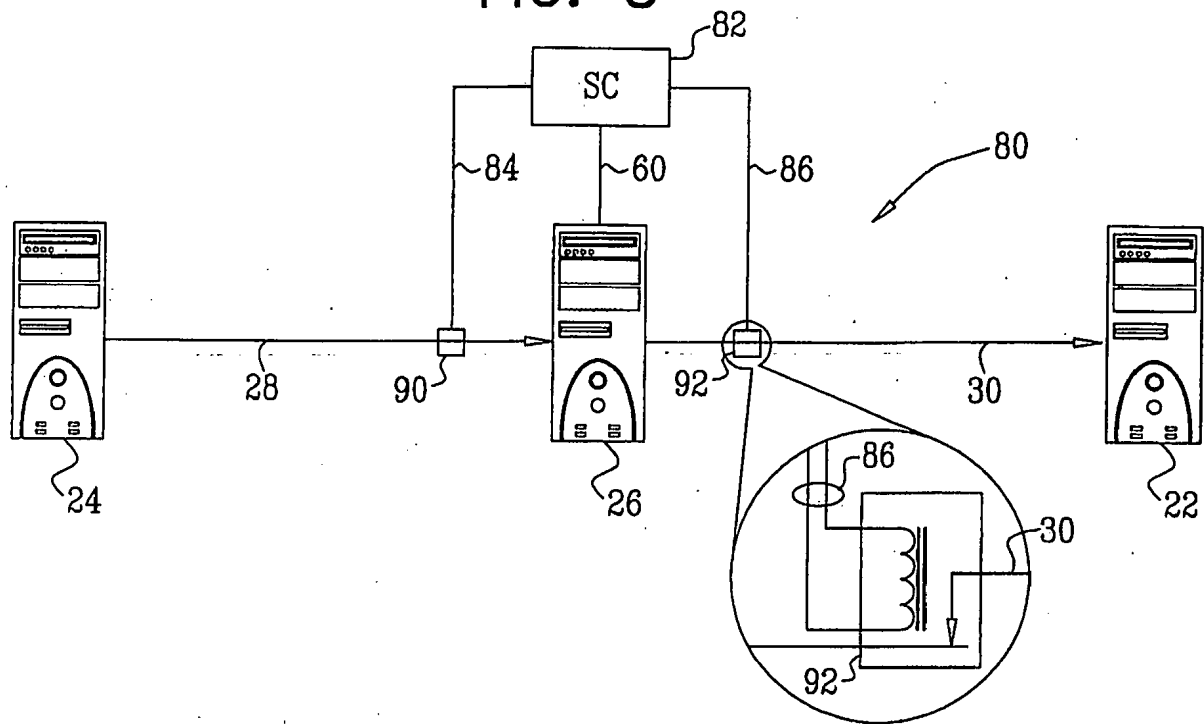


FIG. 4

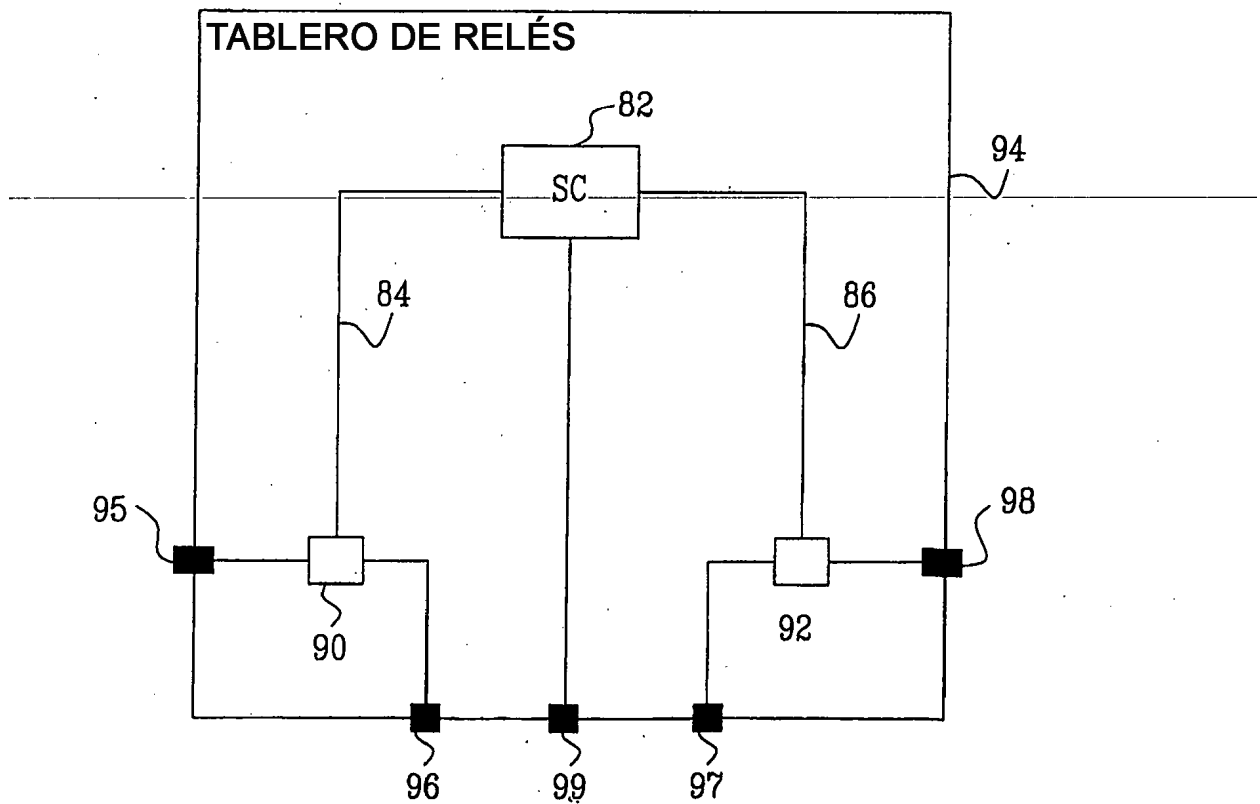


FIG. 5

