(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 670**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 4/00 (2008.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.08.2002 PCT/IB2002/02992**

(87) Fecha y número de publicación internacional: **20.02.2003 WO03014861**

(96) Fecha de presentación y número de la solicitud europea: **01.08.2002 E 02755406 (2)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 1415231**

(54) Título: **Método y sistema para visualizar un nivel de confianza de las operaciones de comunicación de red y la conexión de servidores**

(30) Prioridad:

07.08.2001 US 922672

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.06.2020

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

COFTA, PIOTR y
PAATERO, LAURI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y sistema para visualizar un nivel de confianza de las operaciones de comunicación de red y la conexión de servidores

Campo técnico

La presente invención se refiere a un sistema y método que permite al usuario de un terminal visualizar un nivel de confianza de las comunicaciones de red y las conexiones a los servidores.

Descripción de la técnica anterior

El documento WO01/26401 (D1) desvela un aparato de comunicación portátil que tiene una interfaz hombre-máquina, un controlador, un sistema operativo, un dispositivo de almacenamiento local para almacenar una primera aplicación, un recurso seguro al que solo se puede acceder desde el sistema operativo y una interfaz inalámbrica para conectar el aparato de comunicación portátil a un dispositivo remoto. De acuerdo con D1, la interfaz hombre-máquina proporciona interacción entre un usuario del aparato de comunicación portátil y la primera aplicación cuando es ejecutada por el controlador y el sistema operativo. En D1, la interfaz hombre-máquina proporciona también interacción entre el usuario y una segunda aplicación que se origina en el dispositivo remoto. De acuerdo con D1, el sistema operativo y solo el sistema operativo puede proporcionar un indicador de seguridad a través de la interfaz hombre-máquina. En D1, el indicador de seguridad representa una conexión segura entre el recurso seguro y una de la primera y segunda aplicaciones, que actualmente utiliza la interfaz hombre-máquina.

La Figura 1 muestra un terminal móvil 1 de la técnica anterior del cesionario utilizado para telecomunicaciones celulares, que se comunica a través de una red inalámbrica de telecomunicaciones, por ejemplo, una red celular.

El teclado 2 tiene un primer grupo de doce teclas 7, por ejemplo, teclas alfanuméricas, por medio de las que el usuario puede ingresar un número de teléfono, escribir un mensaje de prueba utilizando el servicio de mensajes cortos (SMS), escribir un nombre (asociado al número de teléfono), etc. Cada una de las doce teclas alfanuméricas 7 está provista de números de identificación "0-9" o un signo "#" o "*", respectivamente. En el modo alfa, cada tecla está asociada a varias letras y se usan signos especiales en la edición de texto.

El teclado 2 comprende adicionalmente un segundo grupo de teclas que son dos teclas programables 8, dos teclas de manejo de llamadas 9 y una tecla de navegación 10. Las dos teclas programables 8 funcionan junto con la pantalla de cristal líquido 3 para mostrar el texto que varía de acuerdo con el modo de operación y proporcionan al usuario la capacidad de seleccionar diferentes modos de operación programados proporcionados por la programación residente en la memoria 17. Las teclas programables no se limitan a la selección de una única función de terminal dedicada. Las teclas programables 8 ilustradas pueden tener una funcionalidad correspondiente a los modelos 2110™ y 8110™ del Cesionario. Al menos una de las teclas programables se define como una tecla de operación 8a que tiene múltiples funciones para manejar el acceso a una estructura de menú. La funcionalidad de la tecla de operación 8a depende del estado actual del terminal móvil. La tecla de operación 8a se dispone para realizar un grupo de acciones predeterminadas asociadas a un estado. La función predeterminada o la función actual de la tecla de operación 8a se puede visualizar en un área predeterminada 21 de la pantalla 3.

La tecla de desplazamiento 10, que también se puede llamar tecla de navegación, es una tecla de arriba/abajo y se coloca centralmente en la superficie frontal del terminal móvil entre la pantalla 3 y el grupo de teclas alfanuméricas 7. El usuario controla la tecla de desplazamiento 10 simplemente presionando la tecla de arriba/abajo usando su pulgar que le permite desplazarse entre un grupo de elementos en un menú proporcionado en la interfaz de usuario. Puesto que muchos usuarios experimentados están acostumbrados al control con una sola mano, es una muy buena solución colocar una tecla de entrada, lo que requiere movimientos precisos del motor. Por lo tanto, el usuario puede colocar el terminal móvil en la mano entre las puntas de los dedos y la palma de la mano. El pulgar queda por tanto libre para entrar información. La tecla de desplazamiento 10 puede ser una tecla de rodillo (no mostrada), que se dispone para girar en una o varias direcciones. La tecla rotativa permite al usuario girar la tecla para desplazarse entre diferentes elementos en un menú. La techa rotativa 10 puede estar de acuerdo con la Solicitud de Patente de Estados Unidos 08/923.696 del Cesionario.

Además, la tecla de desplazamiento 10 permite al usuario desplazarse selectivamente entre un grupo de elementos en un menú. Esto significa que el usuario puede seleccionar un elemento anterior o posterior al elemento en el bucle de menú del teléfono, mientras que él/ella puede acceder a un bucle de submenú debajo del elemento correspondiente en el bucle de menú mediante la activación de la tecla de operación 8a.

En algunos estados, como entrar un número de teléfono en el teclado alfanumérico 7, la otra tecla programable 8b se puede definir como una tecla de borrar, que se puede usar para borrar el último dígito o letra introducida presionando brevemente la tecla de borrar 8b. Si la tecla de borrar 8b se presiona durante más tiempo, se borra todo el número o la palabra.

Aunque las funciones del terminal móvil 10 pueden controlarse mediante la tecla operativa 8a, a veces puede ser conveniente usar dos o más teclas programables operativas en el segundo grupo de teclas, que pueden introducirse en una pantalla táctil (no mostrada) de forma análoga a una pantalla de un asistente digital personal (PDA).

Las dos teclas de manejo de llamadas 9 se usan para establecer una llamada o una llamada de conferencia, finalizar una llamada o rechazar una llamada entrante.

La Figura 2 muestra esquemáticamente un diagrama de bloques de las partes principales del terminal móvil 1 de la Figura 1. Estas partes son convencionales y se usan normalmente en terminales móviles tales como aquellos en los que se puede poner en práctica la presente invención. El micrófono 6 graba la voz del usuario, y las señales analógicas formadas de este modo se convierten en AID en un convertidor A/D (no mostrado) antes de que la voz se codifique en una parte de audio 14. La señal de voz codificada se transfiere a un controlador que es un microprocesador programado 18 que ejecuta la programación para controlar el terminal móvil 1 de la Figura 1. El procesador 18 puede ejecutar diversos tipos de software para proporcionar una amplia variedad de funciones de terminal durante un modo activo que son bien conocidas. El procesador 18 forma también la interfaz con las unidades periféricas, que comprende un controlador LCD 13 que controla la pantalla LCD 3 de la Figura 1 para proporcionar pantallas gráficas al usuario, memoria RAM 17a y una memoria Flash ROM 17b, una tarjeta SIM 16 y el teclado 2 en forma, por ejemplo, sin limitación, de un teclado (así como datos, fuente de alimentación, etc.). El procesador 18 se comunica con un transmisor/receptor 19, que envía/recibe una solicitud/respuesta a/de una o varias redes de telecomunicaciones. La parte de audio 14 descifra la señal, que se transfiere desde el procesador 18 al altavoz 5, a través de un convertidor D/A (no mostrado).

