(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 808 954**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04W 12/08 (2009.01)
H04W 4/12 (2009.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)
H04W 4/14 (2009.01)
G06F 21/53 (2013.01)
G06F 16/23 (2009.01)
G06F 16/951 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.10.2016 PCT/CN2016/103489**

(87) Fecha y número de publicación internacional: **11.05.2017 WO17076210**

(96) Fecha de presentación y número de la solicitud europea: **27.10.2016 E 16861478 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3373626**

(54) Título: **Procedimiento y dispositivo para su uso en la gestión de riesgos de información de aplicación**

(30) Prioridad:

05.11.2015 CN 201510746296

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.03.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

LI, LIZHONG y
ZHANG, YANAN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento y dispositivo para su uso en la gestión de riesgos de información de aplicación

La presente solicitud reivindica la prioridad de la solicitud de patente china n.º 201510746296.6, presentada el 5 de noviembre de 2015, y titulada "PROCEDIMIENTO Y DISPOSITIVO PARA LA GESTIÓN DE RIESGOS DE INFORMACIÓN DE APLICACIÓN".

Campo técnico

La presente solicitud se refiere al campo de la informática, y en particular, a una tecnología de gestión de riesgos de información de aplicación.

Antecedentes

Para procesar información de aplicación de riesgo tal como un mensaje SMS sospechoso de *phishing* (*Smishing*), habitualmente en el teléfono móvil de un usuario tiene que instalarse el software de seguridad correspondiente, de modo que el usuario pueda utilizar el software de seguridad para cargar todos los mensajes SMS en el teléfono móvil del usuario a la nube, y a continuación la nube realiza un análisis de detección a todos los mensajes SMS de uno en uno. En todo el proceso tanto el volumen de los datos transmitidos como el volumen de los datos de validación son relativamente grandes, el riesgo de pérdida de la privacidad del usuario es relativamente elevado y el nivel de participación del usuario en la gestión de la información sobre la privacidad del usuario es bajo. Por consiguiente, la experiencia del usuario es mala.

El documento US 2008/189770 A1 describe procedimientos y sistemas para autenticar y para marcar mensajes de correo electrónico como de confianza.

El documento US 2008/082662 A1 describe un procedimiento y aparato para controlar el acceso a los recursos de red basándose en la reputación.

El documento WO 2015/105222 A1 describe técnicas para evitar que se jaquee un terminal móvil y un sistema y un procedimiento para identificar si la información de enlace es segura.

El documento WO2014148854 da a conocer un procedimiento que permite a un usuario identificar si un mensaje de autenticación transmitido al terminal de comunicación móvil del usuario procede de una fuente de confianza, evitando así un daño producido por *pharming*, *Smishing*.

Sumario

Cuando los mensajes SMS en un equipo de usuario se cargan a un dispositivo de red, la eficiencia de gestión de los mensajes SMS es baja y el riesgo de pérdida de la privacidad del usuario es relativamente alto. La presente solicitud pretende proporcionar un procedimiento y un dispositivo para la gestión de riesgos de información de aplicación y para solucionar estos problemas.

La presente invención se define por las reivindicaciones independientes. Las reivindicaciones dependientes muestran formas de realización ventajosas de la presente invención.

Breve descripción de los dibujos

Tras leer una descripción detallada de las formas de realización no limitativas con referencia a los siguientes dibujos adjuntos resultarán más evidentes otras características, objetivos y ventajas de la presente solicitud.

La figura 1 muestra un diagrama esquemático de un dispositivo de red para la gestión de riesgos de información de aplicación basándose en un aspecto de la presente solicitud.

La figura 2 muestra un diagrama esquemático de un sistema de un dispositivo de red y un equipo de usuario para la gestión de riesgos de información de aplicación basándose en una forma de realización preferida de la presente solicitud.

La figura 3 muestra un diagrama de flujo de un procedimiento para la gestión de riesgos de información de aplicación del lado del dispositivo de red basándose en otro aspecto de la presente solicitud.

La figura 4 muestra un diagrama de flujo de un procedimiento para la gestión de riesgos de información de aplicación del lado del dispositivo de red y del lado del equipo de usuario.

Los números de referencia iguales o similares en los dibujos adjuntos representan componentes iguales o similares.

Descripción de formas de realización

A continuación, se describen las formas de realización de la presente solicitud en detalle con referencia a los dibujos adjuntos.

En una configuración típica de la presente solicitud, un terminal, un dispositivo de red de servicio y una parte confiable incluyen en cada caso una o varias unidades de procesamiento central (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria no persistente, una memoria de acceso aleatorio (RAM), una memoria no volátil, etc. en un medio legible por ordenador, por ejemplo, una memoria de solo lectura (ROM) o una memoria flash (flash RAM). La memoria es un ejemplo del medio legible por ordenador.

El medio legible por ordenador incluye medios persistentes, no persistentes, portátiles y no portátiles que pueden implementar un almacenamiento de información utilizando cualquier procedimiento o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Un medio de almacenamiento informático incluye, pero no está limitado a, una memoria de cambio de fase (PRAM), una memoria de acceso aleatorio estática (SRAM), una memoria de acceso aleatorio dinámica (DRAM), una memoria de acceso aleatorio (RAM) de otro tipo, una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otra tecnología de memoria, una memoria de solo lectura de disco compacto (CD-ROM), un disco versátil digital (DVD), u otro almacenamiento óptico, un casete, un almacenamiento de disco magnético de casete, u otro dispositivo de almacenamiento magnético o cualquier otro medio que no sea de transmisión. El medio de almacenamiento informático puede estar configurado para almacenar información a la que puede accederse mediante un dispositivo informático. Basándose en una definición en esta memoria descriptiva, el medio legible por ordenador no incluye un medio de almacenamiento legible por ordenador no transitorio, tal como una señal digital modulada y una portadora.

La figura 1 muestra un diagrama esquemático de un dispositivo de red 1 para la gestión de riesgos de información de aplicación basándose en un aspecto de la presente solicitud.

El dispositivo de red 1 incluye un aparato de adquisición de información de aplicación objetivo 11, un aparato de validación de información de aplicación objetivo 12 y un aparato de envío de información de aviso 13. El aparato de adquisición de información de aplicación objetivo 11 adquiere información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando el equipo de usuario 2. El aparato de validación de información de aplicación objetivo 12 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. El aparato de envío de información de aviso 13 devuelve la información de aviso correspondiente al equipo de usuario basándose en la información de riesgo.

Específicamente, el aparato de adquisición de información de aplicación objetivo 11 adquiere la información de aplicación objetivo que selecciona el usuario y cuya validación solicita utilizando el equipo de usuario 2 (con referencia a la figura 2). En este caso, el dispositivo de red 1 incluye varios terminales inteligentes, como varios servidores en la nube o grupos de servidores. El equipo de usuario 2 incluye varios dispositivos terminales inteligentes, como varios ordenadores personales y teléfonos inteligentes. En este caso, la información de aplicación incluye, pero no está limitada a, un mensaje SMS, un mensaje de WeChat, un correo electrónico, u otra información transferida basándose en un programa de aplicación específico en el equipo de usuario 2. En este caso, la información de aplicación objetivo adquirida por el dispositivo de red 1 procede del equipo de usuario 2 correspondiente. Preferiblemente, la información de aplicación objetivo se selecciona de manera autónoma por el usuario de la información de aplicación en una aplicación objetivo del equipo de usuario 2. Por ejemplo, el usuario puede copiar la información de aplicación objetivo en un cuadro de texto, y seleccionar para enviar la información de aplicación objetivo. A continuación, el equipo de usuario 2 envía la información de aplicación objetivo al dispositivo de red 1 correspondiente. Como otro ejemplo, el usuario puede seleccionar y enviar directamente la información de aplicación objetivo en una aplicación. En este caso, preferiblemente, el dispositivo de red 1 adquiere la información de aplicación objetivo enviada por el equipo de usuario 2 con una transmisión cifrada. Por ejemplo, la información de aplicación objetivo es un mensaje SMS. Cuando el usuario entra en una interfaz de aplicación de SMS del equipo de usuario 2, como un teléfono móvil, el usuario selecciona directamente un mensaje sospechoso de *Smishing* de varios mensajes SMS visualizados, y determina una información o varias informaciones de aplicación objetivo en la/s que se realizará la validación de riesgo. A continuación, el aparato de adquisición de información de aplicación objetivo 11 del dispositivo de red 1 adquiere la información de aplicación objetivo seleccionada por el usuario y una solicitud de validación correspondiente.

En este caso, la información de aplicación objetivo adquirida por el aparato de adquisición de información de aplicación objetivo 11 puede estar en la forma original de la información de aplicación objetivo adquirida por el equipo de usuario

2. Por ejemplo, si la información de aplicación objetivo es un mensaje SMS, la información de aplicación objetivo adquirida por el dispositivo de red 1 puede estar en forma de un texto de mensaje SMS visualizado en la interfaz de aplicación de SMS del equipo de usuario 2. Además, el equipo de usuario 2 puede analizar en primer lugar la información de aplicación original recibida por el equipo de usuario 2 o extraer la información de la información de aplicación original. Por ejemplo, el equipo de usuario 2 extrae una palabra clave de un mensaje SMS basándose en una categoría y envía la palabra clave extraída al dispositivo de red 1. Así, la información de aplicación objetivo que va a validarse puede analizarse y clasificarse de forma preliminar, y se reduce un volumen de datos transmitidos entre los dispositivos.

Además, cuando se adquiere la información de aplicación objetivo, el dispositivo de red 1 puede adquirir de manera correspondiente información de atributo relacionada de la información de aplicación objetivo, como información de remitente de la información de aplicación objetivo o información de guía de usuario de la información de aplicación objetivo.

Después, el aparato de validación de información de aplicación objetivo 12 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. En este caso, en la presente solicitud, el dispositivo de red 1 realiza un análisis de validación de riesgo en la información de aplicación objetivo utilizando el dispositivo de red 1. En este caso, un riesgo de la información de aplicación objetivo puede incluir un riesgo directo impuesto a la seguridad de la privacidad del usuario y la seguridad del equipo de usuario, y además puede incluir un riesgo potencial impuesto al usuario por información de aplicación basura, como un anuncio falso. Para validar la información de aplicación objetivo, la información de aplicación objetivo y la información de atributo relacionada pueden considerarse o evaluarse exhaustivamente por medio de clasificación. En este caso, de manera flexible pueden seleccionarse y combinarse procedimientos de validación específicos basándose en las necesidades reales. Por ejemplo, la información de aplicación objetivo puede validarse y analizarse basándose en una base de datos de validación previamente existente. Como otro ejemplo, puede realizarse una ejecución de simulación en la información de guía de usuario de la información de aplicación objetivo en un entorno de pruebas seguro para identificar si la información de aplicación objetivo incluye información de riesgo. Por ejemplo, la seguridad de la información de aplicación objetivo puede validarse múltiples veces combinando una pluralidad de procedimientos de validación. Por ejemplo, la información de aplicación objetivo se valida utilizando por separado los procedimientos descritos en los dos ejemplos anteriores para mejorar la precisión de la información de riesgo obtenida finalmente. En este caso, la información de riesgo puede incluir información determinante de que existe un riesgo o información determinante de que no existe ningún riesgo. Además, preferiblemente, la información determinante de que existe un riesgo puede clasificarse y organizarse específicamente basándose en el contenido del riesgo y la consecuencia negativa producida por el riesgo. Por ejemplo, si la información de aplicación objetivo incluye contenido como un sitio web de *phishing*, un troyano o una estación base no autorizada y similar, un valor de riesgo de la información de aplicación objetivo se establece en un 99%, o se define que la información de aplicación objetivo está en un alto nivel de riesgo.

Después, el aparato de envío de información de aviso 13 devuelve, basándose en la información de riesgo, la información de aviso correspondiente al equipo de usuario 2. En este caso, preferiblemente, el dispositivo de red 1 genera la información de aviso correspondiente basándose en la información de riesgo obtenida mediante validación, y devuelve la información de aviso al equipo de usuario 2. Por ejemplo, cuando la información de riesgo es la información determinante de que existe un riesgo, como cuando la información de riesgo es que un mensaje SMS objetivo es información falsa, se genera la información de aviso de riesgo correspondiente. El contenido de la información de aviso de riesgo puede incluir destacar un mensaje SMS con un aviso de riesgo en el equipo de usuario 2, un mensaje SMS de aviso específico, o información de aviso en otra forma, o incluso un proceso directo del mensaje SMS como mensaje SMS basura por el equipo de usuario 2, etc. Como otro ejemplo, cuando la información de riesgo es la información determinante de que no existe ningún riesgo, la información de seguridad de validación correspondiente puede enviarse al equipo de usuario 2.

