(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 748 229**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.01.2017 E 17151095 (1)**

(97) Fecha y número de publicación de la concesión europea: **10.07.2019 EP 3206365**

(54) Título: **Sistema y método de comunicaciones**

(30) Prioridad:

14.02.2016 US 201662295074 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.03.2020

(73) Titular/es:

WATERFALL SECURITY SOLUTIONS LTD. (100.0%)
14 Hamelacha Street, Afek Industrial Park
Rosh HaAyin 4809133, IL

(72) Inventor/es:

FRENKEL, LIOR

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método de comunicaciones

La presente invención se refiere a un sistema y un método de comunicaciones. La invención se refiere, en general, a comunicaciones y control digital, y particularmente a sistemas y métodos para comunicaciones seguras. En realizaciones, la invención se refiere a una conexión segura con instalaciones protegidas.

En una red informática que gestiona procesos físicos o datos sensibles, porciones de la red pueden estar conectadas por enlaces unidireccionales. El término “enlace unidireccional” se usa en el contexto de la presente solicitud de patente y en las reivindicaciones para referirse a un enlace de comunicación que está configurado físicamente para transportar señales en una dirección y ser incapaz de transportar señales en la dirección opuesta. Se pueden implementar enlaces unidireccionales, por ejemplo, utilizando los sistemas Waterfall®, que están fabricados por Waterfall Security Solutions, Ltd. (Rosh HaAyin, Israel). El sistema Waterfall proporciona una conexión unidireccional física basada en la comunicación por fibra óptica, utilizando un protocolo subyacente de transferencia patentado. Cuando un ordenador transmisor está conectado por un sistema Waterfall (u otro enlace unidireccional) a un ordenador receptor, el ordenador receptor puede recibir datos del ordenador transmisor, pero no tiene medios físicos para enviar comunicaciones de retorno al ordenador transmisor.

Se pueden usar enlaces unidireccionales para evitar que los datos entren o salgan de una instalación protegida. Por ejemplo, los datos confidenciales a los que no se debe acceder desde sitios externos pueden almacenarse en un ordenador que está configurado para recibir datos a través de un enlace unidireccional y que no tiene un enlace saliente físico sobre el cual los datos puedan transmitirse a un sitio externo. Por otro lado, en algunas aplicaciones, la empresa explotadora de la instalación protegida puede estar preparada para permitir que los datos salgan libremente de la instalación a través de un enlace unidireccional, al tiempo que evita que los datos ingresen a la instalación para frustrar a los piratas informáticos y los ciberterroristas. A diferencia de los cortafuegos convencionales, los enlaces unidireccionales permiten que la información salga de una instalación protegida sin riesgo para la seguridad o la disponibilidad de la red en la instalación por los ataques que se originan en una red externa. En la práctica, sin embargo, a veces es necesario volver a transmitir al menos pequeñas cantidades de información desde una red externa a la instalación protegida.

La publicación de solicitud de patente estadounidense 2014/0068712 describe aparatos y métodos para controlar automáticamente las entradas a un destino protegido. En una realización descrita, el aparato de comunicaciones incluye un retransmisor de datos unidireccional activado por soporte físico, que incluye una primera interfaz de soporte físico configurada para recibir una instrucción desde una red de comunicaciones y una segunda interfaz de soporte físico configurada para transmitir la instrucción recibida a un destino protegido cuando el retransmisor es activado. Un decodificador incluye una tercera interfaz de soporte físico configurada para recibir de la red de comunicaciones una firma digital para la instrucción, y la lógica de decodificación de soporte físico acoplada para verificar la firma digital y activar el retransmisor al verificar la firma digital, por lo que la instrucción se transmite a través de la interfaz del segundo soporte físico al destino protegido.

La publicación de solicitud de patente estadounidense 2016/0112384 describe un método de comunicaciones que incluye recibir en una instalación segura, a través de una red desde un terminal de usuario remoto, una entrada que comprende una secuencia de símbolos que se ha cifrado utilizando una clave de cifrado preseleccionada. El flujo cifrado de símbolos se decodifica en la instalación segura utilizando una clave de descifrado correspondiente a la clave de cifrado preseleccionada, para producir un flujo de símbolos en claro. Un programa informático que se ejecuta en un procesador en la instalación segura se usa para procesar los símbolos en la secuencia en claro y generar una salida gráfica en un formato de visualización predefinido en respuesta al procesamiento de los símbolos. La salida gráfica se emite desde la instalación segura a la red en un formato sin cifrar para mostrarla en el terminal de usuario remoto.

El documento US-A-2013097283 describe un sistema de comunicaciones, que incluye una estación, que incluye unas interfaces primera y segunda configuradas para conectarse a una red de paquetes de datos y tener respectivas direcciones diferentes de red primera y segunda, y un terminal, que incluye unas interfaces tercera y cuarta configuradas para conectarse a la red de paquetes de datos y tener respectivas direcciones diferentes de red tercera y cuarta. La estación está configurada para transmitir primeros datos al terminal por una primera ruta a través de la red de paquetes de datos dirigida desde la primera interfaz a la tercera dirección de red, mientras que el terminal está configurado para transmitir segundos datos a la estación por una segunda ruta a través del paquete red de datos dirigida desde la cuarta interfaz a la segunda dirección de red. Los dispositivos delegados primero y segundo de protocolo de control de transmisión (TCP) se implementan respectivamente en la estación y en el terminal, y están configurados para emular una conexión TCP entre la estación y el terminal mediante la transmisión de tramas TCP desde la estación al terminal solo a través de la primera ruta y desde el terminal a la estación solo a través de la segunda ruta.

En algunas realizaciones, la estación incluye un primer enlace unidireccional saliente conectado entre el primer dispositivo delegado TCP y la primera interfaz y un primer enlace unidireccional entrante conectado entre la segunda interfaz y el primer dispositivo delegado TCP. En una realización divulgada, el terminal incluye un segundo enlace

unidireccional saliente conectado entre el segundo dispositivo delegado TCP y la cuarta interfaz y un segundo enlace unidireccional entrante conectado entre la tercera interfaz y el segundo dispositivo delegado TCP.

De manera adicional o alternativa, la estación incluye unas centralitas primera y segunda, que se acoplan entre los enlaces unidireccionales saliente y entrante y el primer dispositivo delegado TCP y están configuradas para conectar el primer dispositivo delegado TCP a la red de paquetes de datos a través enlaces de una dirección saliente y entrante solo cuando la conexión TCP emulada está en uso. Normalmente, la estación incluye un ordenador central (anfitrión), que está configurado para transmitir y recibir paquetes de datos hacia y desde la red de paquetes de datos a través de los enlaces unidireccionales saliente y entrante, respectivamente, y que está acoplado al primer dispositivo delegado TCP para transmitir y recibir datos a través de la conexión TCP emulada. Las centralitas primera y segunda están configuradas para aislar el primer dispositivo delegado TCP cuando la conexión TCP emulada no está en uso y para transportar paquetes de datos entrantes desde el enlace unidireccional entrante al ordenador anfitrión y transmitir paquetes de datos salientes desde el ordenador al enlace saliente unidireccional, sin pasar por el primer dispositivo delegado TCP. En una realización divulgada, la estación incluye un módulo de seguridad de soporte físico (HSM), que está acoplado para controlar la activación de las centralitas.