Los usuarios de Internet utilizan navegadores web mundiales (WWW) para acceder a servicios de información en servidores WWW. Los navegadores WWW son programas que se ejecutan en el ordenador de un usuario. El ordenador del usuario puede ser móvil y estar conectado a Internet a través de un enlace inalámbrico o fijo y conectado a Internet a través de una conexión de cable. Un servidor WWW proporciona páginas a un navegador WWW. El servidor WWW almacena o genera la información que se muestra en las páginas y transmite la información al navegador WWW mediante una conexión o sesión de Internet.

Un servidor WWW puede tener un certificado emitido por un tercero confiable (TTP) también conocido como Agencia de certificados (CA) que, junto con una clave secreta, proporciona la identidad del servidor al usuario cliente del terminal fijo o móvil. El certificado contiene el nombre verificado del servidor u organización responsable del servidor.

Las páginas WWW pueden dividirse en marcos generados por diferentes servidores. Los marcos de diferentes servidores se combinan en una página integrada que se muestra en un terminal de usuario bajo el control del navegador WWW.

Es importante evitar que un servidor WWW se haga pasar por un verdadero servidor WWW. Cualquier suplantación podría permitir que el servidor de suplantación obtenga información secreta, confidencial o comercialmente sensible. Actualmente, los navegadores no permiten que la identidad de un servidor que proporciona páginas que contienen marcos integrados entre sí de diferentes servidores se indique a un usuario de forma práctica y fácil.

Actualmente, la identidad del servidor no se muestra a los usuarios en un navegador WWW a través de la interfaz de usuario (UI). En algunas circunstancias, es posible averiguar la identidad del servidor a través de comandos a través de la interfaz UI del navegador. La mayoría de los usuarios de un navegador no verifican la identidad del servidor al que se conecta el navegador porque dicha verificación de identidad no es fácil y, además, muchos usuarios ni siquiera se dan cuenta del problema potencial.

Cuando una página WWW contiene varios marcos, solo se puede ver el estado del primer marco en los navegadores actuales. Esto hace que sea imposible verificar la identidad de los servidores que proporcionan marcos que están integrados en una página usando un navegador.

La Figura 3A muestra una página de inicio de sesión genérica de un navegador WWW que muestra un solo marco 100. El contenido de información del marco 100 no es importante. El indicador 102 en la parte inferior del marco, que es un bloqueo o de otro tipo como el utilizado por el Netscape Navigator™, se utiliza para informar visualmente al usuario si la conexión se considera segura. Como se ilustra, el bloqueo está cerrado, lo que indica que para la única página 100 se indica que el servidor de origen no identificado es seguro. Sin embargo, para descubrir la verdadera identidad del servidor que proporciona el marco único 100, es necesario hacer clic en el indicador 102 para obtener además el certificado del servidor que proporciona el marco 100 que se muestra en la pantalla 104.

La Figura 3B ilustra una página de inicio de sesión 105 que se divide en dos marcos 106 y 108 que se proporcionan desde diferentes servidores. Su contenido no es importante. Los marcos 106 y 108 son proporcionados por diferentes servidores. El indicador de bloqueo 102, como resultado de estar desbloqueado, indica solamente que el marco izquierdo 106 es de un servidor no seguro. Sin embargo, el indicador 102 no transmite ninguna información con respecto al marco derecho 108. Sin embargo, si el marco 108 contiene información que es secreta, confidencial o comercialmente sensible, es crítico que el usuario del navegador sea informado de la identidad del servidor 108

como una que tiene una identidad reconocida para el usuario y es seguro para proporcionar al usuario un grado razonable de seguridad sobre el servidor al que el usuario puede suministrar información secreta, confidencial o comercialmente sensible. Sin embargo, no hay información disponible sobre el servidor que proporciona el marco 108, dejando al usuario en el dilema de continuar con las comunicaciones a través de Internet que involucran información secreta, confidencial o comercialmente sensible que se dirige a un servidor de autenticidad desconocida.

El indicador de seguridad 102 de la técnica anterior no proporciona, incluso cuando se indica seguridad, que una sesión de correo es segura, lo que puede inducir a error al usuario sobre la corrección de la seguridad y no proporciona información sobre el nivel real de seguridad o credibilidad de las fuentes de los marcos. El indicador de seguridad 102 de la técnica anterior puede indicar una seguridad débil sin autenticación que está sujeta a verse comprometida o una seguridad fuerte con autenticación. Las posibles interpretaciones diferentes del indicador 102 hacen que el indicador sea de poco valor para un usuario interesado.

Divulgación de la invención

De acuerdo con varios, pero no necesariamente todos, ejemplos de la divulgación allí se proporciona un método, un programa informático y un aparato de acuerdo con las reivindicaciones adjuntas.

Los ejemplos de la presente divulgación se refieren a un sistema y método que (1) permite a un usuario del terminal que puede ser móvil o fijo, que está acoplado a una red como, pero sin limitarse a Internet, determinar al menos una operación de comunicación y preferentemente todas las operaciones de comunicación asociadas a una sesión de terminal a través de una visualización en la pantalla del terminal de un nivel de confianza de la una o más operaciones de comunicación con respecto a un estándar antes de su transmisión a la red informando al usuario de un nivel de seguridad determinado a asociarse a las operaciones de comunicación) permitida por el usuario para transmitirse a la red, y (2) cuando la pantalla en el terminal contiene múltiples marcos, que la fuente de todos los marcos, que puede ser de múltiples servidores de aplicaciones, se certifique para el usuario como una fuente segura en la que el usuario puede confiar para transmitir información secreta, confidencial o comercial las mismas sin preocuparse por la seguridad del mismo.

La visualización de un nivel de confianza en el dispositivo terminal, que puede ser móvil o fijo y conectado a la red a través de conectividad alámbrica o inalámbrica, informa al usuario de un nivel relativo de seguridad que se determina que está asociado a cada operación de comunicación de un terminal sesión para permitir al usuario elegir si desea continuar con las operaciones de comunicación de la sesión en función del nivel de confianza mostrado. La determinación del nivel de confianza se puede determinar (1) únicamente en el terminal móvil a través de la información almacenada en el terminal móvil al momento de la fabricación o descargada posteriormente, (2) únicamente desde al menos un servidor en una red a la que las operaciones de comunicación se transmitirán antes de la transmisión real de la misma a la red para obtener un nivel de evaluación de confianza de la misma, o (3) compartiendo la determinación del nivel de confianza entre al menos un servidor de red y un procesador en el terminal. Se pueden poner en práctica ejemplos con igual facilidad, independientemente de en qué parte del sistema se determine el nivel de confianza.

