(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 660 623**

(51) Int. CI.:

G08B 25/00 (2006.01)
G08B 25/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.02.2016 E 16154130 (5)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2018 EP 3054435**

(54) Título: **Sistemas y métodos para impedir la apropiación indebida de sistemas de seguridad y componentes**

(30) Prioridad:

06.02.2015 US 201514616196

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.03.2018

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
Intellectual Property-Patent Services, P.O.Box 377, 115 Tabor Road, M/S 4D3
Morris Plains, NJ 07950, US

(72) Inventor/es:

SCHMIT, THOMAS PAUL

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistemas y métodos para impedir la apropiación indebida de sistemas de seguridad y componentes

CAMPO DE LA INVENCIÓN

La solicitud se refiere a sistemas y métodos para impedir la apropiación indebida de sistemas de seguridad que tienen una arquitectura centralizada. Más en particular, la solicitud se refiere a sistemas y métodos que proporcionan un componente descentralizado que incluye agentes de vigilancia para supervisar y autenticar comunicaciones con un servicio de supervisión desplazado.

ANTECEDENTES DE LA INVENCIÓN

Los servicios de supervisión del sistema de seguridad compiten entre sí por los abonados. Como resultado, no es raro que estos servicios modifiquen, sustituyan o agreguen los componentes de las instalaciones del sistema de seguridad existentes para adquirir (es decir, secuestrar) abonados de la competencia. Esto es particularmente perturbador ya que los servicios de supervisión a menudo soportan los costos de los componentes del sistema de seguridad y la instalación inicial.

Los sistemas de seguridad supervisados conocidos utilizan, a menudo, una arquitectura centralizada de modo que una orden y el control del sistema se origina desde el servicio de supervisión. Esta arquitectura depende del servicio de supervisión que mantiene un canal de comunicaciones seguro con la instalación de supervisión. Si este canal es 'secuestrado' por un servicio de la competencia, el servicio de la competencia se puede apropiar, además, de las cuentas de abonados asociados y los ingresos relacionados. Este proceso, en general, se denomina ataque cibernético de 'intermediario'. Dichas prácticas suelen violan contratos previos entre el servicio de supervisión que pagó por la instalación inicial y el abonado de dicha instalación. Asimismo, también se les asigna una alta prioridad en los modelos de amenaza cibernética utilizados en el diseño de los sistemas de seguridad.

El documento de patente número US2007/183597 A1 describe un método para proporcionar un sistema de seguridad, para el hogar o negocio, que se basa en la encriptación de datos tanto para la comunicación como para el almacenamiento de contenido.

La presente invención, en sus diversos aspectos, es según se establece en las reivindicaciones adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 ilustra un diagrama de bloques de un sistema de conformidad con este documento.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Aunque las formas de realización dadas a conocer pueden tener numerosas formas distintas, las formas de realización específicas de las mismas se ilustran en los dibujos y se describirán aquí en detalle en el entendimiento de que la presente idea inventiva se debe considerar como una forma, a modo de ejemplo, de los principios de la misma, así como su mejor modo de puesta en práctica, y no está prevista para limitar la solicitud o reivindicaciones a la forma de realización específica ilustrada.

En un aspecto de la idea inventiva, un componente descentralizado para la arquitectura del sistema mayoritariamente centralizada, mencionada anteriormente, para la finalidad de prevenir la apropiación indebida, no autorizada, referida con anterioridad. Más en general, proporciona protección adicional contra los ciberataques del tipo de intermediario.

En una forma de realización dada a conocer, el componente descentralizado se pone en práctica mediante el diseño de agentes de vigilancia en los componentes de los sistemas de seguridad, más concretamente, los situados en las periferias de la red subyacentes a la arquitectura del sistema (p.ej., sensores, puntos de control de dispositivo, dispositivos de interfaz de usuario, etc.). De conformidad con lo que antecede, los agentes de vigilancia proporcionan, de forma continua, una autenticación adicional de comunicaciones con el servicio de supervisión. Los agentes pueden, además, ponerse en práctica en un modo independiente y se pueden instalar en la zona de interés.

Si un agente de vigilancia del componente determina que las comunicaciones ya no son auténticas, en ese caso, el componente podría, a modo de ejemplo, iniciar una notificación de las partes implicadas y/o interrumpir el funcionamiento o degradar su rendimiento de modo que anule el incentivo para la apropiación indebida. El software de autenticación local y/o circuitos se pueden proporcionar para evaluar mensajes recibidos a partir de los agentes.