Además, de forma adicional o alternativa, el terminal incluye un módulo de soporte de protocolo seguro, que incluye un módulo de seguridad de soporte físico (HSM) en el que se ejecuta el segundo dispositivo delegado TCP. En algunas realizaciones, la activación del HSM para emular la conexión TCP está condicionada a la presentación de una credencial de soporte físico al HSM.

En algunas realizaciones, el módulo de soporte de protocolo seguro incluye una primera centralita, que está acoplada entre la tercera interfaz y el HSM, y una segunda centralita, que está acoplada entre la cuarta interfaz y el HSM, y en el que las centralitas primera y segunda están configuradas para conectar el HSM a la red de paquetes de datos a través de las interfaces tercera y cuarta solo cuando la conexión TCP emulada esté en uso. En una realización divulgada, el terminal incluye un procesador anfitrión, que está configurado para recibir y transmitir paquetes de datos desde y hacia la red de paquetes de datos a través de las interfaces tercera y el terminal, y están configurados para emular una conexión TCP entre la estación y el terminal mediante la transmisión de tramas TCP desde la estación al terminal solo a través de la primera ruta y desde el terminal a la estación solo a través de la segunda ruta. La estación comprende un primer enlace unidireccional saliente conectado entre el primer dispositivo delegado TCP y la primera interfaz y un primer enlace unidireccional entrante conectado entre la segunda interfaz y el primer dispositivo delegado TCP. Los enlaces unidireccionales están configurados físicamente para transportar señales en una dirección y ser incapaces de transportar señales en la dirección opuesta. El documento US-A-2013097283 también describe un método de comunicaciones, que comprende conectar una estación a una red de paquetes de datos a través de interfaces primera y segunda que tienen respectivas direcciones diferentes de red primera y segunda; conectar un terminal a la red de paquetes de datos a través de una interfaces tercera y cuarta que tienen respectivas direcciones diferentes de red tercera y cuarta; y emular una conexión de protocolo de control de transmisión (TCP) entre la estación y el terminal transmitiendo las primeras tramas TCP desde un primer dispositivo delegado TCP implementado en la estación a un segundo dispositivo delegado TCP implementado en el terminal solo sobre una primera ruta a través de la red de paquetes de datos dirigida desde la primera interfaz a la tercera dirección de red, y transmitiendo las segundas tramas TCP desde el segundo dispositivo delegado TCP en el terminal al primer dispositivo delegado TCP en la estación solo a través de una segunda ruta a través de la red de paquetes de datos dirigida desde la cuarta interfaz a la segunda red dirección; comprendiendo la conexión de la estación conectar un primer enlace unidireccional saliente entre el primer dispositivo delegado TCP y la primera interfaz y un primer enlace unidireccional entrante entre la segunda interfaz y el primer dispositivo delegado TCP; estando configurados los enlaces unidireccionales físicamente para transportar señales en una dirección y para ser incapaces de transportar señales en la dirección opuesta.

Las realizaciones de la presente invención que se describen a continuación proporcionan aparatos y métodos para una comunicación segura con una instalación protegida.

Por lo tanto, se proporciona, según un aspecto de la invención, un sistema de comunicaciones como se describe en el documento US-A-2013097283, caracterizado porque la estación comprende unas centralitas primera y segunda, que se acoplan entre los enlaces unidireccionales salientes y entrantes y el primer dispositivo delegado TCP y están configuradas para conectar el primer dispositivo delegado TCP a la red de paquetes de datos a través de enlaces unidireccionales salientes y entrantes solo se vincula cuando la conexión TCP emulada está en uso.

En una realización divulgada, el terminal incluye un segundo enlace unidireccional saliente conectado entre el segundo dispositivo delegado TCP y la cuarta interfaz y un segundo enlace unidireccional entrante conectado entre la tercera interfaz y el segundo dispositivo delegado TCP.

Normalmente, la estación incluye un ordenador anfitrión, que está configurado para transmitir y recibir paquetes de datos hacia y desde la red de paquetes de datos a través de los enlaces unidireccionales salientes y entrantes, respectivamente, y que está acoplado al primer dispositivo delegado TCP para transmitir y recibir datos a través de la conexión TCP emulada. Las centralitas primera y segunda están configuradas para aislar el primer dispositivo delegado TCP cuando la conexión TCP emulada no está en uso y para transportar paquetes de datos entrantes desde el enlace unidireccional entrante al ordenador anfitrión y transmitir paquetes de datos salientes desde el ordenador al

enlace saliente unidireccional, sin pasar por el primer dispositivo delegado TCP. En una realización divulgada, la estación incluye un módulo de seguridad de soporte físico (HSM), que está acoplado para controlar la activación de las centralitas.

Además, de forma adicional o alternativa, el terminal incluye un módulo de soporte de protocolo seguro, que incluye un módulo de seguridad de soporte físico (HSM) en el que se ejecuta el segundo dispositivo delegado TCP. En algunas realizaciones, la activación del HSM para emular la conexión TCP está condicionada a la presentación de una credencial de soporte físico al HSM.

En algunas realizaciones, el módulo de soporte de protocolo seguro incluye una primera centralita, que está acoplada entre la tercera interfaz y el HSM, y una segunda centralita, que está acoplada entre la cuarta interfaz y el HSM, y en el que las centralitas primera y segunda están configuradas para conectar el HSM a la red de paquetes de datos a través de las interfaces tercera y cuarta solo cuando la conexión TCP emulada esté en uso. En una realización divulgada, el terminal incluye un procesador anfitrión, que está configurado para recibir y transmitir paquetes de datos desde y hacia la red de paquetes de datos a través de las interfaces tercera y cuarta, respectivamente, y que está acoplado al HSM para transmitir y recibir datos a través de la conexión TCP emulada. Las centralitas primera y segunda están configuradas para aislar el segundo dispositivo delegado TCP cuando la conexión TCP emulada no está en uso y para transportar paquetes de datos entrantes desde la tercera interfaz al procesador anfitrión y transmitir paquetes de datos salientes desde el procesador anfitrión a la cuarta interfaz, sin pasar por el HSM.

También se proporciona, según un aspecto de la invención, un método de comunicaciones descrito en el documento US-A-2013097283, caracterizado por conectar la estación que, además, comprende activar las centralitas primera y segunda, acopladas respectivamente entre los enlaces unidireccionales salientes y entrantes y el primer dispositivo delegado TCP, para conectar el primer dispositivo delegado TCP a la red de paquetes de datos a través de los enlaces unidireccionales salientes y entrantes solo cuando la conexión TCP emulada está en uso.

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

la figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema para la monitorización y el control seguros, según una realización de la presente invención; y

la figura 2 es un diagrama de bloques que muestra esquemáticamente detalles del terminal de usuario remoto, según una realización de la presente invención.