Se pueden utilizar diversos factores para determinar el nivel de confianza que se muestra. Un primer atributo del nivel de determinación de confianza depende de la tecnología utilizada durante la operación de comunicación entre el terminal y la red. El componente tecnológico es de naturaleza dinámica, puesto que con el paso del tiempo, las tecnologías que inicialmente pueden ser altamente seguras y tienen un alto nivel de seguridad asociado a ellas pueden, debido a la llegada de tecnologías más nuevas, volverse relativamente menos seguras en relación con el estado de la técnica. El nivel de confianza resultante en esta situación debería reducirse aunque la misma tecnología se utilice continuamente. Por ejemplo, sin limitación, el componente tecnológico puede pertenecer a (1) cifrado utilizado durante la transmisión de las operaciones de comunicación entre el terminal y varias entidades en la red, (2) cómo se inicia la sesión, (3) cómo se consigue el almacenamiento en el terminal, y (4) cómo el usuario del terminal realiza la identificación del usuario.

Además, más allá de los atributos tecnológicos mencionados anteriormente del terminal y la red, se pueden utilizar atributos no tecnológicos para determinar el nivel de confianza, tales como, pero sin limitación, la confiabilidad del operador del servidor de aplicaciones al que se conecta el terminal durante la sesión y la viabilidad comercial de cualquier oferta comercial realizada por el operador del servidor de aplicaciones o de otra manera de una fuente de los bienes o servicios adquiridos, etc.

La visualización del nivel de confianza por parte del terminal puede ser, sin limitación, numérica o gráfica. Independientemente del tipo de pantalla, la pantalla es relativa a un estándar de referencia, de modo que una cantidad numérica más grande representa un mayor nivel de confianza o una mayor representación gráfica, como por ejemplo, un número de barras de cero a cuatro con cuatro ser el mejor proporciona al usuario información suficiente para que el usuario pueda hacer una elección inteligente de autorizar la operación de comunicación que se realizará con la red. Si bien la elección final de continuar con una sesión que contiene múltiples operaciones de comunicación que dependen de la visualización del nivel de confianza es la elección del usuario, la visualización de la presente invención del nivel relativo de confianza permite al usuario tomar decisiones inteligentes sobre si

transmitir en una operación de comunicación secreta, confidencial o información comercial a la red.

Numerosos factores de ponderación diferentes pueden estar asociados a los atributos tecnológicos y no tecnológicos utilizados para determinar el nivel de confianza. La presente invención no se limita a ninguna elección particular de atributos usados para determinar el nivel de confianza tanto desde la perspectiva tecnológica como no tecnológica. Además, como se ha indicado anteriormente, la presente invención facilita una evaluación actual del nivel de confianza que se hará dependiente del cambio en los atributos tecnológicos y no tecnológicos a lo largo del tiempo para dar al usuario del terminal durante cualquier sesión actual el máximo hasta la fecha, información relacionada con el nivel de confianza.

El nivel de confianza puede calcularse utilizando un algoritmo basándose en números que suma diferentes componentes de los atributos que se ponderan para determinar la puntuación general que representa una operación de comunicación que se evalúa antes de la transmisión a la red. Un algoritmo basándose en números puede actualizarse fácilmente para reflejar el cambio en la contribución de varios atributos que proporcionan componentes numéricos de la posible puntuación perfecta.

Además, los ejemplos proporcionan la visualización de una sola página que contiene marcos de múltiples servidores con un indicador de si los marcos están certificados como transmitidos desde servidores que son seguros. El terminal muestra una certificación u otra indicación para informar al usuario de si cada página que contiene múltiples marcos proviene del servidor verificado y cada marco proviene de una fuente segura.

En un sistema que comprende un terminal, que incluye una pantalla y una red, el terminal que usa un navegador para comunicarse con una red durante una sesión de terminal que comprende operaciones de comunicación iniciadas por un usuario y transmitidas a la red, un método de acuerdo con ejemplos incluye iniciar un sesión terminal con el navegador haciendo una transmisión a la red; la red, en respuesta al inicio de la sesión del terminal, proporciona información de la red al navegador relacionada con la sesión del terminal; y mostrar en la pantalla un nivel de confianza basándose en un estándar de comparación de al menos una operación de comunicación antes de la transmisión a la red, informando al usuario de un nivel de seguridad determinado como asociado a la al menos una operación de comunicación si el usuario permite que al menos una operación de comunicación se transmita a la red. El terminal puede ser un terminal móvil; y las operaciones de comunicación pueden comprender transmisiones inalámbricas entre el terminal móvil y una entidad en la red. Se puede mostrar un nivel de confianza de cada una de las operaciones de comunicación; y en el que cada nivel de confianza puede basarse, al menos en parte, en la tecnología de la red que participa en la operación de comunicación asociada al nivel de confianza mostrado. La red puede comprender un servidor que determina un nivel de confianza de las operaciones de comunicación; y el nivel de confianza determinado por el servidor puede transmitirse al terminal y mostrarse en la pantalla del mismo. El terminal móvil puede comprender un procesador; y en respuesta a cada operación de comunicación, el procesador puede determinar un nivel de confianza que se muestra en la pantalla. La red puede comprender un servidor y el terminal puede comprender un procesador; y el servidor puede proporcionar información sobre el procesamiento de las operaciones de comunicación por la red al procesador y el procesador en respuesta a la información puede determinar el nivel de confianza que se muestra en la pantalla. El servidor puede determinar un nivel de confianza de cada una de las operaciones de comunicación basándose al menos en parte en la tecnología de la red asociada a la red que proporciona cada operación de comunicación. El nivel de confianza también puede depender, al menos en parte, de al menos un atributo de adición que la red utiliza para procesar la operación de comunicación. El al menos un atributo adicional puede ser al menos uno de confiabilidad de un operador de un servidor que ofrece un servicio durante la sesión a través del navegador al usuario (o mediante la aplicación de otros medios de comunicación, como correo electrónico o SMS) o viabilidad comercial de una oferta de servicio hecha al usuario durante la sesión a través del navegador u otra conexión de red utilizada. La visualización del nivel de confianza puede ser una presentación gráfica o un valor numérico.

Un sistema de acuerdo con ejemplos incluye un terminal que incluye una pantalla; una red a la que se conecta el terminal a través de un enlace de comunicación; y en el que el terminal usa un navegador o correo electrónico o SMS para comunicarse con la red durante una sesión de terminal que comprende operaciones de comunicación iniciadas por el usuario y transmitidas a la red con la sesión del terminal iniciada con el navegador, correo electrónico o SMS haciendo una transmisión a la red, la red, en respuesta al inicio de la sesión del terminal, proporciona información de la red al navegador, correo electrónico o SMS relacionada con la sesión del terminal, y la pantalla muestra un nivel de confianza basándose en un estándar de comparación de al menos una operación de comunicación antes de la transmisión a la red, informando al usuario de un nivel de seguridad determinado que está asociado a la al menos una operación de comunicación si el usuario permite que la operación de comunicación al menos se transmita a la red. Se puede mostrar un nivel de confianza de cada una de las operaciones de comunicación; y en el que cada nivel de confianza se basa, al menos en parte, en la tecnología de la red que participa en la operación de comunicación asociada al nivel de confianza mostrado. La red puede comprender un servidor que determina un nivel de confianza de las operaciones de comunicación; y el nivel de confianza determinado por el servidor puede transmitirse al terminal y mostrarse en la pantalla del mismo. El terminal móvil puede comprender un procesador; y en respuesta a cada operación de comunicación, el procesador puede determinar un nivel de confianza que se muestra en la pantalla. La red puede comprender un servidor y el terminal puede comprender un procesador; y el servidor puede proporcionar información sobre el procesamiento de las

operaciones de comunicación por la red al procesador y el procesador en respuesta a la información puede determinar el nivel de confianza que se muestra en la pantalla. El servidor puede determinar un nivel de confianza de cada una de las operaciones de comunicación basándose al menos en parte en la tecnología de la red asociada a la red que proporciona cada operación de comunicación. El nivel de confianza también puede depender, al menos en parte, de al menos un atributo de adición que la red utiliza para procesar la operación de comunicación. El al menos un atributo adicional puede ser al menos uno de confiabilidad de un operador de un servidor que ofrece un servicio durante la sesión a través del navegador, correo electrónico o SMS al usuario o viabilidad comercial de una oferta de servicio hecha al usuario durante la sesión a través del navegador. La visualización del nivel de confianza puede ser una presentación gráfica o un valor numérico.