En la presente solicitud, la información de aplicación objetivo que selecciona el usuario y cuya validación solicita se valida utilizando el dispositivo de red 1, y la información de aviso correspondiente a la información de riesgo obtenida mediante validación se devuelve al equipo de usuario 2 correspondiente. En este caso, el usuario puede seleccionar directamente una información o varias informaciones de aplicación objetivo de una interfaz de información de aplicación correspondiente del equipo de usuario sin tener que saltar a una operación de aplicación de terceros. Además, el usuario puede determinar de manera autónoma parte de o toda la información de aplicación objetivo a cargar. Por tanto, se mejora el nivel de participación de un usuario en la gestión de la información sobre la privacidad del usuario y se reduce la probabilidad de pérdida de la privacidad del usuario. Además, con una selección flexible, puede reducirse un volumen de datos transmitidos entre los dispositivos, de modo que por consiguiente se reduce un volumen de datos de validación que procesa el dispositivo de red, y se mejora la eficiencia de la gestión de riesgos de información de aplicación global.

En una forma de realización preferida, el aparato de validación de información de aplicación objetivo 12 incluye una unidad de búsqueda de coincidencias (no mostrada) y una primera unidad de determinación de información de riesgo (no mostrada). La unidad de búsqueda de coincidencias realiza una búsqueda de coincidencias en una base de datos

de validación correspondiente basándose en la información de atributo relacionada de la información de aplicación objetivo. La primera unidad de determinación de información de riesgo determina la información de riesgo correspondiente basándose en información de registro que está en la base de datos de validación y que coincide con la información de atributo relacionada.

Específicamente, la unidad de búsqueda de coincidencias realiza una búsqueda de coincidencias en la base de datos de validación correspondiente basándose en la información de atributo relacionada de la información de aplicación objetivo. En este caso, la base de datos de validación es preferiblemente una biblioteca de plantillas de mensajes SMS, una biblioteca de sitios web de *phishing*, una biblioteca de virus troyanos, etc. La biblioteca de plantillas de mensajes SMS incluye un mensaje SMS que se determina como plantilla, y que recopila el dispositivo de red 1 y tiene un alto factor de riesgo histórico, como un mensaje de *Smishing* determinado, o una plantilla de mensajes SMS derivada con una similitud relativamente alta deducida basándose en un mensaje de *Smishing* previamente conocido. La biblioteca de sitios web de *phishing*, la biblioteca de virus troyanos, etc., incluyen información sobre un sitio web que recopila el dispositivo de red 1 y que se determina como un sitio web de *phishing*, o información sobre un archivo que se determina que incluye un virus troyano. La información en la biblioteca de sitios web de *phishing* anterior y la biblioteca de virus troyanos pueden extraerse directamente de la información de aplicación en cada equipo de usuario 2, o pueden ser datos existentes de otra base de datos, o un dispositivo de terceros. En este caso, la información de atributo relacionada incluye cualquier información que está asociada con la información de aplicación objetivo, por ejemplo, información de remitente de la información de aplicación objetivo, la información de contenido de la información de aplicación objetivo, información de guía de usuario de la información de aplicación objetivo, etc. En este caso, basándose en los tipos de las bases de datos de validación diferentes, puede realizarse una búsqueda de coincidencias correspondiente en información apropiada seleccionada de la información de atributo relacionada de la información de aplicación objetivo. Por ejemplo, cuando la base de datos de validación es una biblioteca de sitios web de *phishing*, puede seleccionarse la información de guía de usuario de la información de aplicación objetivo. Por ejemplo, un mensaje SMS objetivo incluye información sobre un sitio web, y se realiza una búsqueda de coincidencias en la información. Como otro ejemplo, si la base de datos de validación es la biblioteca de plantillas de mensajes SMS, se selecciona el contenido de la información de aplicación objetivo, y se realiza una búsqueda de coincidencias en el contenido. En este caso, preferiblemente, cuando una pluralidad de tipos de bases de datos de validación están preconfigurados en el dispositivo de red 1, pueden seleccionarse una o varias bases de datos de validación y utilizarse como base de datos de referencia basándose en las necesidades, por ejemplo, basándose en la selección de un usuario, o basándose en una decisión inteligente de un tipo de la información de aplicación objetivo. Además, preferiblemente, cada base de datos de validación puede clasificarse basándose en el nivel de riesgo correspondiente a la información de aplicación, y se selecciona una base de datos de validación en una clasificación específica para la información de aplicación objetivo basándose en la clasificación, o se seleccionan bases de datos de validación en una pluralidad de clasificaciones para validar sucesivamente la información de aplicación objetivo.

En este caso, un experto en la técnica entenderá que la biblioteca de plantillas de mensajes SMS, la biblioteca de sitios web de *phishing* y la biblioteca de virus troyanos son sólo ejemplos, y que una base de datos existente o una base de datos futura que puedan utilizarse para la validación de información de aplicación objetivo y es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

Después, la primera unidad de determinación de información de riesgo determina la información de riesgo correspondiente basándose en la información de registro que está en la base de datos de validación y que coincide con la información de atributo relacionada. En este caso, si la información de registro que coincide con la información de atributo relacionada se identifica en la base de datos de validación correspondiente, por ejemplo, si un mensaje SMS objetivo incluye información sobre un sitio web, y su registro correspondiente en la biblioteca de sitios web de *phishing* es un sitio web de *phishing*. Como otro ejemplo, si el contenido de texto mencionado anteriormente del mensaje SMS objetivo es coherente con el contenido de una plantilla de mensaje de *Smishing* en la biblioteca de plantillas de mensajes SMS, puede determinarse la información de riesgo correspondiente a la información de aplicación objetivo, por ejemplo, como la información determinante de que existe un riesgo, o, además, la información de riesgo incluye información de nivel de riesgo correspondiente.

Además, cuando la base de datos de validación no incluye la información de registro que coincide con la información de atributo relacionada, puede deducirse que la información de aplicación objetivo es información de seguridad con un riesgo relativamente bajo basándose en las necesidades, y la información de seguridad de validación correspondiente se devuelve al equipo de usuario 2. Alternativamente, se selecciona otra base de datos de validación o incluso otro procedimiento de validación para la validación de riesgo, y se proporciona información de riesgo correspondiente. Por ejemplo, cuando no puede hacerse coincidir información de registro correspondiente utilizando la biblioteca de plantillas de mensajes SMS, adicionalmente se realizan búsquedas de coincidencias basándose en la biblioteca de sitios web de *phishing*. Como otro ejemplo, cuando no puede hacerse coincidir información de registro correspondiente en todas o algunas de las bases de datos de validación predeterminadas, la coincidencia puede realizarse en otro procedimiento de validación, por ejemplo, coincidiendo con una biblioteca de mensajes SMS/números de teléfono de una institución financiera. Por ejemplo, puede realizarse una ejecución de simulación en

la información de guía de usuario de la información de aplicación objetivo en un entorno de pruebas seguro para identificar si la información de aplicación objetivo incluye información de riesgo.

Preferiblemente, la información de atributo relacionada incluye al menos una de las siguientes: información de remitente de la información de aplicación objetivo, información de contenido de la información de aplicación objetivo o información de guía de usuario de la información de aplicación objetivo.

En este caso, específica y preferiblemente, cuando se adquiere la información de aplicación objetivo, el dispositivo de red 1 adquiere la información de atributo relacionada correspondiente al mismo tiempo. La información de atributo relacionada incluye la información de remitente de la información de aplicación objetivo, por ejemplo, un número de dispositivo de un remitente de un mensaje SMS, un número de teléfono móvil, o un número específico de una institución, o información de dirección de correo electrónico de un remitente de un correo electrónico. La información de atributo relacionada incluye además el contenido de la información de aplicación objetivo, por ejemplo, contenido de texto de un mensaje SMS o contenido del cuerpo de un correo electrónico, y similar. La información de atributo relacionada incluye además la información de guía de usuario. La información de guía de usuario incluye cualquier información que indica a un usuario que realice una operación relacionada. Por ejemplo, un hipervínculo del sitio web proporcionado al usuario o información de dirección de descarga proporcionada al usuario, y similar. En este caso, se realizan diferentes operaciones de validación y análisis basándose en diferentes contenidos específicos de la información de atributo relacionada, por ejemplo, se seleccionan diferentes bases de datos de validación para diferente información de atributo relacionada para realizar la búsqueda de coincidencias.

En este caso, un experto en la técnica entenderá que la información de remitente de la información de aplicación objetivo, la información de contenido de la información de aplicación objetivo o la información de guía de usuario de la información de aplicación objetivo son sólo ejemplos, y que la información de atributo relacionada de otra información de aplicación objetivo existente o futura que es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

En una forma de realización preferida (con referencia a la figura 1), la información de atributo relacionada incluye la información de guía de usuario de la información de aplicación objetivo. El aparato de validación de información de aplicación objetivo 12 incluye además una segunda unidad de determinación de información de riesgo (no mostrada). Cuando no se identifica información de registro que coincide con la información de guía de usuario en la base de datos de validación, la segunda unidad de determinación de información de riesgo simula la ejecución de la información de aplicación objetivo basándose en la información de guía de usuario para obtener la información de riesgo correspondiente.

Específicamente, en esta forma de realización, cuando la información de atributo relacionada incluye la información de guía de usuario de la información de aplicación objetivo, si no se identifica información de registro que coincide con la información de guía de usuario en la base de datos de validación, preferiblemente, se realiza una ejecución de simulación específica en la información de guía de usuario. En este caso, considerando que un proceso de ejecución de simulación puede tener un riesgo para la seguridad, el dispositivo de red 1 puede disponerse en un entorno de pruebas seguro para realizar un experimento de simulación. Por ejemplo, cuando la información de guía de usuario es un enlace de descarga o información de sitio web, el dispositivo de red 1 extrae la información de guía de usuario, y ejecuta un navegador u otro programa correspondiente en un entorno de pruebas seguro previamente configurado para abrir la información URL del sitio web anterior o el enlace descendente para realizar la operación indicada por la información de guía de usuario. Además, se analiza el problema de seguridad en un proceso de operación de ejecución, o adicionalmente se determina y analiza el resultado de ejecución de la ejecución de simulación para obtener la información de riesgo correspondiente. Por ejemplo, si se abre un enlace de sitio web correspondiente a la información de guía de usuario a través de una ejecución de simulación, y el resultado corresponde a un sitio web de *phishing*, puede deducirse que la información de aplicación objetivo es de riesgo, y se determina la información de riesgo correspondiente. En este caso, posteriormente se borran los cambios producidos por una operación ejecutada en el entorno de pruebas seguro. Además, los posibles riesgos que pueden producirse al ejecutar un programa en el entorno de ejecución virtual no producen un daño real a los dispositivos relacionados como el dispositivo de red 1.

Además, basándose en una fuente de riesgo, por ejemplo, información de sitio web de *phishing*, un virus troyano, o un riesgo para la seguridad de un texto de mensaje SMS, puede realizarse una extracción y clasificación de información de riesgo en información de aplicación objetivo con riesgo relativamente alto, determinada a través de la ejecución de simulación, para actualizar la información sobre la base de datos de validación correspondiente, y transmitir la información de riesgo a diferentes instituciones financieras basándose en tipos de riesgo.

En esta forma de realización, el dispositivo de red 1 realiza una búsqueda de coincidencias en la base de datos de validación correspondiente basándose en la información de atributo relacionada de la información de aplicación objetivo. Para información de aplicación objetivo que no coincide con la información de registro correspondiente, el dispositivo de red 1 puede simular adicionalmente la ejecución de la información de guía de usuario correspondiente para determinar la información de riesgo correspondiente. Por tanto, se garantiza una precisión de determinación de

información de riesgo con una forma de determinación de múltiples niveles. Así, el usuario puede realizar un procesamiento eficaz basándose en la información de aviso correspondiente a información de riesgo de alta precisión.

Preferiblemente, cuando no se identifica información de registro que coincide con la información de guía de usuario en la base de datos de validación, la segunda unidad de determinación de información de riesgo simula la adquisición, basándose en la información de guía de usuario, de información objetivo que está en la información de aplicación objetivo y hacia la que se guía al usuario para que la adquiera; y valida la correspondencia entre la información objetivo y la información de aplicación objetivo para obtener la información de riesgo correspondiente.

Específica y preferiblemente, la información objetivo que está en la información de aplicación objetivo y se adquiere por un usuario guiado se obtiene en primer lugar por medio de simulación basándose en la información de usuario guiado. En este caso, la información objetivo incluye un resultado correspondiente al que apunta el dispositivo de red 1 ejecutando la información de usuario de guía mediante simulación. Por ejemplo, la información objetivo puede ser una página web hacia la que se guía al usuario para que la abra, o puede ser un archivo hacia el que se guía al usuario para que lo descargue. A continuación, el dispositivo de red 1 valida la correspondencia entre la información objetivo y la información de aplicación objetivo para obtener la información de riesgo correspondiente. En este caso, los riesgos producidos por la información objetivo incluyen un riesgo directo impuesto a la seguridad de la privacidad del usuario y seguridad del equipo de usuario, por ejemplo, un archivo descargado incluye un virus. Los riesgos producidos por la información objetivo también incluyen un riesgo potencial producido por cierta información de spam, por ejemplo, cuando un sitio web abierto es un sitio web de anuncio falso, puede producirse un cierto daño si el usuario realiza una operación correspondiente basándose en información de instrucción en el sitio web. En este caso, se determina la correspondencia entre la información objetivo y la información de aplicación objetivo para determinar la relevancia de la información objetivo y la información de aplicación objetivo. En general, existe información de aplicación objetivo de alto riesgo tal como un mensaje SMS falso con el propósito de engañar al usuario para que realice una operación contra su voluntad o para que realice involuntariamente una operación desfavorable. Por tanto, existe una posibilidad relativamente alta de que la información objetivo correspondiente a tal información de aplicación objetivo sea incoherente con o no coincida con la información de aplicación objetivo. Esta es una base importante para validar la correspondencia en la presente solicitud. La validación de correspondencia entre la información objetivo y la información de aplicación objetivo puede incluir comprobar si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo; comprobar si el contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo; o comprobar si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo.