La Figura 1 ilustra aspectos de la idea inventiva, según se describió con anterioridad, de un sistema 10 de conformidad con este documento. Tipos pertinentes del sistema 10, sin limitación, incluyen al menos sistemas de supervisión de seguridad de zona y/o condición ambiental o, sistemas de automatización de edificios.

El sistema, a modo de ejemplo, 10, incluye un elemento de control del sistema o panel 12. El elemento 12 puede incluir una pluralidad de interfaces de I/O (entrada/salida) 12a, circuitos de control local 12b, software de autenticación y/o circuitos 12c y una interfaz de usuario local 12d con entradas de audio/visuales para permitir a un usuario local comprobar el funcionamiento del sistema, introducir comentarios o parámetros o transmitir comunicaciones, según sea necesario.

Tal como entenderá un experto en esta técnica, el elemento 12, a través de las interfaces 12a, puede estar en comunicación con una pluralidad de detectores, dispositivos de entrada o salida, generalmente indicados en 14. Los dispositivos de la pluralidad 14, tales como 14i, pueden incluir detectores de condición ambiental, tales como detectores de intrusión, sin limitación, detectores de detección de condición, tales como detectores de humo o de incendio, así como dispositivos de entrada o salida de indicación de alarma.

Los miembros de la pluralidad 14 se pueden comunicar con el elemento de control 12 a través de un medio inalámbrico o cableado, indicado generalmente por la referencia 16. Los miembros de la pluralidad 14 se instalarán según sea adecuado en una zona R que se supervisa y controla.

El elemento de control 12 puede estar en comunicación, a través de uno o más medios inalámbricos o cableados, tales como 20a, b y una red informática 20c, con una instalación de servicio de supervisión 22 que, normalmente, no está situada con el sistema 10. La instalación 22 es la auténtica instalación prevista para proporcionar funciones de seguridad, supervisión o control en relación con la zona R a través del sistema 10. La instalación 22 puede evaluar condiciones en la zona R sobre la base de señales e información recogida a través del elemento de control local 12. Dependiendo de las circunstancias, la instalación 22 puede transmitir información o mensajes con respecto a la zona R a través de la red 20c con un dispositivo de comunicación de usuario, un teléfono o un ordenador 24.

Desde el punto de vista conceptual, debe entenderse que los sistemas, tales como el sistema 10, pueden estar caracterizados por tener una estructura similar a un árbol. Están situados nodos en la raíz del árbol (referida, a continuación, como ‘la raíz’ o el ‘nodo raíz’) y en cada punto de bifurcación (rama), representando las funciones comunes para un sistema de seguridad, detección de incendios o automatización de instalaciones (referido, a continuación como ‘el sistema’). En esta configuración, las bifurcaciones representan el flujo de comunicaciones entre los nodos.

Los nodos de terminación o periféricos (referidos a continuación como ‘periféricos’ o ‘periférico’), más alejados de la raíz, representan normalmente sensores, puntos de control de dispositivo, dispositivos de interfaz de usuario, etc.

Los nodos entre la raíz y los nodos periféricos se refieren como nodos intermedios o simplemente ‘intermedios’. La estructura de árbol entre la raíz y los periféricos varía sobre la base de los requisitos y restricciones del diseño del sistema. Los nodos intermedios representan, normalmente, uno o más paneles de control, fuentes de alimentación de energía, repetidores/concentradores de comunicaciones, etc.

El nodo raíz no suele estar situado, físicamente, en los emplazamientos de instalación de los nodos intermedio y periférico. De forma similar, pueden instalarse agrupamientos de nodos intermedios y periféricos en emplazamientos físicamente separados.

Una vez completada la instalación del sistema, el nodo raíz del árbol representa el punto de supervisión, de orden y de control, tal como la instalación de supervisión 22, que tiene la máxima autoridad dentro del sistema. La raíz suele ser propiedad de lo que normalmente nos referimos como el servicio de supervisión.

El servicio de supervisión es el principal responsable de garantizar que se notifique a las partes afectadas de los eventos transmitidos a la raíz sobre la base de cambios en el estado de los diversos nodos/funciones que componen el árbol. Un servicio secundario del propietario de la raíz es mantener y/o cambiar la configuración y el funcionamiento del sistema.

