(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 899**

(51) Int. CI.:
H04W 12/02 (2009.01)
H04M 1/673 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09156911 .1**
(96) Fecha de presentación: **22.07.2004**
(97) Número de publicación de la solicitud: **2071884**
(97) Fecha de publicación de la solicitud: **17.06.2009**

(54) Título: **SEGURIDAD PARA DISPOSITIVOS DE COMUNICACIONES MÓVILES.**

(30) Prioridad:
22.07.2003 GB 0317118

(45) Fecha de publicación de la mención BOPI:
07.03.2012

(45) Fecha de la publicación del folleto de la patente:
07.03.2012

(73) Titular/es:
RESEARCH IN MOTION LIMITED
295 Phillip Street
Waterloo, Ontario N2L 3W8 , CA

(72) Inventor/es:
Robertson, Ian

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Seguridad para dispositivos de comunicaciones móviles.

ANTECEDENTES DE LA INVENCIÓN

La presente invención se refiere a las comunicaciones móviles.

Como resultado de su movilidad, los dispositivos de comunicaciones móviles algunas veces se pierden o son robados. Frecuentemente, la pérdida de información almacenada en un dispositivo extraviado es de mayor preocupación que la pérdida del dispositivo en sí misma. Por ejemplo, el dispositivo puede tener información sensible y/o confidencial almacenada en él que podría causar daños si se adquiere por otros. Tal información sensible podría incluir, entre otras cosas, mensajes almacenados de naturaleza confidencial, e información de las comunicaciones almacenadas que permitiría a terceras partes hacerse pasar electrónicamente por la persona a la que legítimamente pertenece el dispositivo móvil.

En algunas redes de comunicación móvil, una vez que un usuario descubre que su dispositivo móvil está perdido, puede contactar con el operador de red y requerir que sea enviado un “paquete asesino” al dispositivo móvil perdido dando instrucciones al dispositivo para que borre la información sensible de su memoria. No obstante, tal sistema requiere que el usuario se dé cuenta que el dispositivo móvil está perdido, y que el dispositivo móvil está en comunicación con la red. Si el usuario depende del dispositivo para la comunicación, puede ser incapaz de informar de la pérdida o robo de una manera oportuna.

De esta manera, la seguridad de los dispositivos de comunicaciones móviles es una preocupación.

La US 6.542.729 B1 describe un sistema y método para minimizar el uso fraudulento de un teléfono móvil en el que el teléfono móvil es desactivado si una variación en el uso excede un determinado umbral. La US 5.862.472 describe un circuito y método de control para indicar la pérdida de un teléfono portátil en el que la generación de una alarma audible se detiene cuando se pone una determinada contraseña en la entrada. La US.6.370.402 B1 describe un terminal de radio portátil en el que una unidad de control del terminal portátil espera una contraseña y, en respuesta a la contraseña introducida, borra los contenidos de una memoria de registro de datos de usuario.

SUMARIO DE LA INVENCIÓN

De acuerdo con una realización ejemplo de la invención, hay proporcionado un dispositivo de comunicaciones móviles para comunicar con una red inalámbrica. El dispositivo de comunicaciones móviles incluye un almacenamiento electrónico que tiene datos almacenados inmediatamente después, un procesador conectado al almacenamiento para el acceso de los datos, un subsistema de comunicaciones conectado al procesador para el intercambio de señales con la red inalámbrica y con el procesador, un interfaz de entrada de usuario conectado para enviar las señales de entrada de usuario al procesador en respuesta a la acción del usuario, y un módulo de seguridad asociado con el procesador para detectar una condición de desencadenamiento que comprende una carencia de comunicación con la red inalámbrica durante un periodo de tiempo predeterminado, y tomar automáticamente una acción de seguridad si no se detecta una acción de desviación del usuario después de la detección de la condición de desencadenamiento, en la que la acción de seguridad incluye borrar los datos de, o cifrar los datos en, el almacenamiento electrónico.