En este caso, un experto en la técnica entenderá que los procedimientos anteriores para validar la correspondencia entre la información objetivo y la información de aplicación objetivo son sólo ejemplos, y que un procedimiento existente o futuro para validar la correspondencia entre la información objetivo y la información de aplicación objetivo y que es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

Más preferiblemente, la validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye al menos una de las siguientes: comprobar si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo; comprobar si el contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo; o comprobar si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo.

Específicamente, la validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye comprobar si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo. Si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo, puede deducirse que la información objetivo coincide con la información de aplicación objetivo. Por tanto, por la validación puede deducirse que la información de aplicación objetivo tiene una alta seguridad y un bajo riesgo. Por el contrario, se deduce que la información objetivo no coincide con la información de aplicación objetivo. Por la validación puede deducirse que la información de aplicación objetivo tiene una baja seguridad y un alto riesgo. En este caso, por ejemplo, la información de aplicación objetivo es un mensaje SMS. Si un remitente del mensaje SMS es un número de un operador móvil, el contenido del mensaje SMS está relacionado con proporcionar llamadas gratuitas, y la información de guía de usuario es un enlace de página web del operador, y si la información objetivo adquirida es de hecho una página web relacionada de la operación móvil, se considera que el remitente de la información objetivo es coherente con el remitente del mensaje SMS, y puede deducirse que la información objetivo coincide con la información de aplicación objetivo. Por el contrario, si después de pinchar en el enlace se abre una página web irrelevante, puede deducirse que la información objetivo no coincide con la información de aplicación objetivo. En este caso, preferiblemente, si la información de remitente es incoherente, adicionalmente puede determinarse si el remitente de la información de aplicación objetivo es una estación base no autorizada que de manera dedicada envía información falsa. En tal caso,

puede deducirse que la información de aplicación enviada por el remitente es información falsa. Además, el dispositivo de red 1 puede registrar adicionalmente información sobre la estación base no autorizada, y avisar al equipo de usuario 2 relacionado.

En este caso, la validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye además comprobar si el contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo. En este caso, si el contenido de la información objetivo coincide con el contenido de la información de aplicación objetivo, se considera que la correspondencia entre la información objetivo y la información de aplicación objetivo es relativamente alta, y se deduce que la seguridad de la información de aplicación objetivo es relativamente alta, y el riesgo es bajo. Por el contrario, se deduce que la información de aplicación objetivo es menos segura y tiene un mayor riesgo. En este caso, por ejemplo, la información de aplicación objetivo es un mensaje SMS. Si el contenido del mensaje SMS es un enlace sobre información sobre descuentos en centros comerciales, pero después de pinchar en el enlace se abre un sitio web de pago irrelevante, se deduce que el contenido de la información objetivo no está relacionado con el contenido de la información de aplicación objetivo, y que la información objetivo puede ser potencialmente peligrosa.

En este caso, la validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye además comprobar si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo. En este caso, si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo, la información de aplicación objetivo es relativamente segura con un menor riesgo. Por el contrario, si la información de operación en el entorno de pruebas seguro de la información objetivo no coincide con la información de aplicación objetivo, puede deducirse que la información de aplicación objetivo tiene una baja seguridad y un alto riesgo. En este caso, por ejemplo, la información de aplicación objetivo es un mensaje SMS. Cuando la información objetivo es una aplicación descargada correspondiente a un enlace de descarga en el mensaje SMS, si la aplicación descargada se instala o ejecuta en el entorno de pruebas seguro, y si una etapa de operación específica es diferente de lo descrito en la información de aplicación objetivo, o un resultado obtenido ejecutando la aplicación es diferente de lo descrito en la información de aplicación objetivo, puede deducirse que la información de operación en el entorno de pruebas seguro de la información objetivo no coincide con la información de aplicación objetivo, y que hay un alto riesgo para la seguridad.

En este caso, un experto en la técnica entenderá que los procedimientos anteriores para validar la correspondencia entre la información objetivo y la información de aplicación objetivo son sólo ejemplos, y que un procedimiento existente o futuro para validar la correspondencia entre la información objetivo y la información de aplicación objetivo y que es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

En la invención (con referencia a la figura 1), la información de aplicación objetivo incluye un mensaje SMS, y el dispositivo de red 1 incluye además un aparato de envío de información de aviso de estación base no autorizada (no mostrado). El aparato de envío de información de aviso de estación base no autorizada envía información de aviso de estación base no autorizada al equipo de usuario cercano del equipo de usuario cuando la información de riesgo es que el mensaje SMS es información falsa. Una distancia entre el equipo de usuario cercano y el equipo de usuario es menor que o igual a un umbral de distancia predeterminado entre dispositivos.

Específicamente, en este caso, la estación base no autorizada es una pseudoestación base, y habitualmente comprende un anfitrión y un portátil. La estación base no autorizada puede estar configurada para buscar la información sobre una tarjeta de módulo de identidad de abonado (SIM) en un área dentro de un determinado radio de la estación base utilizando un dispositivo como un dispositivo de envío de mensajes SMS, un remitente de mensajes SMS, o similar. La estación base no autorizada envía a la fuerza un mensaje SMS como un mensaje de *Smishing* o un mensaje SMS de publicidad al teléfono móvil del usuario mostrándose a sí misma como una estación base de un operador y utilizando de manera fraudulenta un número de teléfono móvil de otro usuario. En esta forma de realización, la información de aplicación objetivo incluye información de mensaje SMS. Si la información de riesgo de la información de aplicación objetivo obtenida mediante la validación por el dispositivo de red 1 incluye que el mensaje SMS es información falsa, y además puede deducirse que la información falsa se envía por una estación base no autorizada correspondiente, puede determinarse la información de ubicación de la estación base no autorizada, o puede determinarse una pista de movimiento de la estación base no autorizada para deducir la información de ubicación de la estación base no autorizada. Además, el aparato de envío de información de aviso de estación base no autorizada envía la información de aviso de estación base no autorizada al equipo de usuario cercano del equipo de usuario, siendo la distancia entre el equipo de usuario cercano y el equipo de usuario menor que o igual a una información de umbral de distancia predeterminado entre dispositivos. El equipo de usuario cercano incluye varios dispositivos terminales inteligentes móviles, y preferiblemente, incluye un dispositivo con una función de comunicación móvil, por ejemplo, un dispositivo terminal que puede recibir un mensaje SMS, como un teléfono móvil, o un ordenador de tableta con una función de recepción/envío de mensajes SMS. En este caso, el umbral de distancia predeterminado entre dispositivos puede establecerse basándose en la información de ubicación de la estación base no autorizada y la

cobertura del envío del mensaje SMS. En este caso, la información de aviso de estación base no autorizada se envía al equipo de usuario cercano cuando el dispositivo de red 1 adquiere y determina en primer lugar la información sobre la estación base no autorizada. Cada vez que se determina que el mensaje SMS es información falsa, la información de aviso de estación base no autorizada se envía al equipo de usuario cercano al mismo tiempo. En este caso, si se habilita una función de posicionamiento correspondiente en el equipo de usuario cercano, por ejemplo, una función GPS (*Global Positioning System*, sistema de posicionamiento global) de un teléfono móvil, el dispositivo de red 1 puede buscar y obtener información de latitud y longitud correspondiente del teléfono móvil. En este caso, si la distancia entre el equipo de usuario cercano y el equipo de usuario es menor que o igual al umbral de distancia predeterminado entre dispositivos, la información de aviso de estación base no autorizada se envía al equipo de usuario cercano.

En esta forma de realización, cuando la información de riesgo incluye que la información de mensaje SMS es información falsa, el dispositivo de red 1 envía la información de aviso de estación base no autorizada al equipo de usuario cercano del equipo de usuario 2. Cuando la información falsa corresponde a una estación base no autorizada, puede enviarse un aviso a otro equipo de usuario que se encuentre en el área de cobertura de la estación base no autorizada y que pueda recibir el mensaje de *Smishing* para reducir y evitar más riesgos producidos por la información falsa enviada por la estación base no autorizada. Específicamente, cuando otro equipo de usuario utiliza una aplicación objetivo, el dispositivo de red 1 puede enviar información sobre la existencia de una estación base no autorizada cerca del dispositivo de red 1, y el dispositivo de red 1 puede emitir directamente un aviso con el permiso del otro equipo de usuario.

La figura 2 muestra un diagrama esquemático de un sistema de un dispositivo de red 1 y un equipo de usuario 2 para la gestión de riesgos de información de aplicación basándose en una forma de realización preferida de la presente solicitud.

El dispositivo de red 1 incluye un aparato de adquisición de información de aplicación objetivo 11', un aparato de validación de información de aplicación objetivo 12' y un aparato de envío de información de aviso 13'. El equipo de usuario 2 incluye un aparato de adquisición de información de aplicación objetivo seleccionada por el usuario 21', un aparato de envío de información de aplicación objetivo 22' y un aparato de recepción de información de aviso 23'. El aparato de adquisición de información de aplicación objetivo 11' adquiere información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando el equipo de usuario 2. El aparato de validación de información de aplicación objetivo 12' valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. El aparato de envío de información de aviso 13' devuelve la información de aviso correspondiente al equipo de usuario 2 basándose en la información de riesgo. El aparato de adquisición de información de aplicación objetivo seleccionada por el usuario 21' adquiere la información de aplicación objetivo que selecciona el usuario y cuya validación solicita utilizando el equipo de usuario 2. El aparato de envío de información de aplicación objetivo 22' envía la información de aplicación objetivo al dispositivo de red 1 correspondiente. El aparato de recepción de información de aviso 23' adquiere la información de aviso que se devuelve por el dispositivo de red 1 y que se basa en la información de riesgo de la información de aplicación objetivo. En este caso, el aparato de adquisición de información de aplicación objetivo 11', el aparato de validación de información de aplicación objetivo 12' y el aparato de envío de información de aviso 13' son básicamente iguales que el aparato de adquisición de información de aplicación objetivo 11, el aparato de validación de información de aplicación objetivo 12 y el aparato de envío de información de aviso 13 mostrados en la figura 1. Aquí no se describen de nuevo los detalles, y se incorporan al presente documento por referencia.

Específicamente, en este caso, el aparato de adquisición de información de aplicación objetivo seleccionada por el usuario 21' adquiere la información de aplicación objetivo que selecciona el usuario y cuya validación solicita utilizando el equipo de usuario 2. En este caso, preferiblemente, la información de aplicación objetivo se determina directamente basándose en una operación de selección autónoma del usuario. En este caso, la información de aplicación como un mensaje SMS, un mensaje de WeChat o un correo electrónico incluye información masiva de la privacidad del usuario. Por tanto, si toda la información se carga por una aplicación de un tercero, se aumenta el riesgo de pérdida de información. Por tanto, en la presente solicitud, preferiblemente, el usuario puede seleccionar de manera autónoma una información o varias informaciones de aplicación objetivo que en realidad es necesario enviar al dispositivo de red para su validación. En este caso, además, preferiblemente, el usuario puede realizar directamente una operación de selección en una interfaz de operación de una aplicación objetivo correspondiente a la información de aplicación objetivo en el equipo de usuario 2. Por ejemplo, si la información de aplicación objetivo es un mensaje SMS, el usuario puede seleccionar directamente un mensaje sospechoso de *Smishing* cuando entra en la aplicación de SMS, de modo que se evita la necesidad de tener que saltar a otra interfaz de aplicación de un tercero. En este caso, puede implementarse una operación de respuesta para una instrucción del usuario para una selección y solicitud de validación ejecutando un programa de aplicación independiente cargado en el dispositivo de red 1, o ejecutando un complemento correspondiente que coincide con la aplicación objetivo como la aplicación de SMS.