Durante la instalación del sistema, la raíz puede ser, de forma temporal, propiedad de un vendedor y/o instalador del sistema. En este caso, la función de orden y control de la raíz se utiliza para adaptar la configuración del sistema al emplazamiento de la instalación y para comprobar y realizar pruebas al sistema. Después de que se complete la instalación, la propiedad de la raíz se transfiere al servicio de supervisión aunque, en algunos casos, la propiedad de la función de orden y control se puede mantener por el servicio de instalación o transferirse a un servicio separado, con la finalidad realizar un mantenimiento del equipo instalado (esto es, un servicio de mantenimiento del emplazamiento).

En formas de realización del presente documento, se proporciona protección para evitar a una unidad competidora, que el servidor de apropiación indebida 30, ilustrado en líneas discontinuas en la Figura 1, desplace la instalación auténtica 22 y se comunique con el sistema 10. El servicio de apropiación indebida 30 puede estar situado a distancia de cualquier parte del sistema 10 o la instalación de servicio auténtica 22, a modo de ejemplo, en cualquier parte donde haya una conexión de red en la nube.

Se puede instalar una pluralidad de agentes, indicados en general con la referencia 34, en la zona R. Los agentes se pueden poner en práctica como dispositivos autónomos, tales como 34a, 34b … 34n. De forma alternativa, los agentes pueden ponerse en práctica como complementos o módulos acoplados a miembros de la pluralidad 14, según se ilustra por 36a, b, c … r.

Debe entenderse que los agentes 36 podrían comunicarse con el software de autenticación y/o circuitos 12c (que podrían ponerse en práctica con uno o más microprocesadores que ejecutan dicho software) en el elemento 12, entre sí, o a través de la red 20c con el servicio de supervisión auténtico 22.

Los agentes 36 ponen en práctica, al menos en parte, un sistema de supervisión descentralizado secundario que se superpone al sistema de supervisión más centralizado 10, según se describió con anterioridad. Dichos agentes pueden considerarse como situados en nodos intermedios y/o periféricos del sistema 10. Los expertos en la técnica entenderán que los nodos intermedios podrían incluir uno o más paneles de control, fuentes de alimentación de energía, dispositivos de comunicaciones, o repetidores, o similares, sin limitación. Los nodos periféricos pueden incluir detectores, puntos de control de dispositivo, estacones de activación de alarma, cualesquiera dispositivos de interfaz de usuario, sin limitación.

En un aspecto de la idea inventiva, los agentes pueden supervisar, de forma pasiva, eventos que se originan localmente, dentro de un nodo respectivo. Como alternativa, agentes respectivos pueden supervisar eventos en el sistema completo. Los agentes pueden buscar modelos que indican que la autoridad raíz del sistema, a modo de ejemplo, la instalación de servicio de supervisión 22, ha sido comprometida. En otro aspecto, los agentes pueden causar, activamente, eventos locales, tales como eventos del sistema completo que pueden indicar que la instalación de servicio 22 se ha visto comprometida al ser desplazada por la instalación de servicio de apropiación indebida 30.

Si un agente comprueba que la autoridad raíz se ha visto comprometida (p.ej., bloqueada por un proveedor de servicios competidor), inicia acciones de contramedida (denominadas a continuación "contramedidas") que deben transmitirse por el dispositivo que aloja los nodos y agentes, anteriormente mencionados. Los detalles y la gravedad de las contramedidas se determinan teniendo en cuenta las características específicas de la instalación del sistema y sus usuarios.

Si una cuenta residencial se ha visto comprometida/objeto de apropiación indebida, entonces, una finalidad puede ser una respuesta más moderada y oculta que dirija la insatisfacción del usuario hacia el servicio del pirata informático. Esta respuesta puede permitir que el sistema continúe funcionando, pero genera mensajes de diagnóstico intermitentes, falsos y molestos que requieren costosas visitas al emplazamiento por parte del servicio del pirata informático.

Por otro lado, si el sistema está instalado en un banco, la respuesta puede incluir una advertencia contundente al usuario de que el sistema ha dejado de funcionar debido a que la ciber-seguridad del sistema se ha visto comprometida.

Las respuestas, a modo de ejemplo, descritas anteriormente podrían iniciarse y ponerse en práctica, de manera autónoma mediante dispositivos periféricos, tales como interfaces de usuario o sensores.