De acuerdo con otra realización ejemplo la invención, hay proporcionado un método para proporcionar seguridad para un dispositivo de comunicación móvil que se configura para comunicar sobre una red de comunicaciones inalámbrica, que incluye los pasos de: (a) monitorizar la condición de desencadenamiento, que cubre una carencia de comunicación por el dispositivo con la red inalámbrica durante una extensión de tiempo predeterminada; (b) con posterioridad a la aparición de la condición de desencadenamiento, monitorizar una acción de desviación del usuario predeterminada en el dispositivo de comunicación móvil; y (c) tras el fallo para detectar la acción de desviación del usuario predeterminada dentro de una extensión de tiempo predeterminada después de la aparición de la condición de desencadenamiento, tomar automáticamente la acción de seguridad para proteger los datos almacenados en el dispositivo de comunicación móvil, en el que dicha acción de seguridad incluye el borrado de los datos almacenados en el dispositivo de comunicación móvil, o el cifrado de los datos almacenados en el dispositivo de comunicación móvil.

Otros aspectos y rasgos de la presente invención llegarán a ser evidentes a aquellos expertos ordinarios en la técnica tras la revisión de la siguiente descripción de las realizaciones específicas de la invención en conjunto con las Figuras anexas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Las realizaciones de la presente invención se describirán ahora, a modo de ejemplo solamente, con referencia a las

Figuras adjuntas, en las que:

La Figura 1 es un diagrama de bloques que muestra un sistema de comunicaciones que incluye un dispositivo de comunicaciones móviles para el cual la presente invención se puede aplicar;

La Figura 2 es un diagrama de flujo de un proceso de seguridad de acuerdo con las realizaciones de la invención.

Similares números de referencia se usan a través de las Figuras para indicar similares elementos y rasgos.

DESCRIPCIÓN DETALLADA

Con referencia ahora a los dibujos, la Figura 1 es un diagrama de bloques de un dispositivo de comunicación móvil 10 al que se aplica la presente invención en una realización ejemplo. El dispositivo de comunicación móvil 10 es un dispositivo de comunicación de dos vías que tiene al menos capacidades de comunicación de datos y preferentemente también de voz. El dispositivo preferentemente tiene la capacidad de comunicar con otros sistemas de ordenador en Internet. Dependiendo de la funcionalidad proporcionada por el dispositivo, en diversas realizaciones el dispositivo puede ser un dispositivo de comunicación de datos, un dispositivo de comunicación de modo múltiple configurado tanto para comunicación de voz y datos, un teléfono móvil, un PDA (asistente personal digital) habilitado para comunicación inalámbrica, o un sistema de ordenador con un módem inalámbrico, entre otras cosas.

El dispositivo incluye un subsistema de comunicación 11, que incluye un receptor 12, un transmisor 14, y los componentes asociados tales como uno o más, preferentemente integrados o internos, elementos de antena 16 y 18, osciladores locales (LO) 13, y un módulo de procesamiento tal como un procesador digital de señal (DSP) 20. Como será evidente para aquellos expertos en el campo de las comunicaciones, el diseño particular del subsistema de comunicación 11 será dependiente de la red de comunicación en la que se pretende que funcione el dispositivo.

Las señales recibidas por la antena 16 a través de una red de comunicación inalámbrica 50 se introducen al receptor 12, el cual puede realizar tales funciones de receptor común como la amplificación de señal, la conversión hacia abajo en frecuencia, el filtrado, la selección de canal y similares, y en algunas realizaciones, la conversión analógica a digital. De una manera similar, se procesan las señales a ser transmitidas, incluyendo la modulación y codificación por ejemplo, por el DSP 20 y se introducen al transmisor 14 para la conversión digital a analógica, la conversión hacia arriba en frecuencia, el filtrado, la amplificación y transmisión sobre la red de comunicaciones 50 a través de la antena 18. En ciertas realizaciones del dispositivo, la antena 16 y la antena 18 pueden ser la misma antena mientras que otras realizaciones incluirán dos sistemas de antena separados para una antena receptora y una antena transmisora.

El dispositivo 10 incluye un microprocesador 38 que controla la operación total del dispositivo. El microprocesador 38 interactúa con el subsistema de comunicaciones 11 y también interactúa con subsistemas del dispositivo adicionales tales como la pantalla 22, la memoria rápida 24, la memoria de acceso aleatorio (RAM) 26, los subsistemas auxiliares de entrada/salida (E/S) 28, el puerto serie 30, el teclado 32, el altavoz 34, el micrófono 36, un subsistema de comunicaciones de corto alcance 40, y cualesquiera otros subsistemas de dispositivo indicados de manera general como 42. Algunos de los subsistemas mostrados en la Figura 1 realizan las funciones de comunicación relacionadas, mientras que otros subsistemas pueden proporcionar las funciones “residentes” o en el dispositivo. Señaladamente, algunos subsistemas, tales como el teclado 32 y la pantalla 22 por ejemplo, se pueden usar tanto para las funciones de comunicación relacionadas, tales como introducir un mensaje texto para la transmisión sobre una red de comunicación, como las funciones residentes en el dispositivo tales como una calculadora o lista de tareas.