Después, el aparato de envío de información de aplicación objetivo 22' envía la información de aplicación objetivo al dispositivo de red 1 correspondiente. En este caso, la información de aplicación objetivo enviada al dispositivo de red

1 puede estar en la forma original de la información de aplicación objetivo adquirida por el equipo de usuario 2. Por ejemplo, si la información de aplicación objetivo es un mensaje SMS, la información de aplicación objetivo adquirida por el dispositivo de red 1 puede estar en forma de un texto de mensaje SMS visualizado en la interfaz de aplicación de SMS del equipo de usuario 2. Además, el equipo de usuario 2 puede analizar en primer lugar la información de aplicación original recibida por el equipo de usuario 2 o extraer la información de la información de aplicación original. Por ejemplo, el equipo de usuario 2 extrae una palabra clave de un mensaje SMS basándose en una categoría y envía la palabra clave extraída al dispositivo de red 1. Así, el equipo de usuario 2 en primer lugar y de manera preliminar, puede analizar y clasificar la información de aplicación objetivo que va a validarse, y puede reducir un volumen de datos transmitidos entre dispositivos. Además, cuando se envía la información de aplicación objetivo, el equipo de usuario 2 puede enviar además, al dispositivo de red 1, información de atributo relacionada correspondiente a la información de aplicación objetivo, como información de remitente de la información de aplicación objetivo o información de guía de usuario de la información de aplicación objetivo, para realizar posteriormente operaciones de validación de riesgo en la información de aplicación objetivo en el dispositivo de red 1 de múltiples maneras. En este caso, preferiblemente, el equipo de usuario 2 envía la información de aplicación objetivo al dispositivo de red 1 con una transmisión cifrada.

Por consiguiente, el aparato de adquisición de información de aplicación objetivo 11' del dispositivo de red 1 adquiere la información de aplicación objetivo que selecciona el usuario y cuya validación solicita utilizando el equipo de usuario 2. A continuación, el aparato de validación de información de aplicación objetivo 12' del dispositivo de red 1 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente.

Después, el aparato de envío de información de aviso 13' del dispositivo de red 1 devuelve la información de aviso correspondiente al equipo de usuario 2 basándose en la información de riesgo. Por consiguiente, el aparato de recepción de información de aviso 23' del equipo de usuario 2 adquiere la información de aviso que se devuelve por el dispositivo de red 1 y que se basa en la información de riesgo de la información de aplicación objetivo. En este caso, preferiblemente, la información de aviso recibida por el equipo de usuario 2 es información de aviso correspondiente generada por el dispositivo de red 1 basándose en la información de riesgo obtenida mediante validación. Por ejemplo, cuando la información de riesgo es información determinante de que existe un riesgo, como cuando la información de riesgo es que un mensaje SMS objetivo es información falsa, se genera la información de aviso de riesgo correspondiente. El contenido de la información de aviso de riesgo puede incluir destacar un mensaje SMS con un aviso de riesgo en el equipo de usuario 2, un mensaje SMS de aviso específico, o información de aviso en otra forma, o incluso un proceso directo del mensaje SMS como mensaje SMS basura por el equipo de usuario 2, etc. Como otro ejemplo, cuando el dispositivo de red 1 determina que la información de riesgo es información determinante de que no existe ningún riesgo, el equipo de usuario 2 adquiere información de seguridad de validación correspondiente. Además, en este caso, preferiblemente, el usuario puede elegir adoptar la información de aviso enviada por el dispositivo de red 1 para realizar un procesamiento posterior en la información de aplicación como un mensaje SMS del usuario, o elegir no adoptar la información de aviso y retener la información de aplicación objetivo. Así, se respeta totalmente el derecho del usuario de procesar información relacionada con la privacidad del usuario. Además, el contenido de información de aviso puede ejecutarse automáticamente basándose en ajustes predeterminados realizados por el usuario cuando se obtiene la información de aviso correspondiente. Por ejemplo, el usuario puede realizar una preselección. Así, después de que el dispositivo de red 1 realice una validación de riesgos, si un riesgo de la información de aplicación objetivo es relativamente alto y alcanza un nivel predeterminado, la información de aplicación objetivo se borra automáticamente. Por tanto, después de que el equipo de usuario 2 reciba información de aviso que cumple con una condición, automáticamente puede realizarse una operación de instrucción correspondiente, y no tiene que preguntarse al usuario. En resumen, la operación automática no va en contra de la voluntad del usuario, sino que es el resultado de la participación del usuario en la operación.

En este caso, el equipo de usuario 2 envía la información de aplicación objetivo seleccionada por el usuario al dispositivo de red 1 correspondiente para su validación, y recibe la información de aviso que se devuelve por el dispositivo de red 1 y que se basa en la información de riesgo de la información de aplicación objetivo. Así, el equipo de usuario actúa conjuntamente con el dispositivo de red 1 para implementar la gestión de riesgos en la información de aplicación.

aparato (no mostrado) y un aparato de visualización de información de aplicación (no mostrado). El aparato de preanálisis de riesgo realiza un preanálisis de riesgo en la información de aplicación recibida por el equipo de usuario 2. El aparato de visualización de información de aplicación visualiza, en una aplicación correspondiente, una información o varias informaciones de aplicación que están en riesgo, adquiridas mediante el preanálisis de riesgo. El aparato de adquisición de información de aplicación objetivo seleccionada por el usuario 21' adquiere la información de aplicación objetivo que el usuario selecciona de la una información o las varias informaciones de aplicación y solicita su validación utilizando el equipo de usuario 2.

Específicamente, de manera habitual no puede reconocerse fácilmente la información de aplicación objetivo con un riesgo relativamente alto como un mensaje SMS falso. Por tanto, para facilitar la selección autónoma de la información de aplicación objetivo por el usuario, mejorar la probabilidad de que la información de aplicación objetivo seleccionada

de manera autónoma por el usuario se determine como información de aplicación de alto riesgo y mejorar la eficiencia de la realización posterior de la validación de riesgo de información de aplicación objetivo por el dispositivo de red 1, preferiblemente, el aparato de preanálisis de riesgo puede estar configurado para realizar el preanálisis de riesgo en la información de aplicación recibida por el equipo de usuario 2, y a continuación se proporciona una asistencia inmediata correspondiente al usuario basándose en el resultado del preanálisis de riesgo. En este caso, el equipo de usuario 2 puede adquirir y almacenar de antemano cierta información relacionada sobre información de aplicación que se recopiló recientemente y que tiene un riesgo relativamente alto. Por ejemplo, se adquiere previamente una base de datos de recopilación reciente de números de remitentes de mensajes *Smishing*, y a continuación, basándose en información de la base de datos, se realiza un preanálisis de riesgo en un mensaje SMS recibido por el equipo de usuario 2. En este caso, la información de datos que se utiliza como datos de referencia de preanálisis puede proceder del dispositivo de red 1 correspondiente, por ejemplo, de una recopilación de información relacionada sobre información de base de datos de validación reciente correspondiente al dispositivo de red 1, por ejemplo, información de base de datos de validación en un mes. Como otro ejemplo, una lista de datos de riesgo recientes en una región actual puede almacenarse en el equipo de usuario 2, y a continuación se compara la información de aplicación adquirida por el equipo de usuario 2 con la lista de datos. En este caso, puede realizarse un análisis de evaluación preliminar de la información de aplicación sin aumentar la carga de la operación del equipo de usuario 2, para avisar de manera eficaz al usuario.

Después, el aparato de visualización de información de aplicación visualiza, en una aplicación correspondiente, una información o varias informaciones de aplicación que están en riesgo, adquiridas mediante el preanálisis de riesgo. En este caso, el resultado del preanálisis de riesgo puede

La figura 3 muestra un diagrama de flujo de un procedimiento para la gestión de riesgos de información de aplicación en un lado de dispositivo de red basándose en otro aspecto de la presente solicitud.

El procedimiento incluye las etapas S31, S32 y S33. En la etapa S31, un dispositivo de red 1 adquiere información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando el equipo de usuario 2. En la etapa S32, el dispositivo de red 1 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. En la etapa S33, el dispositivo de red 1 devuelve la información de aviso correspondiente al equipo de usuario basándose en la información de riesgo.

Específicamente, en la etapa S31, el dispositivo de red 1 adquiere la información de aplicación objetivo que selecciona el usuario y cuya validación solicita utilizando el equipo de usuario 2 (con referencia a la figura 4). En este caso, el dispositivo de red 1 incluye varios terminales inteligentes, como varios servidores en la nube o grupos de servidores. El equipo de usuario 2 incluye varios dispositivos terminales inteligentes, como varios ordenadores personales y teléfonos inteligentes. En este caso, la información de aplicación incluye, pero no está limitada a, un mensaje SMS, un mensaje de WeChat, un correo electrónico, u otra información transferida basándose en un programa de aplicación específico en el equipo de usuario 2. En este caso, la información de aplicación objetivo adquirida por el dispositivo de red 1 procede del equipo de usuario 2 correspondiente. Preferiblemente, la información de aplicación objetivo se selecciona de manera autónoma por el usuario de la información de aplicación en una aplicación objetivo del equipo de usuario 2. Por ejemplo, el usuario puede copiar la información de aplicación objetivo en un cuadro de texto, y seleccionar enviar la información de aplicación objetivo. Entonces el equipo de usuario 2 envía la información de aplicación objetivo al dispositivo de red 1 correspondiente. Como otro ejemplo, el usuario puede seleccionar y enviar directamente la información de aplicación objetivo en una aplicación. En este caso, preferiblemente, el dispositivo de red 1 adquiere la información de aplicación objetivo enviada por el equipo de usuario 2 con una transmisión cifrada. Por ejemplo, la información de aplicación objetivo es un mensaje SMS. Cuando el usuario entra en una interfaz de aplicación de SMS del equipo de usuario 2 como un teléfono móvil, el usuario selecciona directamente un mensaje sospechoso de *Smishing* de varios mensajes SMS visualizados, y determina una información o varias informaciones de aplicación objetivo en la/s que se realizará la validación de riesgo. A continuación, el aparato de adquisición de información de aplicación objetivo 11 del dispositivo de red 1 adquiere la información de aplicación objetivo seleccionada por el usuario y una solicitud de validación correspondiente.

En este caso, la información de aplicación objetivo adquirida por el dispositivo de red 1 puede estar en la forma original de la información de aplicación objetivo adquirida por el equipo de usuario 2. Por ejemplo, si la información de aplicación objetivo es un mensaje SMS, la información de aplicación objetivo adquirida por el dispositivo de red 1 puede estar en forma de un texto de mensaje SMS visualizado en la interfaz de aplicación de SMS del equipo de usuario 2. Además, el equipo de usuario 2 puede analizar en primer lugar la información de aplicación original recibida por el equipo de usuario 2 o extraer la información de la información de aplicación original. Por ejemplo, el equipo de usuario 2 extrae una palabra clave de un mensaje SMS basándose en una categoría y envía la palabra clave extraída al dispositivo de red 1. Así, la información de aplicación objetivo que va a validarse puede analizarse y clasificarse de forma preliminar, y se reduce un volumen de datos transmitidos entre los dispositivos.

Además, cuando se adquiere la información de aplicación objetivo, el dispositivo de red 1 puede adquirir de manera correspondiente información de atributo relacionada de la información de aplicación objetivo, como información de

remitente de la información de aplicación objetivo o información de guía de usuario de la información de aplicación objetivo.

Después, en la etapa S32, el dispositivo de red 1 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. En este caso, en la presente solicitud, el dispositivo de red 1 realiza un análisis de validación de riesgo en la información de aplicación objetivo utilizando el dispositivo de red 1. En este caso, un riesgo de la información de aplicación objetivo puede incluir un riesgo directo impuesto a la seguridad de la privacidad del usuario y seguridad del equipo de usuario, y además puede incluir un riesgo potencial impuesto al usuario por información de aplicación basura como un anuncio falso. Para validar la información de aplicación objetivo, la información de aplicación objetivo y la información de atributo relacionada pueden considerarse o evaluarse exhaustivamente por medio de clasificación. En este caso, de manera flexible pueden seleccionarse y combinarse procedimientos de validación específicos basándose en las necesidades reales. Por ejemplo, la información de aplicación objetivo puede validarse y analizarse basándose en una base de datos de validación previamente existente. Como otro ejemplo, puede realizarse una ejecución de simulación en la información de guía de usuario de la información de aplicación objetivo en un entorno de pruebas seguro para identificar si la información de aplicación objetivo incluye información de riesgo. Por ejemplo, la seguridad de la información de aplicación objetivo puede validarse múltiples veces combinando una pluralidad de procedimientos de validación. Por ejemplo, la información de aplicación objetivo se valida utilizando por separado los procedimientos descritos en los dos ejemplos anteriores para mejorar la precisión de la información de riesgo obtenida finalmente. En este caso, la información de riesgo puede incluir información determinante de que existe un riesgo o información determinante de que no existe ningún riesgo. Además, preferiblemente, la información determinante de que existe un riesgo puede clasificarse y organizarse específicamente basándose en el contenido del riesgo y la consecuencia negativa producida por el riesgo. Por ejemplo, si la información de aplicación objetivo incluye contenido como un sitio web de *phishing*, un troyano, o una estación base no autorizada y similar, un valor de riesgo de la información de aplicación objetivo se establece en un 99%, o se define que la información de aplicación objetivo está en un alto nivel de riesgo.

Después, en la etapa S33, el dispositivo de red 1 devuelve, basándose en la información de riesgo, la información de aviso correspondiente al equipo de usuario 2. En este caso, preferiblemente, el dispositivo de red 1 genera la información de aviso correspondiente basándose en la información de riesgo obtenida mediante validación, y devuelve la información de aviso al equipo de usuario 2. Por ejemplo, cuando la información de riesgo es la información determinante de que existe un riesgo, como cuando la información de riesgo es que un mensaje SMS objetivo es información falsa, se genera la información de aviso de riesgo correspondiente. El contenido de la información de aviso de riesgo puede incluir destacar un mensaje SMS con un aviso de riesgo en el equipo de usuario 2, un mensaje SMS de aviso específico, o información de aviso en otra forma, o incluso un proceso directo del mensaje SMS como mensaje SMS basura por el equipo de usuario 2, etc. Como otro ejemplo, cuando la información de riesgo es la información determinante de que no existe ningún riesgo, la información de seguridad de validación correspondiente puede enviarse al equipo de usuario 2.