Como se señaló anteriormente, un enlace unidireccional saliente desde una instalación protegida es un medio eficaz para permitir que la información salga de una instalación protegida sin riesgo para la seguridad o la disponibilidad de la red en la instalación debido a ataques que se originen en una red externa. Sin embargo, en la práctica, a veces es necesario volver a transmitir al menos pequeñas cantidades de información desde una red externa a la instalación protegida, como instrucciones, actualizaciones de soporte lógico o cambios de configuración a sitios remotos desatendidos o instalaciones de fabricación. Hay una serie de riesgos asociados con tales comunicaciones. Un riesgo es que si el programa maligno se ha introducido de alguna manera en la red protegida (posiblemente por colaboración de un empleado con acceso a la misma), las comunicaciones de regreso a la red protegida podrían ser utilizadas para desencadenar un ataque. Otro riesgo es que un atacante podría obtener capacidades de control remoto a través de un sistema dentro de la red protegida o podría usar el canal de comunicaciones de la instalación para causar condiciones inseguras o poco fiables en la red protegida; por ejemplo, mediante un ataque de desbordamiento de la antememoria.

La publicación de solicitud de patente estadounidense 2014/0068712 mencionada anteriormente describe una posible solución a estos problemas, permitiendo un flujo controlado de pequeñas cantidades de información en una red protegida. El flujo se controla automáticamente para que los ataques basados en soporte lógico en equipos protegidos sean difíciles o imposibles de llevar a cabo aunque partes del sistema de instrucciones y comunicaciones se ven comprometidas. A diferencia de los cortafuegos convencionales, el control se lleva a cabo mediante lógica de soporte físico, en lugar de soporte lógico. En consecuencia, los atacantes remotos no pueden cambiar la configuración operativa de la lógica de protección ni hacer que realice ninguna función distinta de las programadas inicialmente por el diseñador de la lógica. En las realizaciones descritas, la lógica del soporte físico está configurada para controlar el formato y el contenido de las instrucciones que pueden enviarse a un destino protegido. La lógica del soporte físico también puede autenticar estas instrucciones para garantizar que fueron producidas por un transmisor autorizado. Como resultado, al comprometer a un transmisor autorizado, un atacante puede, en el peor de los casos, enviar una instrucción incorrecta al destino, pero no podrá obtener el control sobre la instalación protegida.

La publicación de solicitud de patente estadounidense 2016/0112384, también citada anteriormente, lleva este modelo un paso más allá para proporcionar una funcionalidad segura de escritorio remoto, al tiempo que mantiene un alto nivel de seguridad contra el acceso no autorizado. Estas realizaciones usan componentes de soporte físico para separar la entrada de un terminal de usuario remoto a la instalación segura de la salida de pantalla gráfica que proporciona la instalación y, por lo tanto, evitan crear un bucle cerrado de comunicaciones que podría ser aprovechado por una persona maliciosa. La entrada a la instalación segura comprende una secuencia de símbolos que ha sido

cifrada por el terminal de usuario remoto utilizando una clave de cifrado preseleccionada. Un decodificador en la instalación segura vuelve a convertir la entrada cifrada en un flujo de símbolos en claro, utilizando una clave de descifrado correspondiente. Por lo tanto, solo se puede acceder a la funcionalidad de escritorio remoto de la instalación segura mediante un dispositivo cliente que posea la clave de cifrado adecuada. Para mayor seguridad, el flujo de símbolos cifrados puede generarse usando un codificador basado en soporte físico en un dispositivo de entrada seguro del terminal de usuario remoto.

Los tipos de funcionalidad de control remoto que se describen en las publicaciones anteriores dependen del operario humano del terminal de usuario para “cerrar el bucle” entre la información recibida por el terminal desde la instalación protegida y la entrada transmitida desde el terminal de regreso a la instalación. El flujo de entrada a la instalación protegida se transmite desde un puerto del terminal de usuario a un puerto correspondiente de la instalación protegida a través de una ruta de red determinada, mientras que la salida de la pantalla normalmente atraviesa una ruta de red diferente entre un par diferente de puertos. (La separación de los puertos se aplica en la instalación protegida, y las rutas son determinadas de forma independiente por dispositivos de encaminamiento en la red entre el terminal y la instalación protegida, como dispositivos de encaminamiento de protocolo de Internet [IP]). Esta segregación de las dos direcciones de comunicación palia muchos de los riesgos de seguridad que de otro modo estarían involucrados en la interacción bidireccional con la instalación protegida, ya que impide el establecimiento de conexiones de protocolo de proceso a proceso, como los interfaces de conexión del protocolo de control de transmisión (TCP), que generalmente se requieren para interacciones cliente/servidor y entre dispositivos del mismo nivel.

Sin embargo, en algunos casos, se requiere una conexión de protocolo bidireccional real entre la instalación protegida y un terminal remoto u otro ordenador. Tal conexión puede ser necesaria, por ejemplo, para actualizar el soporte lógico que se ejecuta en la instalación protegida, tanto durante la actualización como después, para permitir la verificación del funcionamiento adecuado, particularmente cuando la instalación se encuentra en una ubicación remota sin personal cualificado (o posiblemente sin personal) *in situ*. También se puede necesitar una conexión bidireccional en situaciones de emergencia, de modo que la sede central pueda ejercer un control total, directo y sin restricciones del sitio por razones operativas y de seguridad.

Las realizaciones de la presente invención que se describen en el presente documento permiten la creación de una conexión de protocolo bidireccional a través de un par de tramos unidireccionales separados en una red, mientras se mantiene un alto nivel de protección basada en soporte físico contra el aprovechamiento malicioso de la conexión. Estas realizaciones se basan en un dispositivo delegado TCP, que es capaz de abrir y mantener una conexión TCP con un dispositivo remoto del mismo nivel mientras recibe paquetes TCP entrantes del dispositivo del mismo nivel por un puerto de entrada con una dirección dada de protocolo de Internet (IP) y transmite paquetes TCP salientes al dispositivo remoto del mismo nivel a través de un puerto de salida con una dirección IP diferente. El dispositivo delegado TCP emula el funcionamiento de TCP a través de un puerto IP bidireccional convencional, de modo que las aplicaciones de soporte lógico que se ejecutan en un procesador anfitrión en cualquier extremo de la conexión TCP pueden transmitir y recibir comunicaciones a través del dispositivo delegado TCP como si fuera una pila de soporte lógico de TCP convencional.

Dichos dispositivos delegados TCP pueden instalarse en uno o ambos extremos del enlace TCP; por ejemplo, tanto en una instalación protegida como en un terminal de usuario remoto que se comunica con la instalación. Para una mayor seguridad, el dispositivo delegado TCP se puede instalar y ejecutar dentro de módulos de soporte físico resistentes a los ataques, como un módulo de seguridad de soporte físico (HSM). Como medida de seguridad adicional o alternativa, el dispositivo delegado TCP recibe los paquetes entrantes del puerto de entrada a través de un enlace unidireccional entrante y transmite los paquetes salientes al puerto de salida a través de un enlace unidireccional saliente separado.

En una realización ejemplar que se describe más adelante en el presente documento, se instala un dispositivo delegado TCP de ese tipo en una instalación protegida y segura, y el otro en un terminal de usuario remoto. En el funcionamiento normal de este sistema, como se explicó anteriormente, la instalación segura transmite datos al terminal del usuario a través de una ruta unidireccional a través de una red, mientras que el terminal del usuario transmite instrucciones a la instalación segura a través de una ruta unidireccional separada, con segregación impuesta por enlaces unidireccionales tanto en la instalación segura como en el terminal de usuario. Durante dicha operación normal, los dispositivos delegados TCP están aislados de los enlaces unidireccionales y, por lo tanto, de la red, mediante circuitos de conmutación impuestos por soporte físico.