Lo que antecede ilustra los aspectos descentralizados y matizados de este documento. De forma similar a cómo aumentan los aspectos centralizados la forma de tratar con piratas informáticos del sistema y las amenazas cibernéticas.

Debe entenderse que no se pretende o debe inferirse ninguna limitación con respecto al aparato específico ilustrado en este documento. Por supuesto, se pretende cubrir mediante las reivindicaciones adjuntas todas las modificaciones que caigan dentro del alcance de las reivindicaciones. Además, los flujos lógicos ilustrados en las figuras no requieren el orden particular mostrado, u orden secuencial, para lograr resultados deseables. Se pueden dar a conocer otras etapas, o se pueden eliminar etapas, a partir de los flujos descritos, y se pueden añadir otros componentes, o eliminarlos a partir de las formas de realización descritas.

REIVINDICACIONES

1. Un sistema que comprende:

un elemento de control común (12) en comunicación con una instalación de servicio de supervisión autenticada (22);

una pluralidad de detectores (14) acoplados al elemento de control común, en donde la pluralidad de detectores incluye sensores de condición, sensores de seguridad o sensores relativos a la automatización de edificios; y

una unidad de supervisión descentralizada, en donde la unidad de supervisión descentralizada realiza una evaluación de las comunicaciones entre la instalación de servicio de supervisión autenticada y el elemento de control común, para uno o más modelos que indican que al menos alguna de las comunicaciones proviene de una fuente no autenticada, distinta de la instalación de servicio de supervisión autenticada; y

en donde, cuando la unidad de supervisión descentralizada determina que al menos alguna de las comunicaciones proviene de la fuente no autorizada, el elemento de control común genera, de forma intermitente, mensajes de diagnóstico.

2. El sistema según la reivindicación 1, en donde cuando la unidad de supervisión descentralizada detecta la fuente no autenticada, la unidad de supervisión descentralizada genera mensajes de notificación o modifica el rendimiento de al menos uno de la pluralidad de detectores.

3. El sistema según la reivindicación 1 en donde, en respuesta a la determinación de que ningún modelo indica que las al menos algunas de las comunicaciones provienen de la fuente no autenticada, la unidad de supervisión descentralizada actualiza un registro local.

4. El sistema según la reivindicación 3, en donde la unidad de supervisión descentralizada transmite un indicio de autenticación al elemento de control común, en respuesta a la determinación de que ningún modelo indica que las al menos algunas de las comunicaciones provienen de la fuente no autenticada.

5. El sistema según la reivindicación 1, en donde la unidad de supervisión descentralizada comprende una pluralidad de unidades de supervisión descentralizadas.

6. El sistema según la reivindicación 1 en donde, en presencia de una fuente autenticada, el elemento de control común sigue transmitiendo las condiciones locales detectadas a la fuente autenticada.

7. El sistema según la reivindicación 6, en donde, en una presencia de la fuente no autenticada, la unidad de supervisión descentralizada proporciona indicios al elemento de control común indicativos de la fuente no autenticada.

8. Un método que comprende:

proporcionar un sistema de supervisión de zona que detecta condiciones en una zona asegurada, en donde un panel de control (12) del sistema de supervisión de zona, se comunica con una instalación de servicio de supervisión autenticada (22); y

proporcionar un sistema de supervisión descentralizado que al menos, de forma intermitente, realiza la autenticación de las comunicaciones entre el panel de control y la instalación de servicio de supervisión autenticada, mediante la evaluación de las comunicaciones para modelos que indican que al menos alguna de las comunicaciones proviene de una fuente no autenticada distinta de la instalación de servicio de supervisión autenticada,

en donde, cuando el sistema de supervisión descentralizado determina que la al menos alguna de las comunicaciones procede de la fuente no autenticada, el panel de control genera, de forma intermitente, mensajes de diagnóstico.

9. El método según la reivindicación 8 que comprende, además, la generación de un indicador en respuesta a un fallo de autenticación.

10. El método según la reivindicación 9 que comprende, además, la transmisión del indicador al sistema de supervisión de zona.

11. El método según la reivindicación 8 que comprende, además, la generación de indicadores de alerta a la detección de una instalación de supervisión no autenticada.