En este caso, en la presente solicitud, la información de aplicación objetivo que selecciona el usuario y cuya validación solicita se valida utilizando el dispositivo de red 1, y la información de aviso correspondiente a la información de riesgo obtenida mediante validación se devuelve al equipo de usuario 2 correspondiente. En este caso, el usuario puede seleccionar directamente una información o varias informaciones de aplicación objetivo de una interfaz de información de aplicación correspondiente del equipo de usuario sin tener que saltar a una operación de aplicación de terceros. Además, el usuario puede determinar de manera autónoma parte de o toda la información de aplicación objetivo a cargar. Por tanto, se mejora el nivel de participación de un usuario en la gestión de la información sobre la privacidad del usuario y se reduce la probabilidad de pérdida de la privacidad del usuario. Además, con una selección flexible, puede reducirse un volumen de datos transmitidos entre los dispositivos, de modo que por consiguiente se reduce un volumen de datos de validación que procesa el dispositivo de red, y se mejora la eficiencia de la gestión de riesgos de información de aplicación global.

En una forma de realización preferida, la etapa S32 incluye la etapa S321 (no mostrada) y la etapa S322 (no mostrada). En la etapa S321, el dispositivo de red 1 realiza una búsqueda de coincidencias en una base de datos de validación correspondiente basándose en información de atributo relacionada de la información de aplicación objetivo. En la etapa S322, el dispositivo de red 1 determina la información de riesgo correspondiente basándose en información de registro que está en la base de datos de validación y que coincide con la información de atributo relacionada.

Específicamente, en la etapa S321, el dispositivo de red 1 realiza una búsqueda de coincidencias en la base de datos de validación correspondiente basándose en la información de atributo relacionada de la información de aplicación objetivo. En este caso, la base de datos de validación es preferiblemente una biblioteca de plantillas de mensajes SMS, una biblioteca de sitios web de *phishing*, una biblioteca de virus troyanos, etc. La biblioteca de plantillas de mensajes SMS incluye un mensaje SMS que se determina como plantilla, y que recopila el dispositivo de red 1 y tiene un alto factor de riesgo histórico, como un mensaje de *Smishing* determinado, o una plantilla de mensajes SMS derivada con una similitud relativamente alta deducida basándose en un mensaje de *Smishing* previamente conocido. La biblioteca de sitios web de *phishing*, la biblioteca de virus troyanos, etc. incluyen información sobre un sitio web

que recopila el dispositivo de red 1 y que se determina como un sitio web de *phishing*, o información sobre un archivo que se determina que incluye un virus troyano. La información en la biblioteca de sitios web de *phishing* anterior y la biblioteca de virus troyanos pueden extraerse directamente de la información de aplicación en cada equipo de usuario 2, o pueden ser datos existentes de otra base de datos, o un dispositivo de terceros. En este caso, la información de atributo relacionada incluye cualquier información que está asociada con la información de aplicación objetivo, por ejemplo, información de remitente de la información de aplicación objetivo, la información de contenido de la información de aplicación objetivo, información de guía de usuario de la información de aplicación objetivo, etc. En este caso, basándose en los tipos de las bases de datos de validación diferentes, puede realizarse una búsqueda de coincidencias correspondiente en información apropiada seleccionada de la información de atributo relacionada de la información de aplicación objetivo. Por ejemplo, cuando la base de datos de validación es una biblioteca de sitios web de *phishing*, puede seleccionarse la información de guía de usuario de la información de aplicación objetivo. Por ejemplo, un mensaje SMS objetivo incluye información sobre un sitio web, y se realiza una búsqueda de coincidencias en la información. Como otro ejemplo, si la base de datos de validación es la biblioteca de plantillas de mensajes SMS, se selecciona el contenido de la información de aplicación objetivo, y se realiza una búsqueda de coincidencias en el contenido. En este caso, preferiblemente, cuando una pluralidad de tipos de bases de datos de validación están preconfigurados en el dispositivo de red 1, pueden seleccionarse una o varias bases de datos de validación y utilizarse como base de datos de referencia basándose en las necesidades, por ejemplo, basándose en la selección de un usuario, o basándose en una decisión inteligente de un tipo de la información de aplicación objetivo. Además, preferiblemente, cada base de datos de validación puede organizarse basándose en el nivel de riesgo correspondiente a la información de aplicación, y se selecciona una base de datos de validación en una clasificación específica para la información de aplicación objetivo basándose en la clasificación, o se seleccionan bases de datos de validación en una pluralidad de clasificaciones para validar sucesivamente la información de aplicación objetivo.

En este caso, un experto en la técnica entenderá que la biblioteca de plantillas de mensajes SMS, la biblioteca de sitios web de *phishing* y la biblioteca de virus troyanos son sólo ejemplos, y que una base de datos existente o una base de datos futura que pueden utilizarse para la validación de información de aplicación objetivo y es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

Después, en la etapa S322, el dispositivo de red 1 determina la información de riesgo correspondiente basándose en la información de registro que está en la base de datos de validación y que coincide con la información de atributo relacionada. En este caso, si la información de registro que coincide con la información de atributo relacionada se identifica en la base de datos de validación correspondiente, por ejemplo, si un mensaje SMS objetivo incluye información sobre un sitio web, y su registro correspondiente en la biblioteca de sitios web de *phishing* es un sitio web de *phishing*. Como otro ejemplo, si el contenido de texto mencionado anteriormente del mensaje SMS objetivo es coherente con el contenido de una plantilla de mensaje de *Smishing* en la biblioteca de plantillas de mensajes SMS, puede determinarse la información de riesgo correspondiente a la información de aplicación objetivo, por ejemplo, determinarse como la información determinante de que existe un riesgo, o, además, la información de riesgo incluye información de nivel de riesgo correspondiente.

Además, cuando la base de datos de validación no incluye la información de registro que coincide con la información de atributo relacionada, puede deducirse que la información de aplicación objetivo es información de seguridad con un riesgo relativamente bajo basándose en las necesidades, y la información de seguridad de validación correspondiente se devuelve al equipo de usuario 2. Alternativamente, se selecciona otra base de datos de validación o incluso otro procedimiento de validación para la validación de riesgo, y se proporciona información de riesgo correspondiente. Por ejemplo, cuando no puede hacerse coincidir información de registro correspondiente utilizando la biblioteca de plantillas de mensajes SMS, adicionalmente se realizan búsquedas de coincidencias basándose en la biblioteca de sitios web de *phishing*. Como otro ejemplo, cuando no puede hacerse coincidir información de registro correspondiente en todas o algunas de las bases de datos de validación predeterminadas, la coincidencia puede realizarse en otro procedimiento de validación, por ejemplo, coincidiendo con una biblioteca de mensajes SMS/números de teléfono de una institución financiera. Por ejemplo, puede realizarse una ejecución de simulación en la información de guía de usuario de la información de aplicación objetivo en un entorno de pruebas seguro para identificar si la información de aplicación objetivo incluye información de riesgo.

Preferiblemente, la información de atributo relacionada incluye al menos una de las siguientes: información de remitente de la información de aplicación objetivo, información de contenido de la información de aplicación objetivo o información de guía de usuario de la información de aplicación objetivo.

En este caso, específica y preferiblemente, cuando se adquiere la información de aplicación objetivo, el dispositivo de red 1 adquiere la información de atributo relacionada correspondiente al mismo tiempo. La información de atributo relacionada incluye la información de remitente de la información de aplicación objetivo, por ejemplo, un número de dispositivo de un remitente de un mensaje SMS, un número de teléfono móvil, o un número específico de una institución, o información de dirección de correo electrónico de un remitente de un correo electrónico. La información de atributo relacionada incluye además el contenido de la información de aplicación objetivo, por ejemplo, contenido

de texto de un mensaje SMS o contenido del cuerpo de un correo electrónico, y similar. La información de atributo relacionada incluye además la información de guía de usuario. La información de guía de usuario incluye cualquier información que indica a un usuario que realice una operación relacionada. Por ejemplo, un hipervínculo del sitio web proporcionado al usuario o información de dirección de descarga proporcionada al usuario, y similar. En este caso, se realizan diferentes operaciones de validación y análisis basándose en diferentes contenidos específicos de la información de atributo relacionada, por ejemplo, se seleccionan diferentes bases de datos de validación para diferente información de atributo relacionada para realizar la búsqueda de coincidencias.

En este caso, un experto en la técnica entenderá que la información de remitente de la información de aplicación objetivo, la información de contenido de la información de aplicación objetivo o la información de guía de usuario de la información de aplicación objetivo son sólo ejemplos, y que la información de atributo relacionada de otra información de aplicación objetivo existente o futura que es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

En una forma de realización preferida (con referencia a la figura 3), la información de atributo relacionada incluye la información de guía de usuario de la información de aplicación objetivo. La etapa S32 incluye además la etapa S323 (no mostrada). En la etapa S323, cuando no se identifica información de registro que coincide con la información de guía de usuario en la base de datos de validación, el dispositivo de red 1 simula la ejecución de la información de aplicación objetivo basándose en la información de guía de usuario para obtener la información de riesgo correspondiente.

Específicamente, en esta forma de realización, cuando la información de atributo relacionada incluye la información de guía de usuario de la información de aplicación objetivo, si no se identifica información de registro que coincide con la información de guía de usuario en la base de datos de validación, preferiblemente, se realiza una ejecución de simulación específica en la información de guía de usuario. En este caso, considerando que un proceso de ejecución de simulación puede tener un riesgo para la seguridad, el dispositivo de red 1 puede disponerse en un entorno de pruebas seguro para realizar un experimento de simulación. Por ejemplo, cuando la información de guía de usuario es un enlace de descarga o información de sitio web, el dispositivo de red 1 extrae la información de guía de usuario, y ejecuta un navegador u otro programa correspondiente en un entorno de pruebas seguro previamente configurado para abrir la información URL del sitio web anterior o el enlace descendente para realizar la operación indicada por la información de guía de usuario. Además, se analiza el problema de seguridad en un proceso de operación de ejecución, o adicionalmente se determina y analiza el resultado de ejecución de la ejecución de simulación para obtener la información de riesgo correspondiente. Por ejemplo, si se abre un enlace de sitio web correspondiente a la información de guía de usuario a través de una ejecución de simulación, y el resultado corresponde a un sitio web de *phishing*, puede deducirse que la información de aplicación objetivo es de riesgo, y se determina la información de riesgo correspondiente. En este caso, posteriormente se borran los cambios producidos por una operación ejecutada en el entorno de pruebas seguro. Además, los posibles riesgos que pueden producirse al ejecutar un programa en el entorno de ejecución virtual no producen un daño real a los dispositivos relacionados como el dispositivo de red 1.

Además, basándose en una fuente de riesgo, por ejemplo, información de sitio web de *phishing*, un virus troyano, o un riesgo para la seguridad de un texto de mensaje SMS, puede realizarse una extracción y clasificación de información de riesgo en información de aplicación objetivo con riesgo relativamente alto, determinada a través de la ejecución de simulación, para actualizar la información sobre la base de datos de validación correspondiente, y transmitir la información de riesgo a diferentes instituciones financieras basándose en tipos de riesgo.

En esta forma de realización, el dispositivo de red 1 realiza una búsqueda de coincidencias en la base de datos de validación correspondiente basándose en la información de atributo relacionada de la información de aplicación objetivo. Para información de aplicación objetivo que no coincide con la información de registro correspondiente, el dispositivo de red 1 puede simular adicionalmente la ejecución de la información de guía de usuario correspondiente para determinar la información de riesgo correspondiente. Por tanto, se garantiza una precisión de determinación de información de riesgo con una forma de determinación de múltiples niveles. Así, el usuario puede realizar un procesamiento eficaz basándose en la información de aviso correspondiente a información de riesgo de alta precisión.

Preferiblemente, en la etapa S323, cuando no se identifica información de registro que coincide con la información de guía de usuario en la base de datos de validación, el dispositivo de red 1 simula la adquisición, basándose en la información de guía de usuario, de información objetivo que está en la información de aplicación objetivo y hacia la que se guía al usuario para que la adquiera; y valida la correspondencia entre la información objetivo y la información de aplicación objetivo para obtener la información de riesgo correspondiente.