Por ejemplo, la conexión de los dispositivos delegados TCP a la red puede estar sujeta a la activación de un modelo de seguridad de soporte físico (HSM) en el terminal de usuario, que puede ser el mismo HSM en el que se ejecuta el dispositivo delegado TCP o un HSM separado que se proporciona para este fin. Como resultado, la conexión TCP a la instalación segura estará disponible solo cuando sea activada físicamente por un usuario del terminal con las credenciales criptográficas de soporte físico requeridas, y la conexión no está expuesta en ningún otro momento a un aprovechamiento por parte de atacantes en otra parte de la red. Cuando el HSM no está activado, el propio código del dispositivo delegado TCP está cifrado y es inaccesible desde la red y, por lo tanto, no se puede aprovechar para abrir la conexión bidireccional entre el terminal de usuario y la instalación segura en ausencia de personal autorizado con las credenciales criptográficas necesarias.

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema 20 para la monitorización y el control seguros, según una realización de la presente invención. En este ejemplo, el sistema 20 comprende un terminal 24 de usuario, que se usa para monitorizar y controlar una instalación segura; por ejemplo, una estación 22 de control de servicios públicos, tal como una estación de transmisión y conmutación de una compañía de energía eléctrica. El terminal 24 se comunica con la estación 22 a través de una red 26 de área amplia, que puede comprender cualquier red cableada o inalámbrica adecuada, o una combinación de tales redes, incluidas redes públicas, tales como la Internet pública. La estación 22 normalmente comprende una red interna 40 de control, que incluye elementos operativos, tales como centralitas, que crean, interrumpen y regulan las conexiones de alimentación, así como componentes de monitorización, como sensores. Aunque por simplicidad, solo se muestra una única estación 22 en la Fig. 1, en la práctica, las empresas de servicios públicos generalmente operan muchas de tales estaciones. En muchos sistemas reales, las estaciones 22 no están atendidas *in situ*, y se monitorizan y controlan de forma remota, utilizando un único enlace saliente para transmitir datos para la monitorización. En la presente realización, la estación 22 está controlada por el terminal 24 de usuario remoto, y ofrece la funcionalidad de dispositivo delegado TCP cuando se requiere para este fin, como se describe en la presente memoria.

Aunque el ejemplo ilustrado se refiere, a modo de ilustración, a una red eléctrica, los principios de la presente invención no se limitan a este contexto operativo particular. Por el contrario, el aparato y los métodos que se describen a continuación se pueden aplicar a servicios públicos de otros tipos (como los servicios de gas o agua, por ejemplo), así como en entornos industriales y sustancialmente cualquier otra aplicación en la que se deba ejercer un control estricto sobre datos e instrucciones que puedan introducirse en una instalación protegida. La estación 22 es solo un ejemplo de dicha instalación. Se describen a continuación ciertas realizaciones de la presente invención, en aras de la claridad y sin limitación, con respecto a los elementos del sistema 20, pero los principios de estas realizaciones y las técnicas que incorporan pueden aplicarse de manera similar en otros entornos operativos en los que una instalación deba ser protegida contra la entrada de datos no deseados y el acceso no autorizado.

La estación 22 está diseñada normalmente como una instalación cerrada y segura, protegida físicamente contra la entrada no autorizada. Un ordenador anfitrión 41 en la estación 22 introduce instrucciones a las centralitas en la red 40 y monitoriza el funcionamiento de las centralitas y otros componentes de la estación. Normalmente, la red 40 comprende múltiples sensores y activadores, que se distribuyen a través de la estación 22 e informan a través de una red interna segura al ordenador principal 41. El ordenador 41 emite información, incluyendo posiblemente una salida de pantalla gráfica, a través de un enlace unidireccional 34 a una interfaz 38 de salida. La interfaz 38 de salida está conectada a la red 26, que transmite la información de salida al terminal 24. El enlace unidireccional 34 conecta una zona segura 28, que contiene los componentes protegidos de la estación 22, a una zona 30 de antememoria, que es accesible para la red 26. Aunque la interfaz 38 de salida normalmente comprende un puerto de red convencional y bidireccional, el enlace unidireccional 34 impide cualquier tipo de acceso a la zona segura 28 a través de la interfaz 38 de salida.

El enlace unidireccional 34 transporta información de salida desde la estación 22 a la red 26, pero es físicamente incapaz de transmitir datos de entrada desde la red a la estación. Para este último fin, la estación 22 comprende una entrada segura 36, que normalmente tiene una interfaz de entrada acoplada a la red 26 y otra interfaz a los elementos protegidos de la estación. En este ejemplo, la entrada segura 36 recibe y decodifica un flujo de símbolos (normalmente, símbolos cifrados) transmitidos por el terminal 24 a través de la red 26, y transmite los símbolos decodificados a través de un enlace unidireccional 32 al ordenador principal 41. Detalles de la estructura y operación de la entrada segura 36 se describen adicionalmente, por ejemplo, en la publicación de solicitud de patente estadounidense 2016/01123844 mencionada anteriormente. El ordenador anfitrión 41 en particular y la zona segura 28 en general no reciben entradas de la red 26 salvo a través de la entrada 36 y el enlace unidireccional 32, que normalmente están contenidos en la estación 22 y, así, están protegidos contra manipulaciones físicas y eléctricas indebidas.

El terminal 24 recibe la salida de datos por la estación 22 a través de la salida 38 por medio de una ruta 42 de salida a través de la red 26, e introduce datos, como instrucciones y/o consultas, en la estación 22 a través de una ruta 44 de entrada separada a la entrada 36. Como se señaló anteriormente, la entrada 36 y la salida 38 normalmente comprenden puertos separados e independientes a la red 26, con sus propias direcciones de red diferentes, como direcciones IP. Las rutas 42 y 44 son establecidas por separado por dispositivos de encaminamiento (no mostrados) en la red 26. El terminal 24 está configurado de manera similar con interfaces de entrada y salida separadas, como se muestra y describe a continuación con referencia a la Fig. 2.

Cuando es necesario transmitir tráfico orientado a la conexión hacia y desde el ordenador 41 en la estación 22, se activa un dispositivo delegado TCP 46 en la estación. Típicamente, el dispositivo delegado TCP 46 comprende un procesador, que está separado del ordenador 41 y tiene interfaces y soporte lógico adecuados para llevar a cabo las funciones que se describen en este documento. En la operación normal de la estación 22, las centralitas 48 y 50, normalmente centralitas de datos activadas por soporte físico, aíslan el dispositivo delegado TCP 46 de la red 26, de modo que todas las entradas del enlace unidireccional 32 al ordenador anfitrión 41 y otros elementos de la red interna 40 de control, así como las salidas del ordenador 41 y la red 40 al enlace unidireccional 34, no pasen por el dispositivo delegado TCP.