Los componentes lógicos del sistema operativo 54 y diversas aplicaciones de los componentes lógicos 58 usadas por el microprocesador 38 se almacenan, en una realización ejemplo, en un almacén permanente tal como una memoria rápida 24 o elemento de almacenamiento similar. Aquellos expertos en la técnica apreciarán que el sistema operativo 54, las aplicaciones del dispositivo específico 58, o partes de los mismos, se pueden cargar temporalmente en un almacén volátil tal como la RAM 26. Se contempla que las señales de comunicación recibidas también se pueden almacenar en la RAM 26.

El microprocesador 38, además de sus funciones de sistema operativo, preferentemente permite la ejecución de las aplicaciones de los componentes lógicos 58 en el dispositivo. Un conjunto predeterminado de aplicaciones 58 que controlan las operaciones básicas del dispositivo, incluyendo al menos las aplicaciones de comunicación de voz y datos por ejemplo, se instalarán normalmente en el dispositivo 10 durante la fabricación. También se pueden cargar aplicaciones adicionales en el dispositivo 10 a través de la red 50, un subsistema auxiliar de E/S 28, el puerto serie 30, el subsistema de comunicaciones de corto alcance 40 o cualquier otro subsistema adecuado 42, e instalar por un usuario en la RAM 26 o un almacén no volátil para la ejecución por el microprocesador 38. Tal flexibilidad en la instalación de la aplicación aumenta la funcionalidad del dispositivo y puede proporcionar funciones mejoradas en el dispositivo, funciones relacionadas con la comunicación, o ambas. Por ejemplo, las aplicaciones de comunicación

seguras pueden permitir las funciones de comercio electrónico y otras de tales transacciones financieras a ser realizadas usando el dispositivo 10.

En un modo de comunicación de datos, una señal recibida tal como una descarga de mensaje de texto o página en la red se procesará por el subsistema de comunicación 11 e introducirá al microprocesador 38, el cual procesará además preferentemente la señal recibida para sacar a la pantalla 22, o alternativamente a un dispositivo auxiliar de E/S 28. Un usuario del dispositivo 10 también puede componer elementos de datos tales como mensajes de correo electrónico por ejemplo, usando el teclado 32 en conjunto con la pantalla 22 y posiblemente un dispositivo auxiliar de E/S 28. Tales elementos compuestos se pueden transmitir entonces sobre una red de comunicación a través del subsistema de comunicación 11.

El puerto serie 30 en la Figura 1 se implementaría normalmente en un dispositivo de comunicación tipo asistente digital personal (PDA) para el cual puede ser deseable la sincronización con un ordenador de escritorio del usuario (no se muestra), pero es un componente del dispositivo opcional. Tal puerto 30 permitiría a un usuario establecer las preferencias a través de un dispositivo externo o la aplicación de componentes lógicos y extendería las capacidades del dispositivo proporcionando las descargas de información o programas informáticos al dispositivo 10 distintas de a través de una red de comunicación inalámbrica.

Un subsistema de comunicaciones de corto alcance 40 es un componente adicional que puede proporcionar la comunicación entre el dispositivo 10 y distintos sistemas o dispositivos, que no necesitan necesariamente ser dispositivos similares. Por ejemplo, el subsistema 40 puede incluir un dispositivo de infrarrojos y los circuitos y componentes asociados o un módulo de comunicación Bluetooth® para proporcionar la comunicación con sistemas y dispositivos habilitados de manera similar. El dispositivo 10 puede ser un dispositivo de mano.