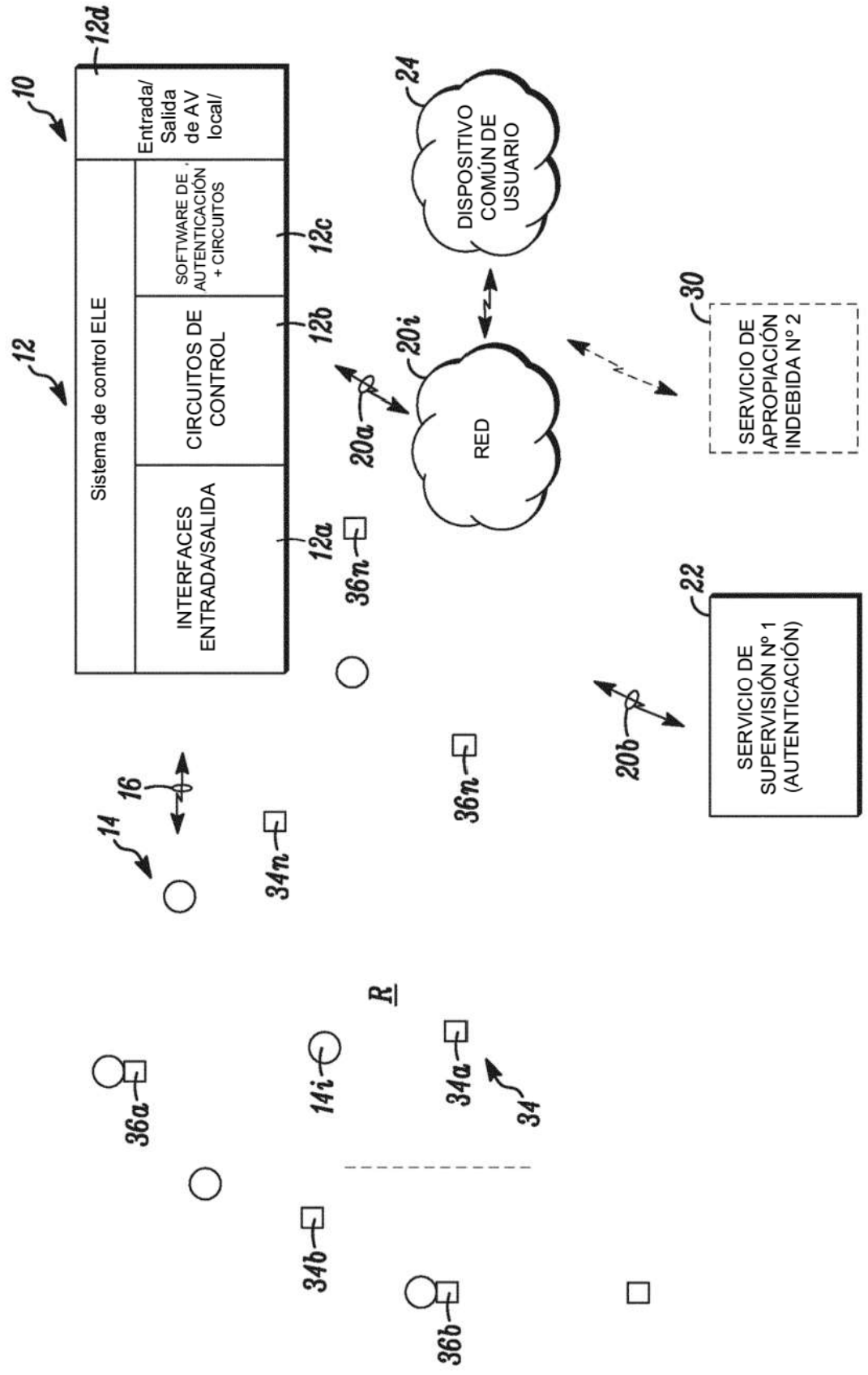
10
12d
Entrada/ Salida de AV local/
12
Sistema de control ELE
SOFTWARE DE AUTENTICACIÓN + CIRCUITOS
12c
CIRCUITOS DE CONTROL
12b
INTERFACES ENTRADA/SALIDA
12a
24
DISPOSITIVO COMÚN DE USUARIO
20a
20i
RED
30
SERVICIO DE APROPIACIÓN INDEBIDA Nº 2
22
SERVICIO DE SUPERVISIÓN Nº 1 (AUTENTICACIÓN)
20b
14
16
34n
36n
36n
R
14i
34a
34
36a
34b
36b

FIG. 1