Sin embargo, cuando se invoca una conexión TCP con el terminal remoto 24, las centralitas 48 y 50 se activan para conectar enlaces unidireccionales 32 y 34 hacia y desde el dispositivo delegado TCP 46, el cual puede comenzar a

continuación la emulación TCP. Normalmente, el dispositivo delegado TCP 46 se ejecuta en un módulo 47 de seguridad de soporte físico (HSM) instalado en la zona segura 28, para evitar manipulaciones indebidas y ataques. Además o alternativamente, el dispositivo delegado TCP 46 y/o las centralitas 48 y 50 comprenden otros componentes y soporte lógico de autenticación, como un módulo de plataforma fiable (TPM). El uso de dicho soporte físico seguro garantiza que las centralitas se activen y se pueda establecer una conexión TCP con el terminal 24 solo después de que el usuario del terminal se haya autenticado correctamente.

Normalmente, el HSM 47 (y de manera similar un HSM utilizado para el dispositivo delegado TCP en el terminal 24, como se describe a continuación) comprende un procesador controlado por soporte lógico, como una unidad central de procesamiento (CPU), con una memoria e interfaces de comunicaciones adecuadas para recibir y transmitir tramas TCP de datos desde y hacia las centralitas 48 y 50. Para estos fines, el HSM 47 puede comprender un subsistema de soporte físico disponible comercialmente, como el coprocesador criptográfico PCIe de IBM, que es una tarjeta criptográfica PCIe®, programable y de respuesta a manipulaciones indebidas, que contiene una CPU, soporte físico de cifrado, RAM, memoria persistente, un generador de números aleatorios de soporte físico, reloj, soporte lógico inalterable de infraestructura y soporte lógico. El soporte lógico que se ejecuta en la CPU está hecho a medida, en la presente realización, para incluir la pila de dispositivo delegado TCP y la interfaz. Por lo tanto, como se señaló anteriormente, el propio código del dispositivo delegado nunca es realmente accesible desde la red 26. El código se almacena en la memoria del HSM en forma cifrada y se activa y descifra para ejecutarse en la CPU del HSM, solo después de la autenticación adecuada. Debido a que el código se ejecuta solo internamente dentro del entorno de ejecución segura del HSM 47, no es posible copiar el código para usarlo desde otro ordenador en la red ni siquiera cuando el dispositivo delegado TCP 46 está activado.

La figura 2 es un diagrama de bloques que muestra esquemáticamente detalles del terminal 24 de usuario remoto, según una realización de la presente invención. En la realización ilustrada, el terminal 24 comprende una interfaz de usuario, que comprende un dispositivo 62 de entrada seguro y una pantalla 60, que son elementos separados física y funcionalmente. El dispositivo y la pantalla de entrada especiales y seguros son útiles en las operaciones rutinarias del terminal 24, cuando no se necesita una comunicación TCP bidireccional completa. Estos componentes seguros no son necesarios cuando el terminal 24 opera solo en un modo de monitorización, sin introducir datos o instrucciones en la estación 22, ni son necesarios cuando los dispositivos delegados TCP están en uso (en cuyo caso son suficientes un dispositivo de entrada de usuario convencional y una pantalla). El dispositivo 62 de entrada seguro y la pantalla 60 se describen aquí, sin embargo, junto con los enlaces unidireccionales 56 y 66, en aras de la integridad para demostrar un terminal de usuario con múltiples funciones y prestaciones completas.

El dispositivo 62 de entrada seguro, como un teclado, un ratón u otro elemento operado por el usuario, recibe entradas de un operario del terminal 24 y codifica estas entradas como una secuencia de símbolos cifrados utilizando una clave de cifrado preseleccionada. El enlace unidireccional 66 transporta la salida cifrada del dispositivo 62 a una interfaz 68 de salida del terminal 24.

La interfaz 68 de salida transmite la secuencia de símbolos cifrados desde el dispositivo 62 de entrada a través de la ruta 44 de entrada a través de la red 26 a la entrada 36, que decodifica los símbolos y, por lo tanto, proporciona una correspondiente secuencia de símbolos en claro al ordenador anfitrión 41. La interfaz 68 de salida puede, por ejemplo, establecer un conexión segura (como una conexión cifrada de seguridad de la capa de transporte [TLS], como se conoce en la técnica) con la entrada 36 a través de la red 26. Este tipo de medida convencional de seguridad de datos agrega una capa adicional de protección al funcionamiento de las otras medidas de seguridad descrito en la presente memoria. Sin embargo, esta conexión, que se establece entre las direcciones IP de la interfaz 68 de salida y la entrada 36, lleva solo la información que sale del terminal 24 a través del enlace unidireccional 66 (y posiblemente los paquetes de reconocimiento de la entrada 36), mientras que los enlaces 66 y 32 evitan que datos significativos lleguen al terminal 24 a través de la conexión.

Normalmente, aunque no necesariamente, el dispositivo 62 de entrada cifra las entradas del operario usando lógica de soporte físico y mantiene la clave de cifrado en una memoria (no mostrada) que es inaccesible para el usuario del terminal 24. Esta clave también puede ser inaccesible para un procesador anfitrión 72 que se utilice para ejecutar funciones basadas en el soporte lógico del terminal. Para el propósito de estas funciones basadas en soporte lógico (incluidas las aplicaciones que se ejecutan a través de conexiones TCP a la estación 22), el dispositivo 62 de entrada puede tener un modo de operación adicional no cifrado. Alternativamente, uno o más dispositivos de entrada adicionales (no mostrados) pueden conectarse al terminal 24, o, si el terminal 24 está configurado para enviar entradas a la estación 22 solo a través de una conexión TCP segura, el dispositivo 62 de entrada puede ser reemplazado por un dispositivo ordinario de entrada sin cifrado.

Paralelamente a la operación de la ruta 44 de entrada que se describe anteriormente, una interfaz 54 de entrada del terminal 24 recibe la salida de datos generada por la estación 22 y transmitida a través de la ruta 42 de salida a través de la red 26 a través de la salida 38. La interfaz 54 de entrada transmite los datos a través de un enlace unidireccional 56 a la pantalla 60, que presenta los datos en forma alfanumérica y/o gráfica. Para estos fines, la interfaz 54 de entrada normalmente comprende un controlador de interfaz de red (NIC), acoplado para transmitir y recibir paquetes hacia y desde la red 26, junto con un controlador de comunicaciones adecuado para transmitir datos a través del enlace unidireccional 56 y una antememoria adecuada y circuitos lógicos (controlados por soporte físico o soporte lógico) que

los conectan. Estas funciones pueden llevarse a cabo, por ejemplo, mediante una pasarela de enlace unidireccional Waterfall.

Como se señaló anteriormente, en el funcionamiento normal del terminal 24, la ruta 44 de entrada desde la interfaz 68 de salida del terminal 24 a la estación 22 y la ruta 42 de salida desde la estación 22 a la pantalla 60 están separadas y son independientes, sin ninguna interacción electrónica entre estas rutas dentro del terminal 24. La interfaz 54 de entrada puede establecer una conexión segura adicional (como una conexión TLS) con la salida 38 a través de la red 26, que es independiente de la conexión entre la interfaz 68 de salida y la entrada 36. La única conexión real que normalmente existe entre las rutas 44 y 42 de entrada y salida es la conexión cognitiva realizada por el operario del terminal 24.