Específica y preferiblemente, la información objetivo que está en la información de aplicación objetivo y se adquiere por un usuario guiado se obtiene en primer lugar por medio de simulación basándose en la información de usuario guiado. En este caso, la información objetivo incluye un resultado correspondiente al que apunta el dispositivo de red 1 ejecutando la información de usuario de guía mediante simulación. Por ejemplo, la información objetivo puede ser una página web hacia la que se guía al usuario para que la abra, o puede ser un archivo hacia el que se guía al usuario

para que lo descargue. A continuación, el dispositivo de red 1 valida la correspondencia entre la información objetivo y la información de aplicación objetivo para obtener la información de riesgo correspondiente. En este caso, los riesgos producidos por la información objetivo incluyen un riesgo directo impuesto a la seguridad de la privacidad del usuario y seguridad del equipo de usuario, por ejemplo, un archivo descargado incluye un virus. Los riesgos producidos por la información objetivo también incluyen un riesgo potencial producido por cierta información de spam, por ejemplo, cuando un sitio web abierto es un sitio web de anuncio falso, puede producirse un cierto daño si el usuario realiza una operación correspondiente basándose en información de instrucción en el sitio web. En este caso, se determina la correspondencia entre la información objetivo y la información de aplicación objetivo para determinar la relevancia de la información objetivo y la información de aplicación objetivo. En general, existe información de aplicación objetivo de alto riesgo tal como un mensaje SMS falso con el propósito de engañar al usuario para que realice una operación contra su voluntad o para que realice involuntariamente una operación desfavorable. Por tanto, existe una posibilidad relativamente alta de que la información objetivo correspondiente a tal información de aplicación objetivo sea incoherente con o no coincida con la información de aplicación objetivo. Esta es una base importante para validar la correspondencia en la presente solicitud. La validación de correspondencia entre la información objetivo y la información de aplicación objetivo puede incluir comprobar si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo; comprobar si el contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo; o comprobar si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo.

En este caso, un experto en la técnica entenderá que los procedimientos anteriores para validar la correspondencia entre la información objetivo y la información de aplicación objetivo son sólo ejemplos, y que un procedimiento existente o futuro para validar la correspondencia entre la información objetivo y la información de aplicación objetivo y que es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

Más preferiblemente, la validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye al menos una de las siguientes: comprobar si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo; comprobar si el contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo; o comprobar si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo.

Específicamente, la validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye comprobar si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo. Si la información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo, puede deducirse que la información objetivo coincide con la información de aplicación objetivo. Por tanto, por la validación puede deducirse que la información de aplicación objetivo tiene una alta seguridad y un bajo riesgo. Por el contrario, se deduce que la información objetivo no coincide con la información de aplicación objetivo. Por la validación puede deducirse que la información de aplicación objetivo tiene una baja seguridad y un alto riesgo. En este caso, por ejemplo, la información de aplicación objetivo es un mensaje SMS. Si un remitente del mensaje SMS es un número de un operador móvil, el contenido del mensaje SMS está relacionado con proporcionar llamadas gratuitas, y la información de guía de usuario es un enlace de página web del operador, y si la información objetivo adquirida es de hecho una página web relacionada de la operación móvil, se considera que el remitente de la información objetivo es coherente con el remitente del mensaje SMS, y puede deducirse que la información objetivo coincide con la información de aplicación objetivo. Por el contrario, si después de pinchar en el enlace se abre una página web irrelevante, puede deducirse que la información objetivo no coincide con la información de aplicación objetivo. En este caso, preferiblemente, si la información de remitente es incoherente, adicionalmente puede determinarse si el remitente de la información de aplicación objetivo es una estación base no autorizada que de manera dedicada envía información falsa. En tal caso, puede deducirse que la información de aplicación enviada por el remitente es información falsa. Además, el dispositivo de red 1 puede registrar adicionalmente información sobre la estación base no autorizada, y avisar al equipo de usuario 2 relacionado.

La validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye además comprobar si el contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo. En este caso, si el contenido de la información objetivo coincide con el contenido de la información de aplicación objetivo, se considera que la correspondencia entre la información objetivo y la información de aplicación objetivo es relativamente alta, y se deduce que la seguridad de la información de aplicación objetivo es relativamente alta, y el riesgo es bajo. Por el contrario, se deduce que la información de aplicación objetivo es menos segura y tiene un mayor riesgo. En este caso, por ejemplo, la información de aplicación objetivo es un mensaje SMS. Si el contenido del mensaje SMS es un enlace sobre información sobre descuentos en centros comerciales, pero después de pinchar en el enlace se abre un sitio web de pago irrelevante, se deduce que el contenido de la información objetivo no está

relacionado con el contenido de la información de aplicación objetivo, y que la información objetivo puede ser potencialmente peligrosa.

La validación de correspondencia entre la información objetivo y la información de aplicación objetivo incluye además comprobar si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo. En este caso, si la información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo, la información de aplicación objetivo es relativamente segura con un menor riesgo. Por el contrario, si la información de operación en el entorno de pruebas seguro de la información objetivo no coincide con la información de aplicación objetivo, puede deducirse que la información de aplicación objetivo tiene una baja seguridad y un alto riesgo. En este caso, por ejemplo, la información de aplicación objetivo es un mensaje SMS. Cuando la información objetivo es una aplicación descargada correspondiente a un enlace de descarga en el mensaje SMS, si la aplicación descargada se instala o ejecuta en el entorno de pruebas seguro, y si una etapa de operación específica es diferente de lo descrito en la información de aplicación objetivo, o un resultado obtenido ejecutando la aplicación es diferente de lo descrito en la información de aplicación objetivo, puede deducirse que la información de operación en el entorno de pruebas seguro de la información objetivo no coincide con la información de aplicación objetivo, y que hay un alto riesgo para la seguridad.

En este caso, un experto en la técnica entenderá que los procedimientos anteriores para validar la correspondencia entre la información objetivo y la información de aplicación objetivo son sólo ejemplos, y que un procedimiento existente o futuro para validar la correspondencia entre la información objetivo y la información de aplicación objetivo y que es aplicable a la solución entrarán dentro del alcance de protección de la presente solicitud, y se incorpora al presente documento por referencia.

En una forma de realización preferida (con referencia a la figura 3), la información de aplicación objetivo incluye un mensaje SMS, y el procedimiento incluye además la etapa S34 (no mostrada). En la etapa S34, el dispositivo de red 1 envía información de aviso de estación base no autorizada al equipo de usuario cercano del equipo de usuario cuando la información de riesgo es que el mensaje SMS es información falsa. Una distancia entre el equipo de usuario cercano y el equipo de usuario es menor que o igual a un umbral de distancia predeterminado entre dispositivos.

Específicamente, en este caso, la estación base no autorizada es una pseudoestación base, y habitualmente comprende un anfitrión y un portátil. La estación base no autorizada puede estar configurada para buscar la información sobre una tarjeta de módulo de identidad de abonado (SIM) en un área dentro de un determinado radio de la estación base utilizando un dispositivo como un dispositivo de envío de mensajes SMS, un remitente de mensajes SMS, o similar. La estación base no autorizada envía a la fuerza un mensaje SMS como un mensaje de *Smishing* o un mensaje SMS de publicidad al teléfono móvil del usuario mostrándose a sí misma como una estación base de un operador y utilizando de manera fraudulenta un número de teléfono móvil de otro usuario. En esta forma de realización, la información de aplicación objetivo incluye información de mensaje SMS. Si la información de riesgo de la información de aplicación objetivo obtenida mediante la validación por el dispositivo de red 1 incluye que el mensaje SMS es información falsa, y además puede deducirse que la información falsa se envía por una estación base no autorizada correspondiente, puede determinarse la información de ubicación de la estación base no autorizada, o puede determinarse una pista de movimiento de la estación base no autorizada para deducir la información de ubicación de la estación base no autorizada. Además, el aparato de envío de información de aviso de estación base no autorizada envía la información de aviso de estación base no autorizada al equipo de usuario cercano del equipo de usuario, siendo la distancia entre el equipo de usuario cercano y el equipo de usuario menor que o igual a una información de umbral de distancia predeterminado entre dispositivos. El equipo de usuario cercano incluye varios dispositivos terminales inteligentes móviles, y preferiblemente, incluye un dispositivo con una función de comunicación móvil, por ejemplo, un dispositivo terminal que puede recibir un mensaje SMS, como un teléfono móvil, o un ordenador de tableta con una función de recepción/envío de mensajes SMS. En este caso, el umbral de distancia predeterminado entre dispositivos puede establecerse basándose en la información de ubicación de la estación base no autorizada y la cobertura del envío del mensaje SMS. En este caso, la información de aviso de estación base no autorizada puede enviarse al equipo de usuario cercano cuando el dispositivo de red 1 adquiere y determina en primer lugar la información sobre la estación base no autorizada. Alternativamente, cada vez que se determina que el mensaje SMS es información falsa, la información de aviso de estación base no autorizada puede enviarse al equipo de usuario cercano al mismo tiempo. En este caso, si se habilita una función de posicionamiento correspondiente en el equipo de usuario cercano, por ejemplo, una función GPS (*Global Positioning System*, sistema de posicionamiento global) de un teléfono móvil, el dispositivo de red 1 puede buscar y obtener información de latitud y longitud correspondiente del teléfono móvil. En este caso, si la distancia entre el equipo de usuario cercano y el equipo de usuario es menor que o igual al umbral de distancia predeterminado entre dispositivos, la información de aviso de estación base no autorizada se envía al equipo de usuario cercano.

En esta forma de realización, cuando la información de riesgo incluye que la información de mensaje SMS es información falsa, el dispositivo de red 1 envía la información de aviso de estación base no autorizada al equipo de usuario cercano del equipo de usuario 2. Cuando la información falsa corresponde a una estación base no autorizada, puede enviarse un aviso a otro equipo de usuario que se encuentre en el área de cobertura de la estación base no

autorizada y que pueda recibir el mensaje de *Smishing* para reducir y evitar más riesgos producidos por la información falsa enviada por la estación base no autorizada. Específicamente, cuando otro equipo de usuario utiliza una aplicación objetivo, el dispositivo de red 1 puede enviar información sobre la existencia de una estación base no autorizada cerca del dispositivo de red 1, y el dispositivo de red 1 puede emitir directamente un aviso con el permiso del otro equipo de usuario.

La figura 4 muestra un diagrama de flujo de un procedimiento para la gestión de riesgos de información de aplicación en un lado de dispositivo de red y un lado de equipo de usuario. En la etapa S41, el equipo de usuario 2 adquiere información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando el equipo de usuario 2. En la etapa S43, el equipo de usuario 2 envía la información de aplicación objetivo a un dispositivo de red 1 correspondiente. En la etapa S42, el dispositivo de red 1 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. En la etapa S44, el dispositivo de red 1 devuelve la información de aviso correspondiente al equipo de usuario 2 basándose en la información de riesgo. En este caso, la etapa S42 y la etapa S44 son iguales o básicamente iguales a la etapa S32 y la etapa S33 mostradas en la figura 3. Aquí no se describen de nuevo los detalles, y se incorporan al presente documento por referencia.

Específicamente, en la etapa S41, el equipo de usuario 2 adquiere la información de aplicación objetivo que selecciona el usuario y cuya validación solicita utilizando el equipo de usuario 2. En este caso, preferiblemente, la información de aplicación objetivo se determina directamente basándose en una operación de selección autónoma del usuario. En este caso, la información de aplicación como un mensaje SMS, un mensaje de WeChat o un correo electrónico incluye información masiva de la privacidad del usuario. Por tanto, si toda la información se carga por una aplicación de un tercero, se aumenta un riesgo de pérdida de información. Por tanto, en la presente solicitud, preferiblemente, el usuario puede seleccionar de manera autónoma una información o varias informaciones de aplicación objetivo que en realidad es necesario enviar al dispositivo de red para su validación. En este caso, además, preferiblemente, el usuario puede realizar directamente una operación de selección en una interfaz de operación de una aplicación objetivo correspondiente a la información de aplicación objetivo en el equipo de usuario 2. Por ejemplo, si la información de aplicación objetivo es un mensaje SMS, el usuario puede seleccionar directamente un mensaje sospechoso de *Smishing* cuando entra en la aplicación de SMS, de modo que se evita la necesidad de tener que saltar a otra interfaz de aplicación de un tercero. En este caso, puede implementarse una operación de respuesta para una instrucción del usuario para una selección y solicitud de validación ejecutando un programa de aplicación independiente cargado en el dispositivo de red 1, o ejecutando un complemento correspondiente que coincide con la aplicación objetivo como la aplicación de SMS.

Después, en la etapa S43, el equipo de usuario 2 envía la información de aplicación objetivo al dispositivo de red 1 correspondiente. En este caso, la información de aplicación objetivo enviada al dispositivo de red 1 puede estar en la forma original de la información de aplicación objetivo adquirida por el equipo de usuario 2. Por ejemplo, si la información de aplicación objetivo es un mensaje SMS, la información de aplicación objetivo adquirida por el dispositivo de red 1 puede estar en forma de un texto de mensaje SMS visualizado en la interfaz de aplicación de SMS del equipo de usuario 2. Además, el equipo de usuario 2 puede analizar en primer lugar la información de aplicación original recibida por el equipo de usuario 2 o extraer la información de la información de aplicación original. Por ejemplo, el equipo de usuario 2 extrae una palabra clave de un mensaje SMS basándose en una categoría y envía la palabra clave extraída al dispositivo de red 1. Así, el equipo de usuario 2 en primer lugar y de manera preliminar, puede analizar y clasificar la información de aplicación objetivo que va a validarse, y puede reducir un volumen de datos transmitidos entre dispositivos. Además, cuando se envía la información de aplicación objetivo, el equipo de usuario 2 puede enviar además, al dispositivo de red 1, información de atributo relacionada correspondiente a la información de aplicación objetivo, como información de remitente de la información de aplicación objetivo o información de guía de usuario de la información de aplicación objetivo, para realizar posteriormente operaciones de validación de riesgo en la información de aplicación objetivo en el dispositivo de red 1 de múltiples maneras. En este caso, preferiblemente, el equipo de usuario 2 envía la información de aplicación objetivo al dispositivo de red 1 con una transmisión cifrada.