Un sistema de acuerdo con los ejemplos comprende un terminal que incluye una pantalla; una red que incluye un servidor al que el terminal está acoplado por un enlace de telecomunicaciones; y en el que el servidor almacena un certificado emitido por un tercero de confianza, como CA que contiene una identidad verificada del servidor o una organización responsable del servidor y una clave secreta, la clave secreta y el certificado, que se transmiten al terminal y se procesan por el terminal para determinar si la identificación del servidor puede mostrarse a un usuario del terminal como si fuera de una fuente confiable, la pantalla que contiene al menos una página que contiene marcos y una pantalla que muestra si los marcos están certificados como de una fuente confiable. El sistema puede incluir además al menos un servidor adicional, el al menos un servidor adicional proporciona al menos un marco al servidor; y el servidor puede procesar el al menos un marco del servidor adicional y cualquier marco proporcionado por el servidor para formar una página integrada que contiene los marcos que se transmiten al terminal y se muestran en la pantalla. La página integrada puede mostrarse con el certificado del servidor que indica que la página integrada proviene de una fuente confiable.

Un método en un sistema que comprende un terminal que incluye una pantalla, una red que incluye un servidor al que el terminal está acoplado por un enlace de telecomunicaciones de acuerdo con ejemplos que incluyen almacenar con el servidor un certificado emitido por un tercero confiable, como CA, que contiene una identidad verificada del servidor o una organización responsable del servidor y una clave secreta; transmitir el certificado y la clave secreta al terminal; y procesar en el terminal el certificado y la clave para determinar si la identidad del servidor puede mostrarse al usuario del terminal como una fuente confiable; y mostrar con los resultados de visualización del procesamiento. La red puede comprender al menos un servidor adicional; el al menos un servidor adicional puede proporcionar al menos una página al servidor; y el servidor puede procesar al menos una página del servidor adicional y cualquier página proporcionada por el servidor para formar una página integrada que se transmite al terminal y se muestra en la pantalla. La página integrada puede mostrarse con el certificado del servidor que indica que la página integrada proviene de una fuente confiable.

Breve descripción de los dibujos

La Figura 1 ilustra un terminal móvil de la técnica anterior que es un tipo de terminal que puede usarse con la práctica de la presente invención.

La Figura 2 ilustra un diagrama de bloques de la electrónica del terminal móvil de la técnica anterior de la Figura 1.

Las Figuras 3A y 3B ilustran las pantallas de inicio de sesión del navegador de la técnica anterior.

Las Figuras 4A-4E ilustran una visualización de un indicador de nivel de confianza de acuerdo con la presente invención.

La Figura 5 ilustra un diagrama de sistema de un sistema de acuerdo con la invención que genera una visualización del nivel de confianza utilizado para informar al usuario del nivel de seguridad de la operación de comunicación y que las páginas mostradas que contienen múltiples marcos son de servidores seguros.

La Figura 6 ilustra un diagrama de flujo del procesamiento de operaciones de comunicación individuales por un servidor de evaluación de confianza en el sistema de la Figura 5.

La Figura 7 ilustra una pantalla de inicio de sesión del navegador visualizada de acuerdo con la presente invención.

Los números de referencia similares identifican partes similares en todos los dibujos.

Mejor modo para realizar la invención

Las Figuras 4A y 4B ilustran una pantalla en un dispositivo terminal de un nivel de confianza de acuerdo con la presente invención. El nivel de confianza es relativo a un estándar de comparación, de modo que la visualización del nivel de confianza en asociación a la una o más operaciones de comunicación antes de su transmisión a una red informa al usuario de un nivel de seguridad que se determina que está asociado al mismo en relación con otras operaciones de comunicación. La visualización del nivel de confianza permite al usuario elegir si una operación de comunicación se transmite a la red después de que el usuario haya considerado el nivel potencial de riesgo de transmitir información secreta, confidencial o comercialmente sensible con la operación de comunicación. La red a la que se transmiten las operaciones de comunicación es parte del sistema de la Figura 5 como se describe a continuación. Las pantallas 100 y 102 pueden producirse por la pantalla LCD 3 del terminal de la técnica anterior de la Figura 1 o pueden producirse por una pantalla de un dispositivo terminal, como una PC. Como se ilustra, la

pantalla es físicamente similar a la producida por el terminal móvil de la técnica anterior de la Figura 1, pero la invención no está limitada a los mismos.

Las pantallas 100 y 102 representan respectivamente la primera y segunda operaciones de comunicación de una sesión de terminal. Con la invención, antes de comunicarse realmente con la red con una operación de comunicación, se produce una pantalla 104, que puede ser gráfica como se ilustra, numérica, textual o cualquier combinación de las mismas, en cada una de las pantallas 100 y 102 asociadas a las diferentes operaciones de comunicación. Cuando la sesión de terminal continúa con la primera operación, el bloque 110 en la Figura 4A, que se identifica por el texto "Tipo de tarjeta", se resalta con un campo contenido dentro de una ventana rectangular como se ilustra. El resaltado del "Tipo de tarjeta" le dice al usuario que la primera comunicación de la sesión del terminal está activa y si el nivel de confianza mostrado es aceptable, el usuario debe ingresar el "Tipo de tarjeta" del usuario.

Cuando la sesión de terminal continúa con la primera operación de comunicación 110 solicitando al usuario que ingrese el "Tipo de tarjeta", se envía una comunicación a la red, como se describe a continuación, a un servidor de evaluación de confianza en su interior o el terminal determina el nivel de confianza o se utiliza una combinación del servidor de evaluación de confianza y el terminal. De acuerdo con la información almacenada dentro de la RAM 17A de un terminal móvil de la técnica anterior u otra memoria, como la RAM en una PC, la determinación del nivel de confianza que se asociará a la primera operación de comunicación se realiza antes de que la primera operación de comunicación sea permitida por el usuario que se transmitirá a la red. Como se ha indicado, la pantalla 104 de la Figura 4A muestra dos barras 112 que indican que se ha determinado que un nivel intermedio de seguridad está asociado a la operación de comunicación inicial por el procesador 18 del terminal móvil de las Figuras 1 y 2 ejecutando programación en su interior o, como alternativa, el servidor de evaluación de confianza, como se describe a continuación en asociación con la Figura 5, o una distribución de la determinación del nivel de confianza entre el procesador del terminal móvil y el servidor de evaluación de confianza de la red. La visualización de dos barras 112 le dice al usuario que hay un nivel intermedio de seguridad asociado a la transmisión del "Tipo de tarjeta" a la red, por ejemplo, la identificación de la tarjeta bancaria o del emisor de la tarjeta de viaje y entretenimiento.