Sin embargo, como se explicó anteriormente, el operario del terminal 24 puede necesitar interactuar ocasionalmente con el ordenador 41 en la estación 22 usando una aplicación cliente/servidor o entre dispositivos del mismo nivel basada en una conexión. Para este fin, el terminal 24 comprende un módulo 52 de soporte de protocolo seguro con un dispositivo delegado TCP 70, que interactúa con el dispositivo delegado TCP 46 en la estación 22 cuando se activa. Como en el lado de la estación, el dispositivo delegado TCP 70 comprende un procesador, que está separado del procesador anfitrión 72 y tiene interfaces y soporte lógico adecuados para llevar a cabo las funciones que se describen en este documento. El módulo 52, que incluye el dispositivo delegado TCP 70 y las centralitas 58 y 64, generalmente se implementa como una unidad de soporte físico segura, a prueba de manipulaciones indebidas, que está reforzada contra el uso y la ingeniería inversa no autorizados. El dispositivo delegado TCP 70 puede conectarse y comunicarse con el procesador anfitrión 72 a través de un bus adecuado, como un bus PCIe.

Dentro del módulo 52, al menos el dispositivo delegado 70 de TCP se ejecuta en un HSM 74, similar al HSM 47 que se describió anteriormente. La activación del HSM 74 está condicionada, por ejemplo, a la inserción por parte del usuario de una llave adecuada 76, como una tarjeta inteligente o SIM, o la presentación de otras credenciales de soporte físico, posiblemente acompañadas de otras medidas de seguridad, como contraseña y/o autenticación biométrica del usuario. Para una mayor seguridad, el HSM 74 puede requerir que el usuario presente una clave adicional para activar el soporte lógico del dispositivo delegado TCP, además de la llave utilizada para activar el HSM.

La llave 76 generalmente contiene una o más claves criptográficas privadas. El HSM 74 utiliza estas claves para enviar instrucciones de activación al HSM 47, y hace que los HSM 47 y 74 activen el código del dispositivo delegado (incluido el descifrado del código almacenado utilizando la clave) y ejecutan el código dentro de la instalación de ejecución segura de los HSM.

En el funcionamiento normal del terminal 24, cuando HSM 74 no se activa, las centralitas 58 y 64 aíslan el dispositivo delegado TCP 70 de la red 26, de modo que todas las entradas del enlace unidireccional 56 y la salida al enlace unidireccional 66 no pasan por el dispositivo delegado TCP. Sin embargo, cuando se activa HSM 74 y se invoca una conexión TCP, las centralitas 58 y 64 operan para conectar enlaces unidireccionales 56 y 66 hacia y desde el dispositivo delegado TCP 70, que a continuación puede comenzar la emulación TCP. Con este fin, el dispositivo delegado TCP 70 también da instrucciones a las centralitas 48 y 50 en la estación 22 para que conecten el dispositivo delegado TCP 46 a la entrada 36 y la salida 38, como se describió anteriormente. Normalmente, la instrucción para las centralitas 48 y 50 va acompañada de credenciales criptográficas, proporcionadas por el HSM 74 que permiten, por ejemplo, que el controlador responsable en la estación 22 autentique la instrucción antes de activar las centralitas.

Alternativamente, el HSM 74 puede ser el único responsable de la seguridad de los datos en el terminal 24. En este caso, las centralitas 58 y 64 pueden ser activadas manualmente por el operario del terminal 24, o pueden eliminarse por completo. (Las centralitas 48 y 50 en la estación 22, sin embargo, aún proporcionan una medida de seguridad adicional útil). Además o alternativamente, los enlaces unidireccionales 56 y 66 en el terminal 24 pueden reemplazarse por una o más conexiones bidireccionales normales, mientras se mantiene el uso de enlaces unidireccionales 32 y 34 para proteger la estación 22 del acceso no autorizado.

En cualquier caso, una vez que se han activado los HSM 47 y 74, como se describió anteriormente, los dispositivos delegados TCP 70 y 46 se comunican entre sí para iniciar y configurar la emulación de la interfaz de conexión TCP. La interacción entre los dispositivos delegados TCP es similar a la que existe entre los puntos finales TCP convencionales, salvo que, en el presente caso, las tramas TCP se transmiten desde el dispositivo delegado TCP 70 al dispositivo delegado TCP 46 por la ruta 44 de entrada y desde el dispositivo delegado TCP 46 al dispositivo delegado TCP 70 por la ruta 42 de salida. Como se explicó anteriormente, los puntos finales de la ruta 44 de entrada tienen direcciones IP diferentes de los puntos finales de la ruta 42 de salida. Una vez que la conexión TCP emulada está configurada y en funcionamiento, los dispositivos delegados TCP 46 y 70 notifican a los respectivos anfitriones 41 y 72 que la conexión está disponible para que la aplicación deseada pueda ejecutarse.

Normalmente, toda la comunicación entre los dispositivos delegados TCP 46 y 70 está firmada por claves. Por lo tanto, cuando se elimina la clave 76, el sistema 20 pasa al estado “sin dispositivo delegado”, en el cual los HSM 47 y 74 son inaccesibles, y las centralitas que conectan los dispositivos delegados TCP a la red 26 están bloqueadas. Además o alternativamente, los servidores delegados TCP 46 y 70 intercambian regularmente mensajes de autorización y se apagan si no llega un mensaje de autorización cuando se esperaba.

Los elementos de la estación 22 y el terminal 24 se muestran en las figuras y se describen anteriormente en términos de bloques funcionales separados únicamente por conveniencia y claridad conceptual. En implementaciones prácticas, dos o más de estos bloques pueden combinarse en un único elemento de circuito o, adicional o alternativamente, ciertos bloques pueden dividirse en subbloques y circuitos separados. Se considera que todas estas realizaciones están dentro del alcance de la presente invención.

REIVINDICACIONES

1. Un sistema (20) de comunicaciones, que comprende:

una estación (22), que comprende unas interfaces primera y segunda (36, 38) configuradas para conectarse a una red (26) de paquetes de datos y tener respectivas direcciones diferentes de red primera y segunda;

un terminal (24), que comprende interfaces tercera y cuarta (54, 68) configuradas para conectarse a la red de paquetes de datos y tener respectivas direcciones diferentes de red tercera y cuarta,

en el que la estación está configurada para transmitir unos primeros datos al terminal a través de una primera ruta (42) a través de la red de paquetes de datos dirigida desde la primera interfaz a la tercera dirección de red, mientras que el terminal está configurado para transmitir segundos datos a la estación durante una segunda ruta (44) a través de la red de paquetes de datos dirigida desde la cuarta interfaz a la segunda dirección de red; y

dispositivos delegados primero y segundo (46, 70) de protocolo de control de transmisión, TCP, que se implementan respectivamente en la estación y en el terminal, y están configurados para emular una conexión TCP entre la estación y el terminal mediante la transmisión de tramas TCP desde la estación al terminal solo sobre la primera ruta y desde el terminal a la estación solo sobre la segunda ruta;

en el que la estación comprende un primer enlace unidireccional saliente conectado entre el primer dispositivo delegado TCP y la primera interfaz y un primer enlace unidireccional entrante conectado entre la segunda interfaz y el primer dispositivo delegado TCP;

en el que los enlaces unidireccionales están configurados físicamente para transportar señales en una dirección y para ser incapaces de transportar señales en la dirección opuesta;

caracterizado por que la estación comprende unas centralitas primera y segunda, que se acoplan entre los enlaces unidireccionales saliente y entrante y el primer dispositivo delegado TCP y están configuradas para conectar el primer dispositivo delegado TCP a la red de paquetes de datos a través de los enlaces unidireccionales saliente y entrante solo cuando la conexión TCP emulada está en uso.