Después, en la etapa S42, el dispositivo de red 1 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente. En la etapa S44, el dispositivo de red 1 devuelve la información de aviso correspondiente al equipo de usuario 2 basándose en la información de riesgo. En este caso, preferiblemente, la información de aviso recibida por el equipo de usuario 2 es información de aviso correspondiente generada por el dispositivo de red 1 basándose en la información de riesgo obtenida mediante validación. Por ejemplo, cuando la información de riesgo es información determinante de que existe un riesgo, como cuando la información de riesgo es que un mensaje SMS objetivo es información falsa, se genera la información de aviso de riesgo correspondiente. El contenido de la información de aviso de riesgo puede incluir destacar un mensaje SMS con un aviso de riesgo en el equipo de usuario 2, un mensaje SMS de aviso específico, o información de aviso en otra forma, o incluso un proceso directo del mensaje SMS como mensaje SMS basura por el equipo de usuario 2, etc. Como otro ejemplo, cuando el dispositivo de red 1 determina que la información de riesgo es información determinante de que no existe ningún riesgo, el equipo de usuario 2 adquiere información de seguridad de validación correspondiente. Además, en este caso, preferiblemente, el usuario puede elegir adoptar la información de aviso enviada por el dispositivo de red 1 para realizar un procesamiento posterior en la información de aplicación como un mensaje SMS del usuario, o elegir no

adoptar la información de aviso y retener la información de aplicación objetivo. Así, se respeta totalmente el derecho del usuario de procesar información relacionada con la privacidad del usuario. Además, el contenido de información de aviso puede ejecutarse automáticamente basándose en ajustes predeterminados realizados por el usuario cuando se obtiene la información de aviso correspondiente. Por ejemplo, el usuario puede realizar una preselección. Así, después de que el dispositivo de red 1 realice una validación de riesgos, si un riesgo de la información de aplicación objetivo es relativamente alto y alcanza un nivel predeterminado, la información de aplicación objetivo se borra automáticamente. Por tanto, después de que el equipo de usuario 2 reciba información de aviso que cumple con una condición, automáticamente puede realizarse una operación de instrucción correspondiente, y no tiene que preguntarse al usuario. En resumen, la operación automática no va en contra de la voluntad del usuario, sino que es el resultado de la participación del usuario en la operación.

En este caso, el equipo de usuario 2 envía la información de aplicación objetivo seleccionada por el usuario al dispositivo de red 1 correspondiente para su validación, y recibe la información de aviso que se devuelve por el dispositivo de red 1 y que se basa en la información de riesgo de la información de aplicación objetivo. Así, el equipo de usuario actúa conjuntamente con el dispositivo de red 1 para implementar la gestión de riesgos en la información de aplicación.

selecciona de la una información o las varias informaciones de aplicación y solicita su validación utilizando el equipo de usuario 2.

Específicamente, de manera habitual no puede reconocerse fácilmente la información de aplicación objetivo con un riesgo relativamente alto como un mensaje SMS falso. Por tanto, para facilitar la selección autónoma de la información de aplicación objetivo por el usuario, mejorar la probabilidad de que la información de aplicación objetivo seleccionada de manera autónoma por el usuario se determine como información de aplicación de alto riesgo y mejorar la eficiencia de la realización posterior de la validación de riesgo de información de aplicación objetivo por el dispositivo de red 1, preferiblemente, en la etapa S45, el equipo de usuario 2 puede realizar el preanálisis de riesgo en la información de aplicación recibida por el equipo de usuario 2, y a continuación se proporciona una asistencia inmediata correspondiente al usuario basándose en el resultado del preanálisis de riesgo. En este caso, el equipo de usuario 2 puede adquirir y almacenar de antemano cierta información relacionada sobre información de aplicación que se recopiló recientemente y que tiene un riesgo relativamente alto. Por ejemplo, se adquiere previamente una base de datos de recopilación reciente de números de remitentes de mensajes *Smishing*, y a continuación, basándose en información de la base de datos, se realiza un preanálisis de riesgo en un mensaje SMS recibido por el equipo de usuario 2. En este caso, la información de datos que se utiliza como datos de referencia de preanálisis puede proceder del dispositivo de red 1 correspondiente, por ejemplo, de una recopilación de información relacionada sobre información de base de datos de validación reciente correspondiente al dispositivo de red 1, por ejemplo, información de base de datos de validación en un mes. Como otro ejemplo, una lista de datos de riesgo recientes en una región actual puede almacenarse en el equipo de usuario 2, y a continuación se compara la información de aplicación adquirida por el equipo de usuario 2 con la lista de datos. En este caso, puede realizarse un análisis de evaluación preliminar de la información de aplicación sin aumentar la carga de la operación del equipo de usuario 2, para avisar de manera eficaz al usuario.

Después, en la etapa S46, el equipo de usuario 2 visualiza, en una aplicación correspondiente, una información o varias informaciones de aplicación que están en riesgo, adquiridas mediante el preanálisis de riesgo. En este caso, el resultado del preanálisis de riesgo puede visualizarse de manera eficaz en una interfaz de aplicación objetivo, por ejemplo, mostrarse de manera destacada. Por ejemplo, la información de aplicación que está en riesgo puede visualizarse de manera que incluya, pero no se limite a diferentes colores o fuentes o marcadores de aviso específicos. Como otro ejemplo, se avisa al usuario mediante una ventana de aviso. Después, en la etapa S41, el equipo de usuario 2 adquiere la información de aplicación objetivo que el usuario selecciona de la una información o las varias informaciones de aplicación

Resultará evidente para un experto en la técnica que la presente solicitud no está limitada a los detalles de las formas de realización de ejemplo anteriores y que la presente solicitud puede implementarse de otra forma específica sin apartarse del espíritu o característica esencial de la presente solicitud. Por tanto, las formas de realización deberán considerarse ilustrativas y no restrictivas en cualquier aspecto, y el alcance de la presente solicitud está limitado por las reivindicaciones adjuntas, en lugar de por la descripción anterior. Por tanto, la presente solicitud abarca todos los cambios dentro del significado y el alcance de los elementos equivalentes de las reivindicaciones. Ningún número de referencia en las reivindicaciones deberá considerarse como una limitación de la reivindicación relacionada. Además, resulta evidente que el término “incluir” no excluye otra unidad o etapa, y que el singular no excluye el plural. Una pluralidad de unidades o aparatos descritos en las reivindicaciones de aparato también pueden implementarse por una unidad o aparato utilizando software o hardware. Términos como “primero” y “segundo” se utilizan para indicar nombres en lugar de cualquier orden particular.

REIVINDICACIONES

1. Un procedimiento para la gestión de riesgos de información de aplicación en un dispositivo de red, comprendiendo el procedimiento:

recibir información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando un dispositivo de usuario (S31), en el que la información de aplicación objetivo comprende un mensaje SMS;

validar la información de aplicación objetivo para determinar información de riesgo correspondiente (S32);

transmitir la información de aviso de estación base no autorizada al dispositivo de usuario basándose en la información de riesgo (S33);

caracterizado por que, si la información de riesgo correspondiente indica que el mensaje SMS comprende información falsa enviada por una estación base no autorizada, el procedimiento comprende, además:

enviar información de aviso de estación base no autorizada a otros dispositivos de usuario cerca del dispositivo de usuario, en el que una distancia entre cada dispositivo de usuario y el dispositivo de usuario es menor que o igual a un umbral de distancia predeterminado entre dispositivos.

2. El procedimiento según la reivindicación 1, en el que validar la información de aplicación objetivo para obtener la información de riesgo correspondiente comprende:

realizar una búsqueda de coincidencias en una base de datos de validación correspondiente basándose en una información de atributo relacionada de la información de aplicación objetivo; y

determinar la información de riesgo correspondiente basándose en una información de registro que está en la base de datos de validación y que coincide con la información de atributo relacionada.

3. El procedimiento según la reivindicación 2, en el que la base de datos de validación comprende al menos una de una biblioteca de plantillas de mensajes y una clasificación que permite una validación sucesiva de la información de aplicación objetivo.

4. El procedimiento según la reivindicación 2, en el que la información de atributo relacionada comprende al menos uno de los siguientes:

una información de remitente de la información de aplicación objetivo;

un contenido de la información de aplicación objetivo; o

una información de guía de usuario de la información de aplicación objetivo.

5. El procedimiento según la reivindicación 4, en el que:

la información de atributo relacionada comprende la información de guía de usuario de la información de aplicación objetivo, y

validar la información de aplicación objetivo para obtener información de riesgo correspondiente comprende, además, si en la base de datos de validación no se identifica información de registro que coincida con la información de guía de usuario, simular una ejecución de la información de aplicación objetivo basándose en la información de guía de usuario para obtener la información de riesgo correspondiente.

6. El procedimiento según la reivindicación 5, en el que simular la ejecución de la información de aplicación objetivo basándose en la información de guía de usuario para obtener la información de riesgo correspondiente comprende:

simular la adquisición, basándose en la información de guía de usuario, de la información objetivo que está en la información de aplicación objetivo y hacia la que se guía al usuario para que la adquiera; y

validar una correspondencia entre la información objetivo y la información de aplicación objetivo para obtener la información de riesgo correspondiente.

7. El procedimiento según la reivindicación 6, en el que validar la correspondencia entre la información objetivo y la información de aplicación objetivo comprende al menos uno de los siguientes:

comprobar si una información de remitente de la información objetivo es coherente con la información de remitente de la información de aplicación objetivo;

comprobar si un contenido de la información objetivo está asociado con el contenido de la información de aplicación objetivo; y

comprobar si una información de operación en el entorno de pruebas seguro de la información objetivo coincide con la información de aplicación objetivo.

8. El procedimiento según la reivindicación 1, en el que el mensaje SMS comprende un mensaje *Smishing*.

9. Un aparato para la gestión de riesgos de información de aplicación, comprendiendo el aparato una pluralidad de módulos configurados para realizar el procedimiento según una cualquiera de las reivindicaciones 1 a 8.

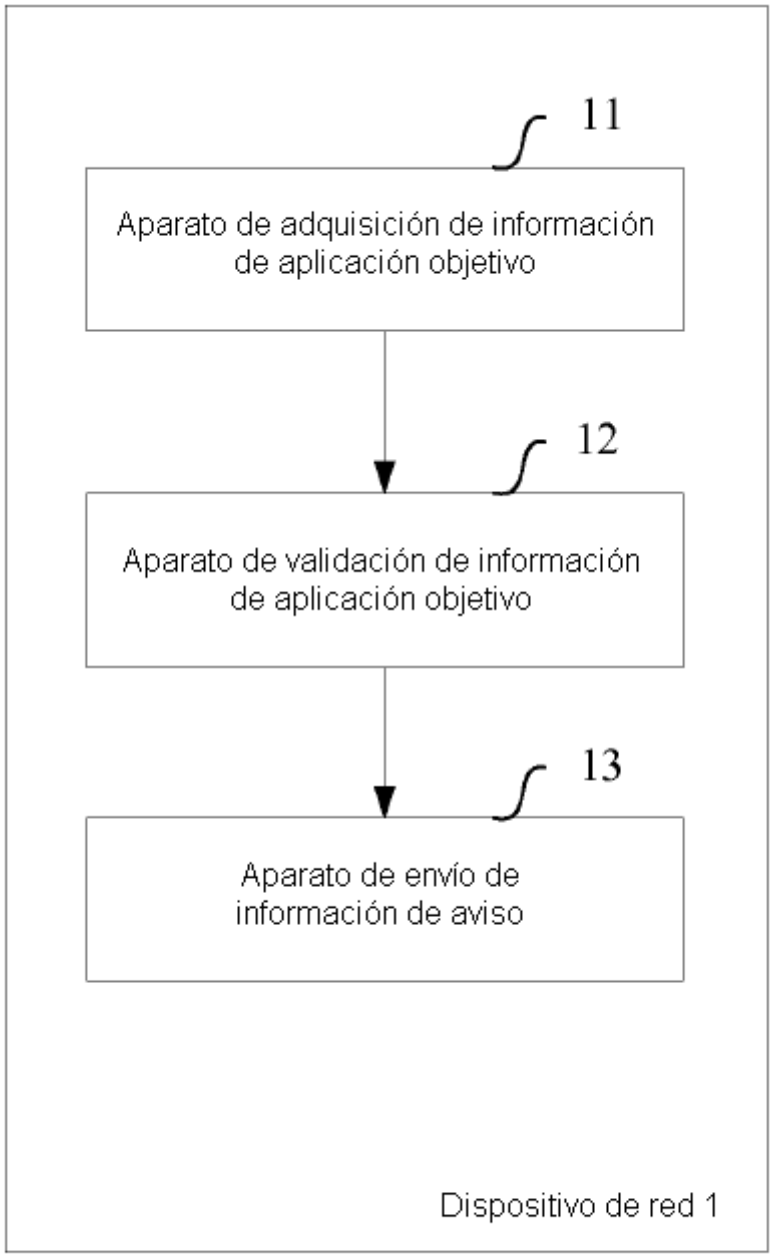
11
Aparato de adquisición de información de aplicación objetivo
12
Aparato de validación de información de aplicación objetivo
13
Aparato de envío de información de aviso
Dispositivo de red 1