En la Figura 4B, el campo 114 asociado al segundo número de tarjeta de operación de comunicación se resalta indicando que la segunda operación de comunicación de la sesión está activa. Al momento de la entrada de la segunda operación de comunicación de la sesión del terminal, la información más sensible del "Número de tarjeta" se transmitirá a la red. El nivel de confianza de la segunda comunicación se determina de la misma manera que la primera operación de comunicación. El nivel determinado de confianza se visualiza como tres barras 112 que indican que hay un mayor nivel de seguridad asociado a la segunda operación de comunicación.

Las operaciones de comunicación "Nombre" y "Dirección" se procesan de manera similar. Si el usuario continúa con las operaciones de comunicación tercera y cuarta asociadas al "Nombre" y la "Dirección" de las Figuras 4A y 4B, cada operación de comunicación de la sesión tendrá, antes de la transmisión a la red, un nivel de confianza mostrado.

Además, debe entenderse que la sesión como se muestra en las Figuras 4A y 4B, es solo un ejemplo de la presente invención. La invención es igualmente aplicable a sesiones que involucran diferentes números y tipos de operaciones de comunicación. Además, aunque la sesión mostrada es de naturaleza comercial y está asociada a la compra de bienes o servicios, las sesiones de acuerdo con la presente invención tienen diversas aplicaciones.

El beneficio del nivel de confianza mostrado para el usuario es varias veces mayor. Primero, la visualización de un nivel de confianza indicado que tiene al menos una barra informa al usuario que hay cierto nivel de seguridad asociado a la operación de comunicación que proporciona un grado limitado de seguridad de que la seguridad está en su lugar. Además, de acuerdo con el nivel de experiencia del usuario de lo que él o ella considera sensible, la pantalla proporciona una cuantificación del nivel de seguridad, ya sea numérica o gráficamente (la cuantificación numérica no se ha ilustrado), lo que permite al usuario evaluar el nivel real de confianza asociada a cada parte de la sesión con un marco de referencia común como se ilustra en las Figuras 4C-4E. En la Figura 4C, el área de sección más a la izquierda 120 de la pantalla del área central (la mitad del ancho de la pantalla) es el marco seleccionado de los dos marcos disponibles 118 y 119. Se indica que el marco 118 seleccionado es el seleccionado con un marco 120 cuadrado. El nivel de confianza determinado se muestra como dos barras 123. En la Figura 4D, el área de sección más a la derecha 130 en el área central de la pantalla es el marco seleccionado de los dos marcos disponibles 128 y 129. Se indica que el marco 129 seleccionado se selecciona con un marco 130 cuadrado. El nivel de confianza determinado se muestra como tres barras 132. En la Figura 4E, la pantalla del usuario incluye dos áreas de marco 138 y 139 en el medio de la pantalla. En el área de marco más a la izquierda 138 hay una sección que es un llamado applet 140 de JAVA. El área de applet 140 ahora se selecciona con el marco de selección 144. El nivel de confianza del applet 144 se muestra como una barra 142. La consideración de al menos una y preferentemente todas las operaciones de comunicación de una sesión permite que la sesión se detenga si el usuario determina que el nivel de confianza mostrado es inaceptablemente bajo con respecto a lo que el usuario considera importante con respecto a la publicación de información solicitada a la red.

El nivel de confianza mostrado es relativo a un estándar de comparación. Las operaciones de comunicación durante

una sesión se evaluarán en relación con el mismo estándar. El nivel de confianza sintético mostrado, ya sea texto gráfico, numérico o alguna combinación de los mismos o texto, le dice al usuario cómo se compara la seguridad de la operación de comunicaciones en particular con respecto a otras operaciones de comunicación. El indicador de nivel de confianza que se muestra, que se determina como se describe a continuación teniendo en cuenta los atributos técnicos y no técnicos de la sesión, permite al usuario colocar en cada operación de comunicación un nivel de confianza al poder ver visualmente el nivel de confianza antes de la transmisión de cada operación de comunicación a la red.

Hay dos metodologías preferidas para determinar el nivel de confianza mostrado. La primera metodología es almacenar en la memoria del procesador asociado al dispositivo terminal el algoritmo de determinación del nivel de confianza que puede ser si el dispositivo terminal es móvil, la RAM 17A asociada al procesador 18 de las Figuras 1 y 2 o en la memoria de una PC si el dispositivo terminal está conectado a la red a través de un cable. La información almacenada contenida en la memoria del dispositivo terminal se usa para analizar al menos los atributos técnicos preferentemente de cada una de las operaciones de comunicación de la sesión actual para determinar el nivel de confianza que se mostrará. Una base para hacer esto es comparar la tecnología utilizada por el dispositivo terminal y la red asociada a la sesión con el estado actual de las tecnologías de terminal y red almacenadas en la memoria, incluida la descarga periódica para actualizar la memoria con las tecnologías actuales. Por ejemplo, si el usuario estuviera a punto de almacenar detalles de la transacción en el terminal, se le pueden presentar opciones de almacenamiento en la memoria del terminal o en el módulo SIM en la Figura 1. En vista de que SIM representa un almacenamiento seguro actual de última generación, mientras que RAM no lo hace, el nivel de confianza para el almacenamiento en SIM se mostrará como más alto. Además, si un usuario va a realizar una conexión cifrada como parte de una operación de comunicación con un servidor remoto en la red, el dispositivo terminal hará que se muestre un mayor nivel de seguridad en vista de que la terminal identifica la operación de comunicación como estar cifrado, lo que se entiende como un mayor nivel de seguridad.

Los ejemplos anteriores de atributos tecnológicos del terminal móvil son solo ejemplos de otros atributos de la tecnología que pueden almacenarse como representativos del estado de la técnica. La información almacenada, incluido el algoritmo, representa el marco de comparación para generar la visualización del nivel de confianza.

La determinación del nivel de confianza por parte del terminal tiene algunas desventajas. En la medida en que el material almacenado en la memoria del dispositivo terminal no se actualice continuamente desde la red, los efectos del cambio tecnológico y las relaciones de la vida real pueden alterar la importancia de un nivel de confianza mostrado con el tiempo. A medida que avanza la tecnología, la SIM puede romperse y dejar de representar la mejor solución para el almacenamiento seguro local. Sin embargo, a menos que la información almacenada en la memoria del terminal se actualice con respecto a SIM, el usuario tiene una pantalla de mayor nivel de confianza que el presente en el futuro cuando SIM puede ser una forma menos segura para almacenar información de forma segura en el terminal en comparación con posibles nuevas tecnologías. Además, la información de la vida real que existe sobre una sesión con un servidor en particular puede ser inconsistente con el nivel de seguridad mostrado, como cuando el terminal determina que se ha realizado una conexión autenticada segura pero, de hecho, dicha conexión resulta ser en un entorno totalmente no seguro. Por supuesto, factores como los anteriores, aunque son posibles, son relativamente improbables. La información proporcionada por la visualización del nivel de confianza de acuerdo con la invención es más fina que la técnica anterior que no proporciona dicha información. En gran medida, incluso con la posibilidad de error, el nivel de confianza será mucho más confiable incluso cuando la memoria del terminal no se actualice para reflejar la ponderación de estas circunstancias en la determinación del nivel de confianza.