2. El sistema según la reivindicación 1 en el que el terminal comprende un segundo enlace unidireccional saliente conectado entre el segundo dispositivo delegado TCP y la cuarta interfaz y un segundo enlace unidireccional entrante conectado entre la tercera interfaz y el segundo dispositivo delegado TCP.

3. El sistema según la reivindicación 1 o 2 en el que la estación comprende un ordenador central (anfitrión), que está configurado para transmitir y recibir paquetes de datos hacia y desde la red de paquetes de datos a través de los enlaces unidireccionales salientes y entrantes, respectivamente, y que está acoplado al primer dispositivo delegado TCP para transmitir y recibir datos a través de la conexión TCP emulada,

en el que las centralitas primera y segunda están configuradas para aislar el primer dispositivo delegado TCP cuando la conexión TCP emulada no está en uso y para transportar paquetes de datos entrantes desde el enlace unidireccional entrante al ordenador anfitrión y transmitir paquetes de datos salientes desde el ordenador al enlace unidireccional saliente, sin pasar por el primer dispositivo delegado TCP.

4. El sistema según la reivindicación 3 en el que la estación comprende un módulo de seguridad de soporte físico (HSM), que está acoplado para controlar la activación de las centralitas.

5. El sistema según una cualquiera de las reivindicaciones 1 a 4 en el que el terminal comprende un módulo de soporte de protocolo seguro, que comprende un módulo de seguridad de soporte físico, HSM, en el que se ejecuta el segundo dispositivo delegado TCP.

6. El sistema según la reivindicación 5 en el que la activación del HSM para emular la conexión TCP está condicionada a la presentación de una credencial de soporte físico al HSM.

7. El sistema según la reivindicación 5 o 6 en el que el módulo de soporte de protocolo seguro comprende una primera centralita, que está acoplada entre la tercera interfaz y el HSM, y una segunda centralita, que está acoplada entre la cuarta interfaz y el HSM, y en el que las centralitas primera y segunda están configuradas para conectar el HSM a la red de paquetes de datos a través de las interfaces tercera y cuarta solo cuando la conexión TCP emulada está en uso.

8. El sistema según la reivindicación 7 en el que el terminal comprende un procesador anfitrión, que está configurado para recibir y transmitir paquetes de datos desde y hacia la red de paquetes de datos a través de las interfaces tercera y cuarta, respectivamente, y que está acoplado al HSM para transmitir y recibir datos a través de la conexión TCP emulada,

en el que las centralitas primera y segunda están configuradas para aislar el segundo dispositivo delegado TCP cuando la conexión TCP emulada no está en uso y para transportar paquetes de datos entrantes desde la tercera interfaz al

procesador anfitrión y transmitir paquetes de datos salientes desde el procesador anfitrión a la cuarta interfaz, sin pasar por el HSM.

9. Un método de comunicaciones que comprende:

conectar una estación (22) a una red (26) de paquetes de datos a través de unas interfaces primera y segunda (36, 38) que tienen respectivas direcciones diferentes de red primera y segunda;

conectar un terminal (24) a la red de paquetes de datos a través de las interfaces tercera y cuarta (54, 68) que tienen respectivas direcciones diferentes de red tercera y cuarta; y

emular una conexión de protocolo de control de transmisión, TCP, entre la estación y el terminal mediante la transmisión de las primeras tramas TCP desde un primer dispositivo delegado TCP (46) implementado en la estación a un segundo dispositivo delegado TCP (70) implementado en el terminal solo por una primera ruta (42) a través de la red de paquetes de datos dirigida desde la primera interfaz a la tercera dirección de red, y transmitir las segundas tramas TCP desde el segundo dispositivo delegado TCP en el terminal al primer dispositivo delegado TCP en la estación solo por una segunda ruta (44) a través del paquete red de datos dirigida desde la cuarta interfaz a la segunda dirección de red;

en el que la conexión de la estación comprende conectar un primer enlace unidireccional saliente entre el primer dispositivo delegado TCP y la primera interfaz y conectar un primer enlace unidireccional entrante entre la segunda interfaz y el primer dispositivo delegado TCP;

en el que los enlaces unidireccionales están configurados físicamente para transportar señales en una dirección y para ser incapaces de transportar señales en la dirección opuesta;

caracterizado por que la conexión de la estación comprende, además, la activación de las centralitas primera y segunda, acopladas respectivamente entre los enlaces unidireccionales salientes y entrantes y el primer dispositivo delegado TCP, para conectar el primer dispositivo delegado TCP a la red de paquetes de datos a través de los enlaces unidireccionales salientes y entrantes solo cuando la conexión TCP emulada está en uso.

10. El método según la reivindicación 9 en el que la conexión del terminal comprende conectar un segundo enlace unidireccional saliente conectado entre el segundo dispositivo delegado TCP y la cuarta interfaz y conectar un segundo enlace unidireccional entrante entre la tercera interfaz y el segundo dispositivo delegado TCP.

11. El método según la reivindicación 9 o 10 en el que la estación (22) comprende un ordenador anfitrión, que transmite y recibe paquetes de datos hacia y desde la red de paquetes de datos a través de los enlaces unidireccionales salientes y entrantes, respectivamente, y que está acoplado al primer dispositivo delegado TCP para transmitir y recibir datos a través de la conexión TCP emulada,

en el que las centralitas primera y segunda aíslan el primer dispositivo delegado TCP cuando la conexión TCP emulada no está en uso y transmiten los paquetes de datos entrantes desde el enlace unidireccional entrante al ordenador anfitrión y transmiten los paquetes de datos salientes desde el ordenador al enlace saliente de ruta, sin pasar por el primer dispositivo delegado TCP.

12. El método según la reivindicación 11 en el que la estación comprende un módulo de seguridad de soporte físico, HSM, que controla la activación de las centralitas.

13. El método según una cualquiera de las reivindicaciones 9 a 12 en el que la emulación de la conexión TCP comprende ejecutar el segundo dispositivo delegado TCP en un módulo de seguridad de soporte físico (HSM) en el terminal.

14. El método según la reivindicación 13 en el que la emulación de la conexión TCP está condicionada a la presentación de una credencial de soporte físico al HSM.