FIG. 1

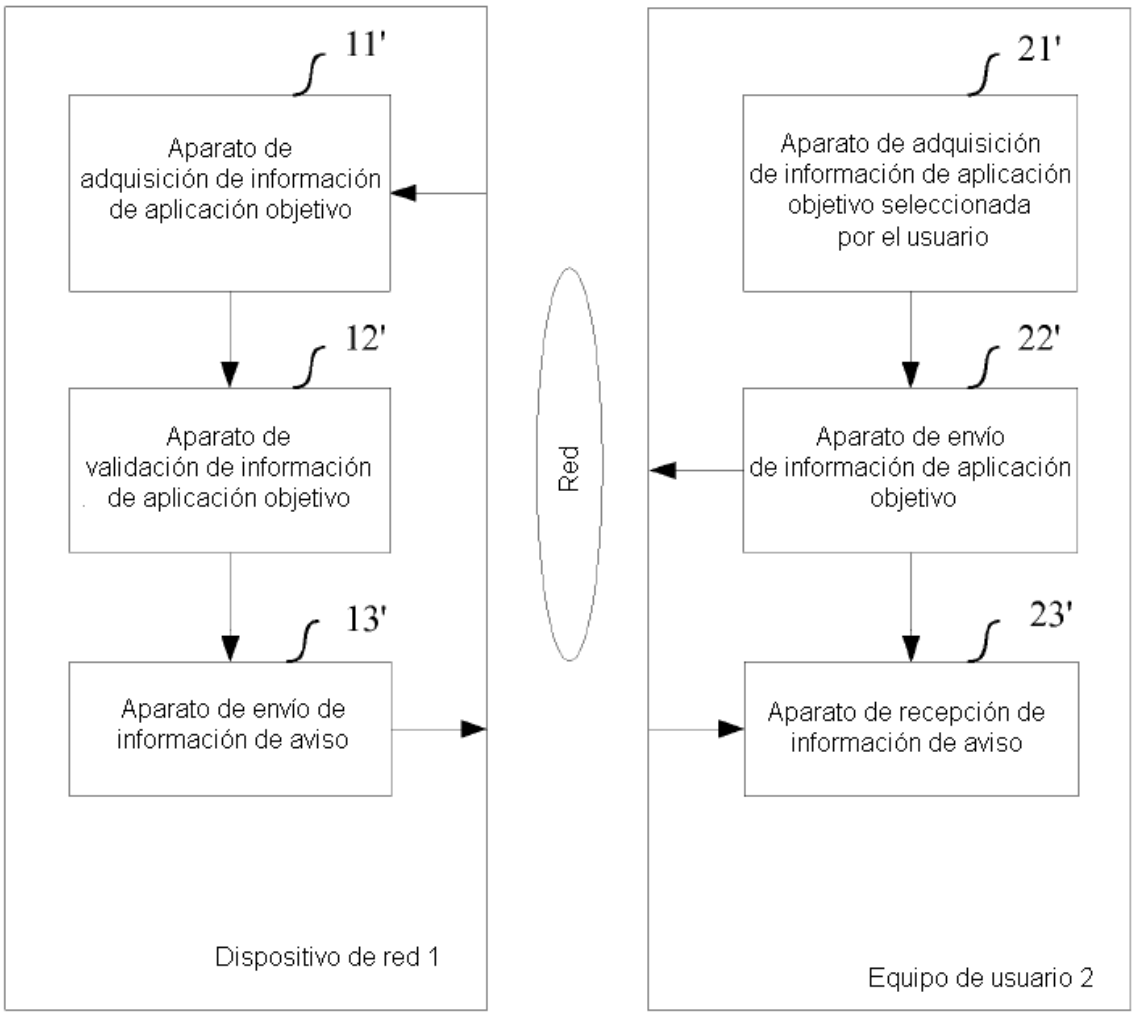
11'
Aparato de adquisición de información de aplicación objetivo
12'
Aparato de validación de información de aplicación objetivo
13'
Aparato de envío de información de aviso
Dispositivo de red 1
Red
21'
Aparato de adquisición de información de aplicación objetivo seleccionada por el usuario
22'
Aparato de envío de información de aplicación objetivo
23'
Aparato de recepción de información de aviso
Equipo de usuario 2

FIG. 2

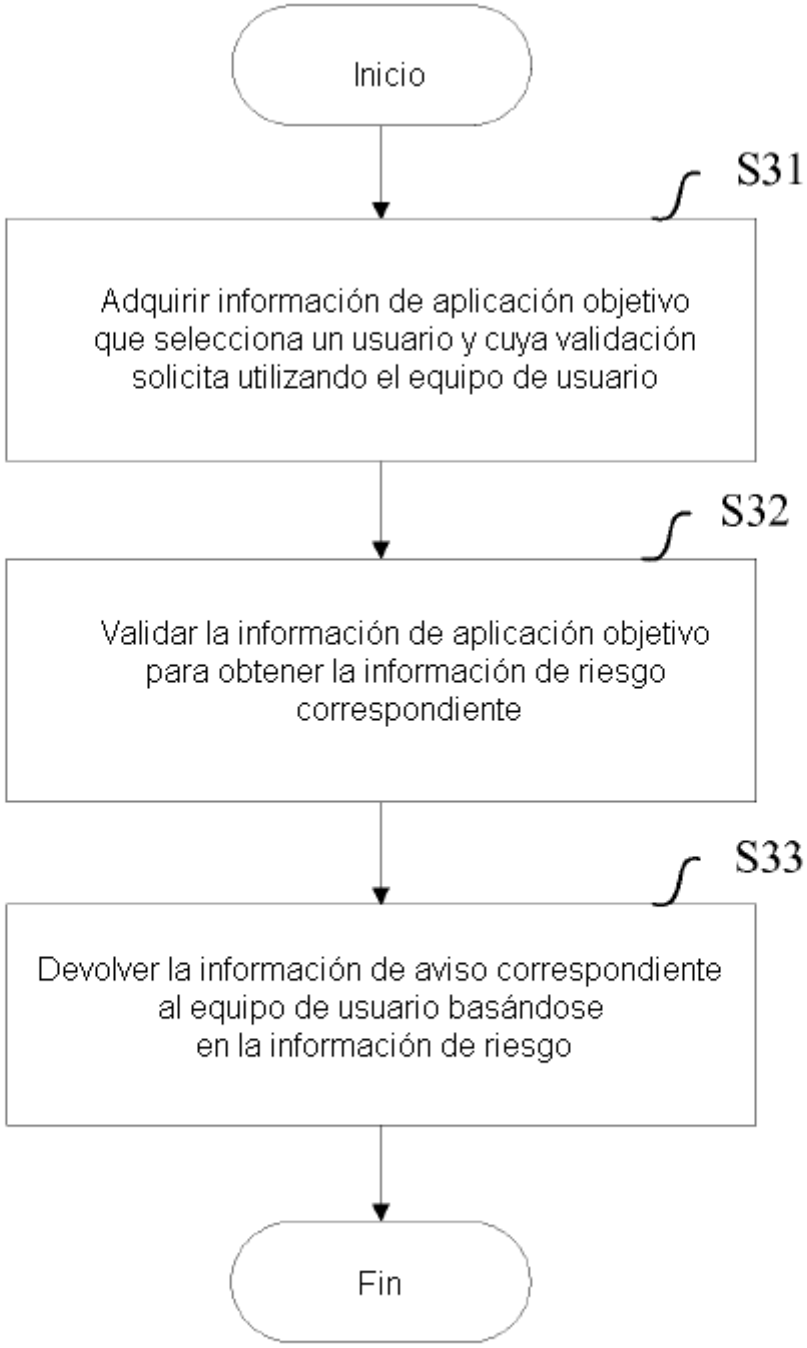
Inicio
S31
Adquirir información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando el equipo de usuario
S32
Validar la información de aplicación objetivo para obtener la información de riesgo correspondiente
S33
Devolver la información de aviso correspondiente al equipo de usuario basándose en la información de riesgo
Fin

FIG. 3

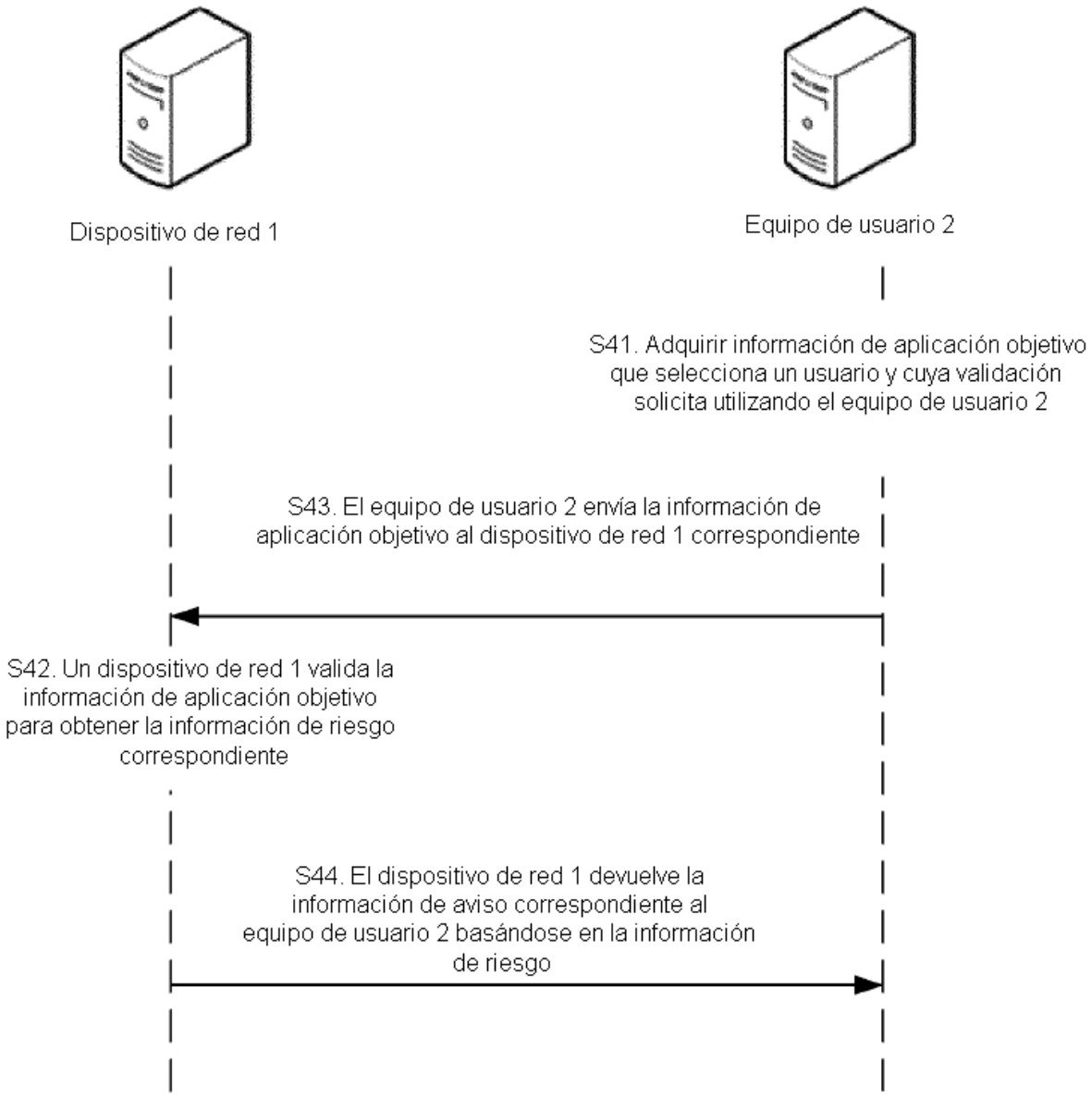
Dispositivo de red 1
Equipo de usuario 2
S41. Adquirir información de aplicación objetivo que selecciona un usuario y cuya validación solicita utilizando el equipo de usuario 2
S43. El equipo de usuario 2 envía la información de aplicación objetivo al dispositivo de red 1 correspondiente
S42. Un dispositivo de red 1 valida la información de aplicación objetivo para obtener la información de riesgo correspondiente
S44. El dispositivo de red 1 devuelve la información de aviso correspondiente al equipo de usuario 2 basándose en la información de riesgo

FIG. 4