El indicador visualizado de nivel de confianza 104, ya sea gráfico, numérico o de otro tipo, tal como con un mensaje de texto o una combinación de los mismos, se genera de la misma manera que se generan otras comunicaciones en dispositivos de visualización para terminales. Para un navegador de Internet, el indicador 104 podría colocarse en la barra de estado.

La Figura 5 ilustra un sistema 200 en el que se puede poner en práctica la presente invención. Este sistema comprende un terminal 202, que puede ser un terminal móvil de acuerdo con la técnica anterior de las Figuras 1 y 2, o un terminal fijo que puede ser también una PC y una red 204. El terminal 202 tiene una pantalla 206 que muestra las pantallas mencionadas anteriormente de las Figuras 4A-4E y otras pantallas para proporcionar al usuario información sobre la sesión de terminal y, específicamente, al menos el nivel de indicador de confianza 124 o equivalente. El terminal 202 está conectado por un enlace de comunicaciones 208, que puede ser inalámbrico o fijo, a un servidor de evaluación de confianza 210. El nivel de confianza puede ser determinado también por un servidor en la red 204, tal como el servidor de evaluación de confianza 210 o mediante las operaciones combinadas de los procesadores en el terminal 202 y en el servidor de evaluación de confianza.

La red 204 incluye una pluralidad de servidores de aplicaciones 212 que son bien conocidos y son representativos de cualquier fuente de información a la que se conecta el terminal 202 durante una sesión de operaciones de comunicación. La conectividad entre el terminal móvil 202 y cada uno de los servidores de aplicaciones 212 puede ser a través de cualquier tipo de red, incluida una red de paquetes de datos 214 tal como, entre otros, Internet. Los servidores de aplicaciones 212 generalmente están controlados por organizaciones. La identidad de las organizaciones es uno de los atributos que pueden tenerse en cuenta durante la determinación del nivel de

confianza determinado únicamente por el procesador del terminal 202, únicamente por el procesador del servidor de evaluación de confianza 210 o una combinación de los mismos en la que cada procesador comparte parte de la tarea de determinación del nivel de confianza. Además, el servidor de evaluación de confianza 210 está conectado a servidores adicionales que son, sin limitación, el servidor de vigilancia tecnológica 218, el servidor emisor de certificados 220 y el servidor de análisis de mercado 222, que proporcionan un análisis de diferentes atributos que se ponderan y/o se consideran para determinar el nivel de confianza por el servidor de evaluación de confianza 210.

La operación de comunicación representada en la Figura 5 es una operación de comunicación "ir y comprar" 224. Se produce una serie de procesamientos en respuesta a la operación de comunicación "ir y comprar" 224 como sigue. La entrada inicial de una operación de comunicación "ir y comprar" 224, como se resalta o se identifica de otro modo en la pantalla, tal como la descrita anteriormente junto con las Figuras 4A-4E hace que se transmita una comunicación 226 desde el terminal móvil 202 al servidor de evaluación de confianza 210. En este punto, el servidor de evaluación de confianza 210 inicia un análisis que considera los atributos tecnológicos de la sesión de terminal y los atributos no tecnológicos. El servidor 210 de evaluación de confianza inicia una comunicación 228 con el servidor 218 de vigilancia tecnológica que solicita una evaluación de si el cifrado 230 de 128 bits que se utilizará en la operación 224 "ir y comprar" representa la tecnología más avanzada. El servidor de vigilancia tecnológica 218, que contiene una base de datos que se actualiza para reflejar las tecnologías utilizadas más actuales, incluida la que implica cifrado, etc., analiza el cifrado 230 de 128 bits y envía un mensaje 230 de estado en la comunicación 232 de nuevo a el servidor de evaluación de confianza 210. El servidor de evaluación de confianza 210 envía después una comunicación 234 que solicita al servidor de emisión de certificados 220 para determinar si el certificado "ABC" que se incluirá en la operación de comunicación "ir y comprar" 224 es auténtico. El servidor emisor de certificados 220 determina que el certificado caducará en una semana como se indica en el mensaje 237 y, por lo tanto, es actualmente auténtico. El servidor de evaluación de confianza 210 envía después la comunicación 238 indicando que el mensaje "ir y comprar" se indica en el mensaje 239 se dirigirá a la empresa "XYZ" y supondría $ 200 dólares estadounidenses. El servidor de análisis de mercado 222 envía una comunicación 240 al servidor de evaluación de confianza 210 que contiene el mensaje 241 de que la compañía "XYZ" tiene una mala reputación. En este momento, el servidor de evaluación de confianza 210 ha considerado la información tecnológica relativa al estado de la técnica proporcionada por el servidor de vigilancia tecnológica 218 y la información no tecnológica. El servidor del emisor del certificado 220 indica la información no tecnológica para determinar si el certificado proporcionado por la operación 224 de "ir y comprar" es actual y la información de análisis de mercado referente a la compañía a que se dirige la transacción se indica por el servidor de análisis de mercado 222.

La combinación de información tecnológica y no tecnológica, que es solo un posible subconjunto de información que puede ser utilizada por el servidor de evaluación de confianza 210 para determinar el nivel de confianza, es procesada por los procesadores dentro del servidor de evaluación de confianza 210 en de acuerdo con los criterios programados utilizados para generar parcial o totalmente el nivel de confianza que se mostrará por la pantalla 206 del terminal 202. Después de realizar el procesamiento de todos los atributos disponibles, tanto de naturaleza tecnológica como no tecnológica reunidos por el servidor de evaluación de confianza 210, la comunicación 242 es transmitida por el servidor de evaluación de confianza 210 de regreso al dispositivo terminal 202. Como se ilustra en 244, la comunicación 242 incluye el mensaje 244 de que la operación "ir y comprar" 224 se manejará con tecnología aceptable pero que la empresa a la que se dirige la transacción tiene una operación cuestionable con un nivel de confianza resultante del 70 % con el nivel de confianza que se mostrará en un 70 %, el componente tecnológico de la transacción utilizada en la red 204 es aceptable, pero el usuario del dispositivo terminal 202 debe tener cuidado porque inferencialmente la compañía a la que se dirigirá la transacción tiene un mala reputación. Por supuesto, si el certificado 235 no era válido, la indicación en la comunicación 242 sería que la operación de comunicación "ir y comprar" no debería iniciarse porque el servidor de aplicaciones 212 de la compañía XYZ (no ilustrado) no está asociado a un certificado emitido por un tercero confiable que es extremadamente importante para informar al usuario del dispositivo terminal 202 que el usuario no está tratando con un servidor autenticado asociado a la compañía XYZ.