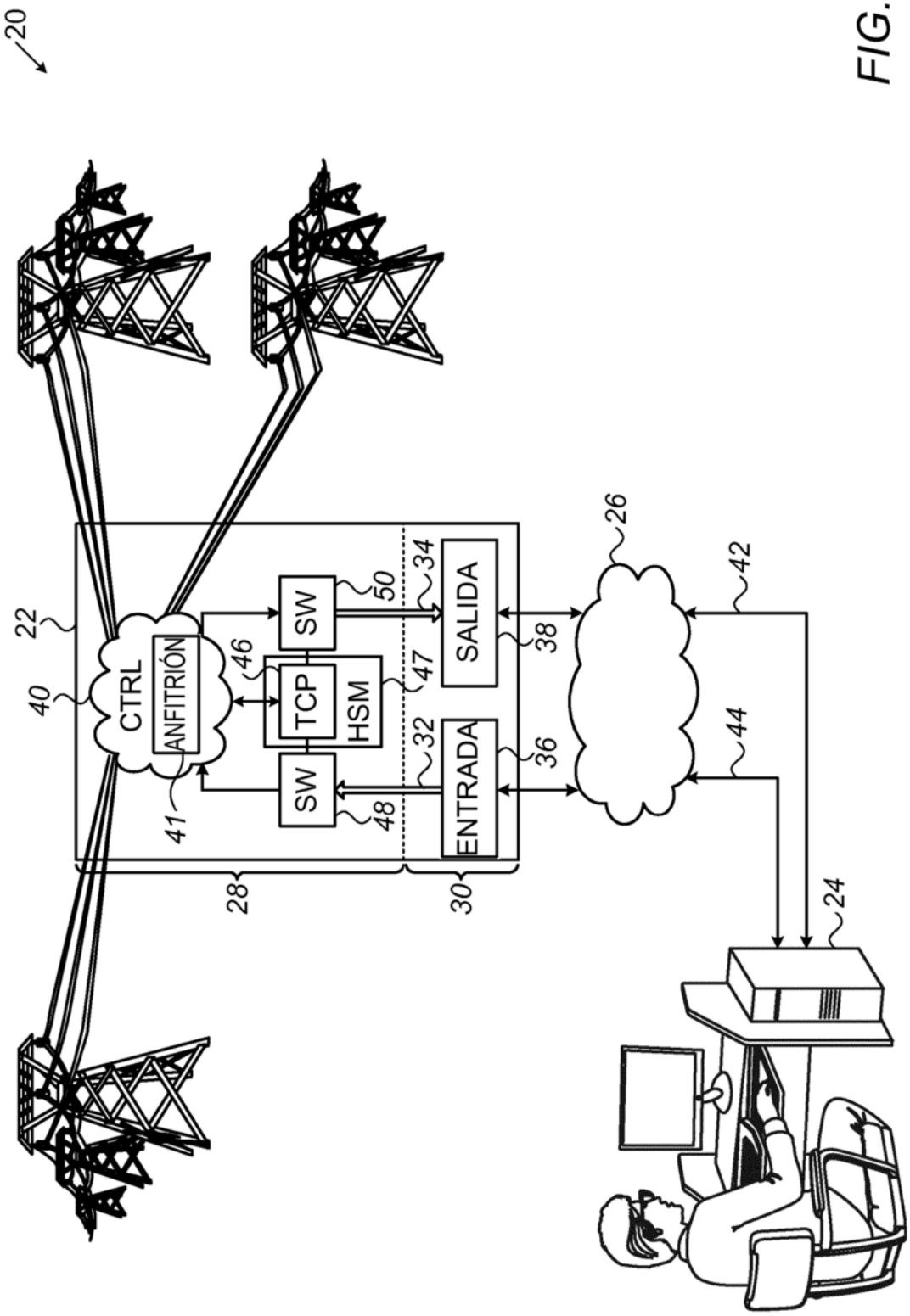
20
22
40
CTRL
ANFITRIÓN
41
46
TCP
HSM
47
SW
50
SW
48
34
SALIDA
32
ENTRADA
38
36
26
42
44
24
28
30

FIG. 1

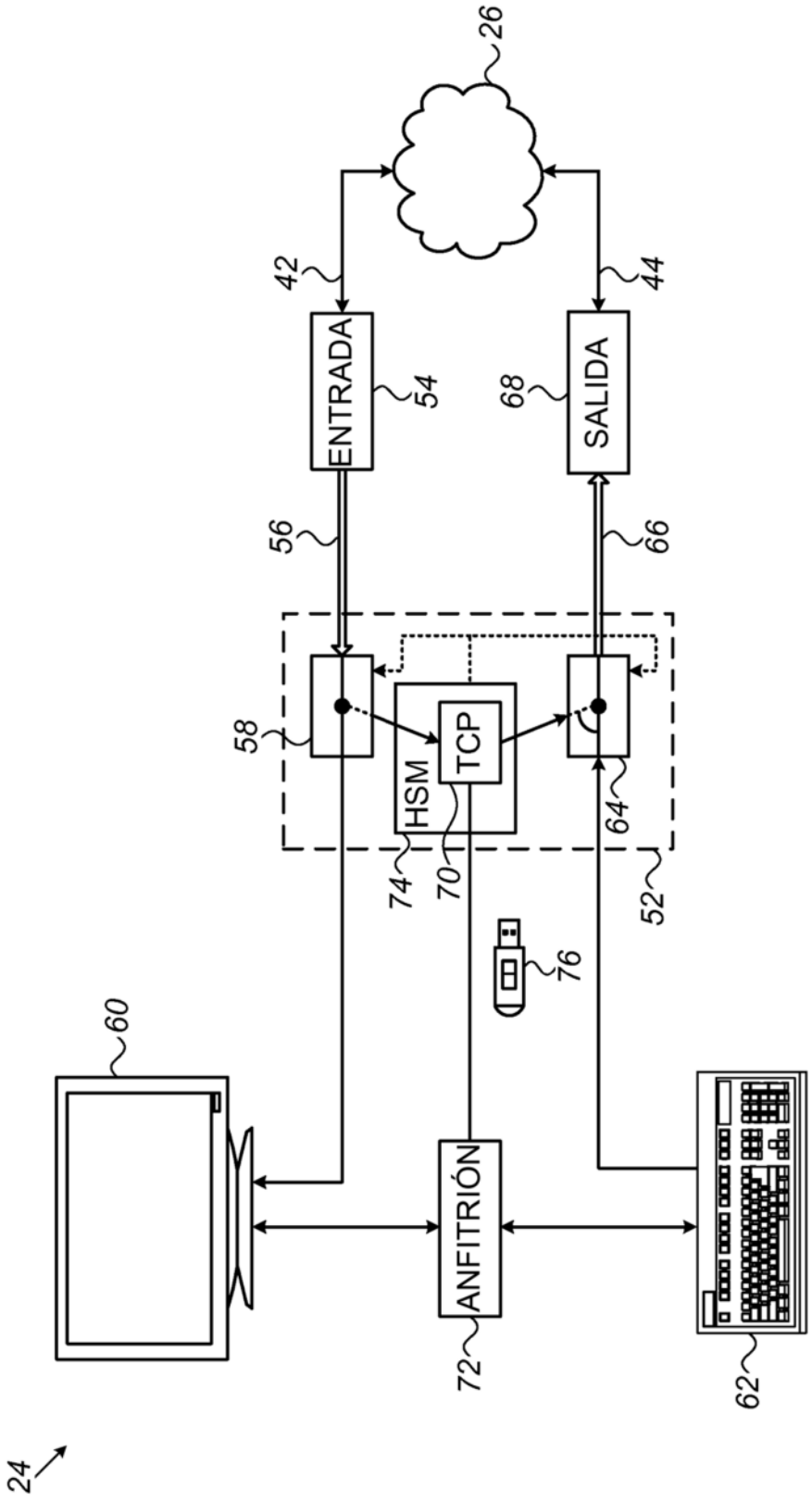
26
42
44
ENTRADA
54
68
SALIDA
56
66
58
HSM
TCP
64
74
70
52
76
60
ANFITRIÓN
72
62
24

FIG. 2