En una realización ejemplo, la pasarela inalámbrica 62 se adapta para encaminar los paquetes de datos recibidos desde un dispositivo de comunicación móvil 10 sobre la red móvil inalámbrica 50 a un servidor de acceso de mensajería de correo electrónico de destino o Internet 68 a través de un sistema de conector inalámbrico 64, y encaminar los paquetes de datos recibidos desde el servidor 68 a través del sistema de conector inalámbrico 64 sobre la red móvil inalámbrica 50 a un dispositivo de comunicaciones móviles de destino. La red móvil inalámbrica 50 es, en una realización ejemplo, una red de paquetes de datos inalámbrica, (por ejemplo Mobitex® o DataTAC®), que proporciona cobertura de radio a los dispositivos móviles 10, aunque podría ser cualquier otro tipo de red inalámbrica. Dependiendo del tipo de red inalámbrica 50, puede ser necesario encaminar los paquetes de datos entre una conexión de pasarela inalámbrica TCP 62 y una conexión de red móvil de direcciones IP o X.25 y viceversa usando un mecanismo de encaminamiento intermedio que proporciona acceso a clientes TCP a una conexión X.25. Como se conoce convencionalmente, tal mecanismo inalámbrico podría usar, entre otras cosas, NET ID (DataTAC) o FST MAN (Mobitex) para conectar con la red móvil inalámbrica 50.

La pasarela inalámbrica 62 forma una conexión o puente entre los servidores y las redes inalámbricas asociadas con la comunicación de correo electrónico inalámbrica y/o el acceso a Internet. Específicamente, la pasarela inalámbrica 62 se acopla entre la red inalámbrica 50 y la red de datos cableada que incluye el sistema de conector inalámbrico 64 y el servidor de correo electrónico de destino 68. En una realización ejemplo, la pasarela inalámbrica 62 almacena la información de la configuración del sistema, los datos de estado del sistema, y las tablas de ese almacén de información del dispositivo móvil 10, y también incluye los módulos de transporte inalámbrico que hacen de interfaz entre los dispositivos móviles 10 y la pasarela inalámbrica 62. El módulo de transporte inalámbrico comunica con la red móvil inalámbrica 50 usando el mecanismo de encaminamiento intermedio tratado anteriormente (que proporciona acceso de clientes TCP a una conexión X.25 o UDP) y reúne los paquetes de datos que se reciben desde el dispositivo móvil 10 sobre la red móvil inalámbrica 50. Una vez que los paquetes de datos se reúnen, se envían a la capa superior del módulo de transporte inalámbrico para el procesamiento a través de la pasarela inalámbrica 62 para el sistema de conexión inalámbrico 64 y eventualmente para el servidor de correo electrónico de destino 68. El sistema de conector inalámbrico 64 es parte de la red troncal cableada y se acopla a la pasarela inalámbrica 62. El sistema de conector inalámbrico 64 comunica con la pasarela inalámbrica 62 y cada servidor de mensajes electrónicos que conecta con la pasarela inalámbrica como una dirección única. El servidor de correo 68 se acopla con el sistema de conector inalámbrico 64 y, en una realización, es un servidor de correo electrónico convencional.

El dispositivo móvil 10 almacena los datos de servicio 60 y otros datos 61 en una memoria permanente borrable, la cual en una realización ejemplo es la memoria rápida 24. En varias realizaciones, los datos de servicio 60 incluyen la información requerida por el dispositivo móvil para establecer y mantener las comunicaciones con la red de comunicaciones inalámbricas 50 (datos de servicio de red inalámbricos) y la pasarela inalámbrica 62 (datos de servicio pasarela). Otros datos 61 pueden incluir, entre otras cosas, los datos de aplicación de usuario tales como los mensajes de correo electrónico, el libro de direcciones y la información de contacto, el calendario y la información de planificación, los documentos de la libreta de notas, los archivos de imágenes, y otra información de usuario almacenada comúnmente en el dispositivo 10 por su usuario. Otros datos 61 también pueden incluir los datos requeridos para las capas de comunicaciones gestionadas por el sistema de conector inalámbrico 64 y los servidores 68.

Para proporcionar seguridad para un dispositivo móvil perdido o robado 10, el dispositivo 10 incluye un módulo de seguridad 56, que en una realización ejemplo es un componente de programa informático que es parte del sistema operativo 54. En otras realizaciones, el módulo de seguridad 56 es, o es parte de, una aplicación de componentes lógicos especializados 58 separada del sistema operativo 54. El módulo de seguridad 56 incluye instrucciones para la configuración del microprocesador 38 para hacer que el dispositivo 10 lleve a cabo el proceso de seguridad 200 que se muestra en la Figura 2. El proceso de seguridad 200 es en efecto un conmutador de "hombre muerto" en que configura el dispositivo para, tras la aparición de una o más condiciones de desencadenamiento predeterminadas, requerir que un usuario tome una acción de anulación o desviación de usuario predeterminada, so pena que el dispositivo móvil 10 tomará automáticamente medidas de seguridad activas.