La Figura 6 ilustra un diagrama de flujo de una posible operación del servidor de evaluación de confianza 210 al analizar las operaciones de comunicación para determinar el nivel de confianza del mismo que se mostrará por la pantalla 206 del terminal 202. El procesamiento del servidor de evaluación de confianza 210 comienza en el punto 300 en el que la operación de comunicación a evaluar es un mensaje recibido desde el terminal 202 en el servidor de evaluación de confianza 210. El procesamiento continúa hasta el punto 302 en el que el mensaje recibido extrae la operación que se va a evaluar para mostrar un nivel de confianza, por ejemplo, las operaciones de comunicación "Tipo de tarjeta" o "Número de tarjeta" 110 y 114 de las Figuras 4A-4E. El procesamiento pasa al punto 304, en el que se determina si la "Identidad" y el "Modelo" del terminal 202 están enumerados en el mensaje. Si la respuesta es "sí", el procesamiento pasa al punto 306 en el que se extrae la información sobre la tecnología utilizada por el terminal. El procesamiento procede al punto 308 desde el punto 304 o el punto 306 en el que se realiza una determinación de los atributos tecnológicos requeridos de la red 204 utilizados para la operación de comunicación. El procesamiento pasa al punto 310 en el que se realiza una determinación si se han evaluado todos los atributos de la información en el mensaje recibido del terminal. Si la respuesta es "no" en el punto 310, el procesamiento pasa al punto 312 para evaluar el siguiente atributo del mensaje proporcionado por el terminal que se repite hasta que se hayan evaluado todos los atributos. Si la respuesta es "sí" en el punto 310, el procesamiento pasa directamente al punto 314 en el que se asigna un valor por defecto para cualquier atributo faltante utilizado como parte de los

criterios para determinar el nivel de confianza.

Los valores predeterminados se eligen para representar una contribución promedio de cada atributo faltante para no reducir erróneamente el nivel de confianza calculado al mínimo. Una vez que se determina que un atributo es parte del procesamiento utilizado para determinar un nivel de seguridad, el mecanismo de valor por defecto se utiliza para permitir que se calcule un nivel de confianza en ausencia de valores numéricos o que de otro modo se proporcione para cada uno de los atributos. Es mejor suponer, en ausencia de cualquier información, que el atributo tiene un valor promedio que no tiene ningún valor.

El procesamiento continúa hasta el punto 316 después de que todos los atributos tienen valores asociados al mismo para calcular la evaluación final del nivel de confianza que normalmente es numérico pero no está limitado a que el dispositivo terminal 202 lo muestre si el servidor de evaluación de confianza 210 es la única fuente del nivel de confianza mostrado. El procesamiento finalmente pasa al punto 318 que representa la comunicación 242 de regreso al terminal 202.

Debe entenderse que el procesamiento anterior realizado por el servidor de evaluación de confianza 210 es meramente ilustrativo. La modificación del procesamiento puede hacerse para incluir diferentes secuencias de procesamiento, incluyendo no calcular el nivel de confianza en el caso de que la sobrecarga de procesamiento sea compartida por el uno o más procesadores dentro del servidor de evaluación de confianza y los procesadores) dentro del dispositivo terminal 202.

El servidor de evaluación de confianza 210 suele ser una entidad diferente a los servidores de aplicaciones 212 que proporcionan al usuario del terminal 210 aplicaciones a las que se accede durante la sesión. Si bien es posible que el servidor de evaluación de confianza 210 y los servidores de aplicaciones 212 sean un solo servidor, es más probable que se utilice la arquitectura ilustrada de un servidor de evaluación de confianza 210 y los servidores de aplicaciones 212.

El servidor de evaluación de confianza 210 puede implementar cualquier metodología de evaluación de confianza para calcular total o parcialmente el nivel de confianza siempre que sea compatible con el funcionamiento del terminal 202. Se puede suponer que el servidor de evaluación de confianza 210 al menos tiene en cuenta los atributos tecnológicos de la operación de comunicación que son específicos del contexto de la operación de comunicación con otra información como se ha explicado anteriormente que también se usa.

Se pueden tener en cuenta muchos atributos de la tecnología utilizada tanto por el terminal 202 como por el servidor de evaluación de confianza 210. Estos atributos tecnológicos incluyen cifrado, inicio de sesión, almacenamiento local e identificación.

La evaluación de confianza global puede ser realizada únicamente por el terminal 202, únicamente por el servidor de evaluación de confianza 210, o una combinación de los mismos. Los atributos tecnológicos evalúan la idoneidad de la tecnología para la operación general prevista. Lo que es aceptable para algunas operaciones de comunicación como seguro puede no ser lo suficientemente seguro para otras operaciones de comunicación para que el usuario permita que la red realice la operación de comunicación.

Una lista de la seguridad relativa de las tecnologías de cifrado, desde las más seguras hasta las inseguras, puede ser la siguiente: operación dentro del terminal, Estándar de cifrado triple de datos (3DES), RC5 128 bit, RC5 56 bit (RC5 128 bit y RC5 56 bit siendo formas de cifrado RAS) y sin cifrado.

Una lista relativa de tecnologías de inicio de sesión de la más segura a la menos segura puede ser la siguiente: operación dentro de la terminal, certificados digitales autenticados por el servidor (el certificado debe evaluarse para asegurarse de que sea válido), secreto compartido autenticado por el servidor, autenticado por el servidor, red dirección y anonimato.

Una lista relativa de tecnologías de almacenamiento local, desde la más segura hasta la menos segura, es la siguiente: cifrado de software a prueba de manipulaciones, basándose en hardware, sin cifrado, memoria simple.

Una lista relativa de tecnologías de identificación, desde la más segura hasta la menos segura, puede ser la siguiente: biometría, huella digital, imagen del iris del ojo, etc., número de identificación personal (PIN) y ninguno.

Debe entenderse que el cifrado, el inicio de sesión, el almacenamiento local y la identificación no incluyen todos los atributos tecnológicos posibles del terminal 202 y la red 204 que pueden evaluarse en la determinación del nivel de confianza. Además, los listados relativos mencionados anteriormente de las tecnologías más seguras a las tecnologías menos seguras están sujetos a cambios y aumentos dependiendo de las nuevas tecnologías candidatas disponibles.

Además, la ponderación relativa de los diferentes atributos en función de consideraciones tecnológicas y no tecnológicas, por ejemplo, la información del servidor de vigilancia tecnológica 218 frente a la información del

servidor de análisis de mercado 210 está sujeta a diferentes implementaciones que darán lugar a diferentes niveles de confianza dependiendo de cuán diferente los atributos se ponderan dentro de la determinación y/o cálculo del nivel de confianza. Son posibles diferentes metodologías para calcular el nivel de confianza y la ponderación de los atributos.

La visualización del nivel de confianza, independientemente de cómo se genere, representa información que es muy útil para el usuario de un terminal en una sesión de operaciones de comunicación con uno o más servidores de destino en una red. El usuario evalúa si las operaciones de comunicación dentro de la sesión representan un riesgo indebido por el que es deseable finalizar la sesión. Además, la visualización del nivel de confianza proporciona al usuario un nivel de confianza de que la sesión general no expondrá la información del usuario ingresada durante la sesión a un riesgo aceptable de divulgación.