En una realización ejemplo, el proceso de seguridad 200 está activo siempre que el dispositivo móvil 10 esté encendido. Como se indica en el paso 204, el proceso 200 incluye un paso 204 de comprobación para ver si una o más condiciones de desencadenamiento predeterminadas han sucedido. Tal paso de comprobación se lleva a cabo periódicamente hasta que un evento de desencadenamiento ocurre. En una realización ejemplo, un evento de desencadenamiento sucede cuando el dispositivo móvil 10 ha estado fuera de comunicación con la red inalámbrica 50 durante una extensión de tiempo predeterminada. Como se indicó en el paso 206, tras la aparición de un evento de desencadenamiento, el dispositivo 10 sugiere al usuario tomar la acción de desviación (paso 206) – por ejemplo, en una realización ejemplo, el dispositivo 10 sugiere al usuario que introduzca una contraseña u otro secreto compartido a través del teclado 32 o, en un dispositivo 10 que tenga capacidades de reconocimiento de voz, a través del micrófono 36. En diversas realizaciones, el dispositivo 10 sugiere al usuario tomar otras acciones o combinaciones de acciones además o en lugar de introducir una contraseña u otro secreto compartido, tal como, a modo de ejemplos no limitativos, sugerir a un usuario pasar una tarjeta que lleva la información de identificación a través de un lector de tarjeta adjunto al dispositivo 10; y/o sugerir al usuario mover el dispositivo de manera que restablezca las comunicaciones con la red inalámbrica 50. En algunas realizaciones, el dispositivo 10 salta el paso 206 y no sugiere activamente al usuario tomar una acción requerida, sino más bien solo espera la acción requerida a ser tomada después de que el evento de desencadenamiento ha ocurrido.

Como se indica en el paso 208, posterior a la aparición de un evento de desencadenamiento y después de sugerir al usuario actuar (en las realizaciones en las que se emite una sugerencia), el dispositivo 10 entonces determina si se toma la acción requerida. En diversas realizaciones ejemplo, la acción de desviación requerida debe ser completada con éxito dentro de una extensión de tiempo predeterminada (por ejemplo dentro de un tiempo "efectivo") posterior a la aparición del evento de desencadenamiento, y/o dentro de un número predeterminado de intentos en la acción (por ejemplo, dentro de tres intentos para introducir la contraseña), de otro modo el dispositivo 10 procederá a tomar medidas de seguridad de precaución. En una realización, el módulo de seguridad 56 provoca que el dispositivo 10 suspenda temporalmente todas las funciones de comunicaciones o las seleccionadas y llegue a estar no operativo de manera efectiva durante el tiempo efectivo, rechazando todas las acciones del usuario intentadas distintas de la acción de desviación. De esta manera, durante el tiempo efectivo el usuario no tiene otra opción distinta de tomar la acción de desviación requerida, y no puede acceder a los datos almacenados o hacer llamadas de teléfono (en los dispositivos habilitados con teléfono) o enviar correos electrónicos (en los dispositivos habilitados con correo electrónico), por ejemplo. En algunas realizaciones habilitadas con teléfono, se pueden permitir las llamadas al 112 durante el tiempo efectivo. En las realizaciones alternativas, se puede mantener completamente la funcionalidad normal durante el tiempo efectivo. Si la acción de desviación requerida se toma con éxito dentro del tiempo efectivo, la funcionalidad del dispositivo se restaura, y el proceso de seguridad vuelve a monitorizar el siguiente evento de desencadenamiento (paso 204).

Volviendo ahora al paso 210, en el caso de que la acción de desviación requerida no se tome con éxito por el usuario en el paso 208 dentro del tiempo efectivo predeterminado o el límite de intentos, el dispositivo 10 automáticamente emprende las medidas de protección de la información. En una realización, el dispositivo 10, para proteger los datos almacenados en el dispositivo 10 de caer en las manos equivocadas o ser usado sin autorización, el módulo de seguridad 56 borra o elimina todos o las partes seleccionadas de los datos de servicio 60 que están almacenados en el almacén permanente y volátil del dispositivo 10. En una realización ejemplo, los datos de servicio 60 requeridos para establecer y mantener la comunicación entre el dispositivo 10 y la red inalámbrica 50 se borran permanentemente, deshabilitando de manera efectiva la capacidad de comunicaciones del dispositivo móvil 10. En algunas realizaciones en las que el dispositivo incluye un teléfono inalámbrico, el servicio de emergencias 112 se puede mantener exclusivamente. Los datos de servicio requeridos para establecer y mantener las comunicaciones a través de la pasarela inalámbrica 62, en diversas realizaciones, también o alternativamente se borran. En diversas realizaciones, además o en lugar de los datos de servicio 60, las partes seleccionadas de todos los otros datos 61 en el dispositivo móvil 10, que incluyen datos de usuario tales como los mensajes de correo electrónico, las listas de contactos y libro de direcciones, el calendario y la información de planificación, los documentos de la libreta de notas, los archivos de imágenes y texto, y/u otra información de usuario se borran permanentemente del almacenamiento del dispositivo móvil 10. De esta manera, en el paso 210, en diversas realizaciones, la información requerida por el dispositivo 10 para funcionar como un dispositivo de comunicaciones se borra, y cualquier texto u otra información que pueda ser confidencial para el usuario se borra, extrayendo por ello, entre otras cosas, la información del dispositivo 10 que podría ser usada por otros para hacerse pasar electrónicamente por el usuario autorizado del dispositivo 10. En diversas realizaciones, la acción de seguridad de protección de datos tomada en el paso 210 incluye cifrar todos o las partes seleccionadas de los datos de servicio y/u otros datos, haciendo tales

datos inutilizables temporalmente, en lugar de borrarlos. En tales realizaciones, el dispositivo 10 tiene un motor de cifrado instalado localmente, y una clave de cifrado almacenada en la memoria permanente del dispositivo se usa para el cifrado. Durante o después del proceso de cifrado, la clave de cifrado o bien es borrada o bien es cifrada para protegerla. Una vez cifrada, se debe obtener una clave de descifrado a partir de una fuente segura de una tercera parte (por ejemplo, el operador de la red inalámbrica 50 y/o la pasarela inalámbrica 62) para descifrar los datos.

En diversas realizaciones, otras condiciones de desencadenamiento predeterminadas son los eventos de desencadenamiento en el paso 204. Por ejemplo, en una realización, la variación en la entrada de usuario de un umbral predeterminado, tal como la carencia de actividad del teclado durante una extensión predeterminada, se usa para desencadenar el requerimiento de la acción del usuario, so pena que las medidas de protección de la información sean tomadas. En algunas realizaciones, las condiciones de desencadenamiento se pueden basar en cambios en las comunicaciones, mensajería o características o patrones de uso del dispositivo 10. Por ejemplo una condición de desencadenamiento podría resultar cuando el volumen de paquetes de datos enviados o recibidos por el dispositivo sobre el tráfico de la red inalámbrica exceda un umbral predeterminado, o cuando el patrón de las estaciones base usado en las comunicaciones varíe a partir de los umbrales predeterminados. Una condición de desencadenamiento podría resultar si el dispositivo estuvo fuera de un área de cobertura predeterminada. En algunas realizaciones, los umbrales para la determinación de las condiciones de desencadenamiento se podrían configurar de manera adaptativa por el módulo de seguridad en base a las características de funcionamiento normales del dispositivo 10.

Las realizaciones descritas anteriormente de la presente invención se pretende que sean solamente ejemplos. Alteraciones, modificaciones y variaciones pueden ser efectuadas a las realizaciones particulares por aquellos expertos en la técnica sin salirse del alcance de la invención, el cual se define por las reivindicaciones adjuntas a esto.

REIVINDICACIONES

1. Un dispositivo de comunicaciones móviles (10) para comunicar con una red inalámbrica (50) que comprende:

un almacenamiento electrónico (24) que tiene datos almacenados inmediatamente después;
un procesador (38) conectado con el almacenamiento (24) para acceder a los datos;
un subsistema de comunicación (11) conectado con el procesador (38) para intercambiar las señales con la red inalámbrica (50) y con el procesador (38);
un interfaz de entrada de usuario conectado para enviar las señales de entrada de usuario al procesador (38) en respuesta a la acción del usuario; y,
un módulo de seguridad (56) asociado con el procesador (38) para borrar una condición de desencadenamiento que comprende una carencia de comunicación por el dispositivo (10) con la red inalámbrica (50) durante una extensión de tiempo predeterminada, y para tomar automáticamente una acción de seguridad si una acción de desviación del usuario no se detecta a través del interfaz de entrada de usuario después de la detección de la condición de desencadenamiento,
en el que la acción de seguridad incluye el borrado de los datos de, o cifrado de datos en, el almacenamiento electrónico.

2. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que la acción de seguridad incluye el borrado de todos los datos o los seleccionados del almacenamiento (24) para proteger los datos.

3. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que la acción de seguridad incluye el cifrado de todos los datos o los seleccionados del almacenamiento (24) para proteger los datos.

4. El dispositivo de comunicaciones móviles (10) de la reivindicación 3, en el que una clave de cifrado almacenada en el almacenamiento (24) del dispositivo se usa para el cifrado y en el que el dispositivo de dispone a borrar la clave de cifrado durante o después del cifrado.

5. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que los datos incluyen los datos de servicio requeridos por el dispositivo móvil (10) para comunicar con éxito sobre la red inalámbrica (50) y en el que la acción de seguridad incluye el borrado de los datos de servicio del almacenamiento (24).

6. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que la acción de seguridad incluye deshabilitar una capacidad del dispositivo (10) para comunicar con la red inalámbrica (50).

7. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que el interfaz de entrada de usuario incluye el un teclado y en el que la condición de desencadenamiento incluye la inactividad del interfaz de entrada de usuario durante una extensión predeterminada.

8. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que el módulo de seguridad toma la acción de seguridad si la acción de desviación del usuario no se detecta dentro de una extensión predeterminada después de la detección de la condición de desencadenamiento.

9. El dispositivo de comunicaciones móviles (10) de la reivindicación 8, en el que el módulo de seguridad toma la acción de seguridad si la acción de desviación del usuario no se detecta dentro del número de intentos predeterminado por el usuario para tomar la acción de desviación de usuario.

10. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que la acción de desviación del usuario incluye la entrada de un secreto compartido por el dispositivo (10) y el usuario a través del interfaz de entrada de usuario.

11. El dispositivo de comunicaciones móviles (10) de la reivindicación 1, en el que el dispositivo incluye un dispositivo de salida de usuario para emitir una sugerencia para la acción, el módulo de seguridad (56) que provoca que la sugerencia sea emitida tras la detección de la condición de desencadenamiento.

12. Un método de suministrar seguridad para un dispositivo de comunicaciones móviles (10) que está configurado para comunicar sobre una red de comunicaciones inalámbricas (50), que incluye los pasos de:

(a) monitorizar una condición de desencadenamiento que comprende una carencia de comunicación por el dispositivo (10) con la red inalámbrica (50) durante una extensión de tiempo predeterminada;
(b) posterior a la aparición de la condición de desencadenamiento, monitorizar una acción de desviación del usuario predeterminada en el dispositivo de comunicaciones inalámbricas (10); y,
(c) tras el fallo para detectar la acción de desviación del usuario predeterminada dentro de una extensión de tiempo predeterminada después de la aparición de la condición de desencadenamiento, tomar automáticamente la acción de seguridad para proteger los datos almacenados en el dispositivo de comunicación móvil (10), en el que la acción de seguridad incluye el borrado de los datos almacenados en el

dispositivo de comunicación móvil (10), o el cifrado de los datos almacenados en el dispositivo de comunicación móvil (10).

13. El método de la reivindicación 12, en el que los datos almacenados en el dispositivo de comunicación móvil (10) incluyen los datos de servicio requeridos por el dispositivo de comunicación móvil (10) para comunicar sobre la red de comunicaciones inalámbrica (50), la acción de seguridad que incluye borrar permanentemente los datos de servicio almacenados en el dispositivo de comunicación móvil (10).

14. El método de la reivindicación 12, en el que la acción de seguridad incluye el cifrado de al menos alguno de los datos almacenados en el dispositivo de comunicación móvil (10).

15. El método de la reivindicación 12, que incluye la emisión de una sugerencia para tomar la acción tras la aparición de la condición de desencadenamiento.

16. El método de la reivindicación 12, que incluye la monitorización de un número de intentos de acción de desviación del usuario y en el paso (c) también tomar la acción de seguridad si la acción de desviación del usuario no se toma con éxito dentro de un número de intentos predeterminado.

17. El método de la reivindicación 12, en el que al menos algunas funciones de comunicaciones del dispositivo (10) se suspenden durante la extensión de tiempo predeterminada.

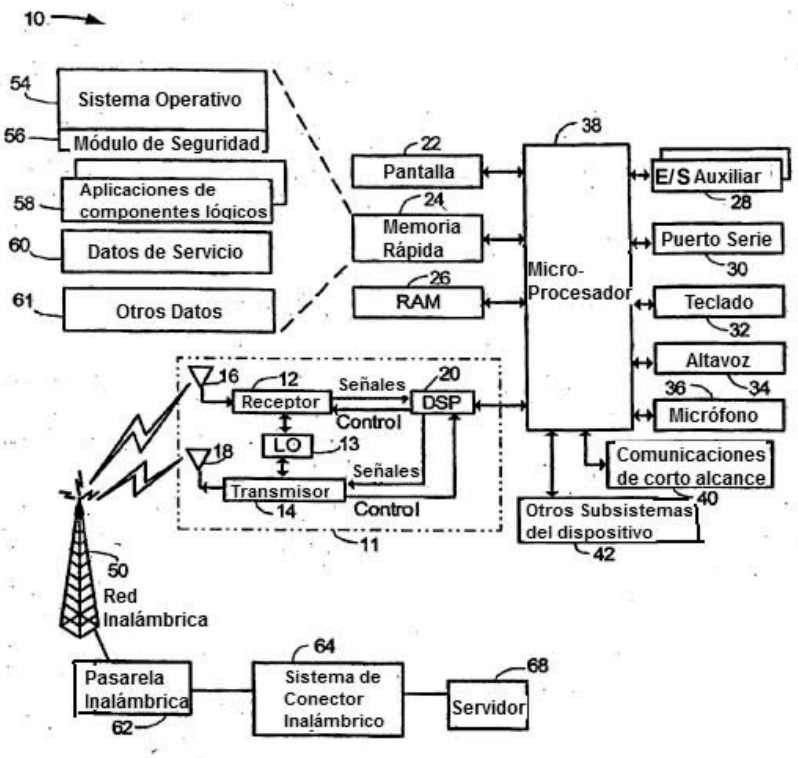
10
54
Sistema Operativo
56
Módulo de Seguridad
58
Aplicaciones de componentes lógicos
60
Datos de Servicio
61
Otros Datos
22
Pantalla
24
Memoria Rápida
26
RAM
38
Micro-Procesador
E/S Auxiliar
28
Puerto Serie
30
Teclado
32
Altavoz
34
36
Micrófono
16
12
Receptor
Señales
20
DSP
Control
LO
13
18
Señales
Transmisor
14
Control
11
Comunicaciones de corto alcance
40
Otros Subsistemas del dispositivo
42
50
Red Inalámbrica
64
Pasarela Inalámbrica
62
Sistema de Conector Inalámbrico
68
Servidor

FIG. 1

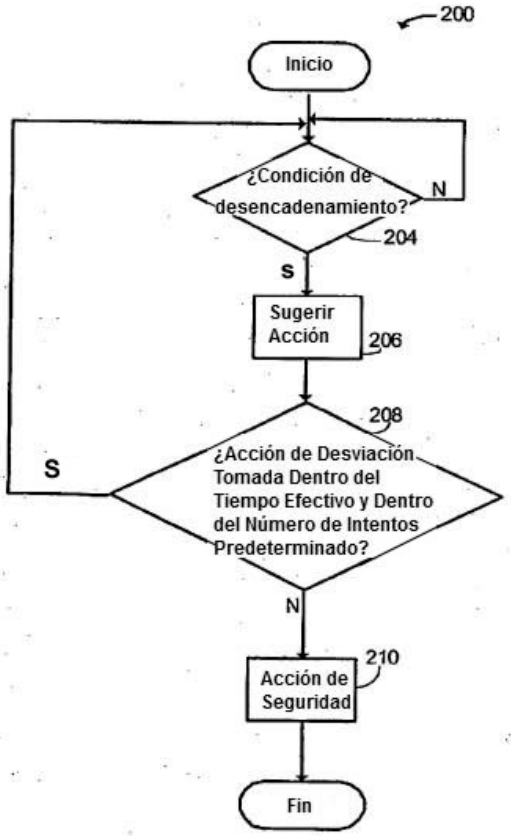
200
Inicio
¿Condición de desencadenamiento?
N
204
S
Sugerir Acción
206
208
¿Acción de Desviación Tomada Dentro del Tiempo Efectivo y Dentro del Número de Intentos Predeterminado?
S
N
210
Acción de Seguridad
Fin

FIG. 2