Además, aunque la determinación del nivel de confianza únicamente por el terminal 202 es más simple, tiene menos flexibilidad que la utilización del servidor de evaluación de confianza 210. Esta diferencia es el resultado de más información disponible a través del servidor de evaluación de confianza de la que está disponible a través del procesador o procesadores del dispositivo terminal 202.

Los atributos no tecnológicos que pueden sobre-ponderarse o considerarse en la determinación del nivel de confianza del servidor de evaluación de confianza incluyen, entre otros, la confiabilidad del operador del servidor y la responsabilidad comercial de cualquier oferta asociada a la sesión. Los atributos no tecnológicos son la confiabilidad del operador del servidor de aplicaciones, la oferta comercial realizada por el operador del servidor de aplicaciones o una fuente de los bienes o servicios adquiridos.

Además, el orden de los pasos para determinar el nivel de confianza es irrelevante siempre que la determinación final del nivel de confianza no dependa del orden.

Como se ha indicado anteriormente, el algoritmo global para determinar el nivel de confianza puede compartirse entre el procesador del servidor de evaluación de confianza 210 y el procesador del terminal 202. Por ejemplo, el terminal 202 puede solicitar al servidor de evaluación de confianza 210 puntajes brutos con respecto a los aspectos de la tecnología que se utilizan según lo obtenido del servidor de vigilancia tecnológica y el terminal 202 puede evaluar otros atributos y calcular el nivel final de confianza por sí mismo. Por otro lado, el servidor de evaluación de confianza 210 puede realizar toda la determinación del nivel de confianza con el terminal 202 solo mostrando el resultado final como se indica en el diagrama de flujo de la Figura 6.

En un algoritmo típico para determinar el nivel de confianza, hay varios atributos tecnológicos y no tecnológicos involucrados, y no todos los atributos suelen estar presentes. Los atributos que están presentes dependen de una operación de comunicación real que se evalúa. Si el terminal 202 no envía al servidor de evaluación de confianza todos los atributos que se requieren para la operación de comunicación dada, el servidor de evaluación de confianza 210 aún continúa calculando un nivel de confianza utilizando los valores predeterminados mencionados anteriormente.

Una forma para que el servidor de evaluación de confianza 210 realice el proceso ilustrado en la Figura 6 es comparar los datos proporcionados por el terminal con la tabla de ponderación. Algunos ejemplos son evaluar una calificación de seguridad o consultar servidores adicionales, por ejemplo, el servidor de vigilancia tecnológica 218, el servidor de emisión de certificados 220 y el servidor de análisis de mercado 222.

El procesamiento de la Figura 6 puede extenderse para que el servidor de evaluación de confianza 210 reciba la identidad del terminal (ya sea en forma de identidad absoluta, por ejemplo, número IME o como información de marca/modelo) y usa después la información almacenada en el servidor o en otro sitio para extraer la tecnología real utilizada por el terminal 202. En esta circunstancia, el terminal envía toda la información sobre la tecnología que se ha actualizado desde el lanzamiento original (por ejemplo, un nuevo software de seguridad) o sobre la tecnología que se utiliza junto con el terminal, por ejemplo, el uso real de una tarjeta inteligente.

La Figura 7 ilustra otra realización de la presente invención que se puede poner en práctica en el sistema de la Figura 5. El servidor de evaluación de confianza 210 transmite al terminal 202 una pantalla 400 de páginas como se ilustra en la Figura 7 que tiene múltiples marcos como la técnica anterior de la Figura 3B. Por ejemplo, solo se ilustran los marcos 402 y 404, pero cada página no se limita a la visualización de cualquier número establecido de marcos por página. Los marcos son normalmente de los servidores de aplicaciones 212 en la red, pero sin limitación de los mismos. El servidor de evaluación de confianza 210 transmite una serie de páginas 400, incluida una certificación 406 que indica que el servidor de evaluación de confianza 210 ha recopilado información dentro de la página 400 que contiene los múltiples marcos 402 y 404, que han sido determinadas por el servidor de evaluación de confianza 210 para ser de fuentes seguras. El mensaje "certificado" 406 informa al usuario del terminal 202 que las fuentes de todos los marcos 402 y 404 provienen de una fuente confiable.

El servidor de evaluación de confianza 210 transmite páginas al navegador del terminal 202 a través de la red 214. El servidor de evaluación de confianza tiene un certificado emitido por un TTP junto con una clave secreta que

proporciona la identidad del servidor de evaluación de confianza 21. Se puede hacer clic en "el certificado" para revelar una identidad verificada del servidor de evaluación de confianza 210 o de la organización responsable del mismo. El certificado 406 informa además al usuario que todas las fuentes de los marcos 402 y 404, por ejemplo, los servidores de aplicaciones 210 provienen de una fuente confiable como se describe en detalle en las Figuras 4C-4E.

El mensaje 406 supera el problema de la técnica anterior de la Figura 3B, en el que, con múltiples marcos, no se proporciona ninguna indicación de si los marcos provienen de una fuente segura más allá de la indicación 102.

Con la invención, la certificación realizada por el servidor de evaluación de confianza 210 asegura al usuario que todas las fuentes de información de marcos en páginas a las que está vinculado el navegador son seguras, lo que permite al usuario proceder con confianza.

Si bien la invención se ha descrito en términos de sus realizaciones preferidas, se pueden realizar numerosas modificaciones a la misma sin apartarse del alcance de la presente invención. Se pretende que todas esas modificaciones caigan dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método que comprende:

recibir, en un servidor (210), una primera solicitud para un análisis de una primera operación de comunicación desde un terminal (202) durante una sesión de terminal;
determinar, por el servidor (210), un primer nivel de confianza, en el que el primer nivel de confianza es indicativo de un primer nivel de seguridad asociado a la primera operación de comunicación si un usuario permite que se lleve a cabo la primera operación de comunicación; y
enviar, desde el servidor (210) al terminal (202), la primera información de confianza que es indicativa del primer nivel de confianza.

2. El método de la reivindicación 1, en el que dicha determinación del primer nivel de confianza incluye:

recibir información de nivel de confianza; y
determinar el primer nivel de confianza a partir de la información de nivel de confianza recibida.

3. El método de las reivindicaciones 1 o 2, en el que dicha determinación de un primer nivel de confianza incluye determinar el primer nivel de confianza basándose en un atributo utilizado para la primera operación de comunicación.

4. El método de la reivindicación 3, en el que el atributo se basa en un tipo de tecnología de red utilizada para la primera operación de comunicación o en la tecnología utilizada por el terminal (202) durante la primera operación de comunicación.

5. El método de la reivindicación 3, en el que el atributo se basa en la confiabilidad de un operador de un servidor de aplicaciones (212) que proporciona un servicio que utiliza la primera operación de comunicación o en una viabilidad comercial de una oferta de servicio durante la sesión del terminal.

6. El método de la reivindicación 1, que comprende además:

recibir una segunda solicitud para una segunda operación de comunicación desde el terminal (202);
determinar por separado un segundo nivel de confianza para la segunda operación de comunicación durante la sesión de terminal; y
enviar segunda información de confianza que sea indicativa del segundo nivel de confianza.

7. El método de la reivindicación 1, en el que la primera solicitud comprende una pluralidad de atributos, el método comprende además:

determinar factores de confianza, en donde cada factor de confianza corresponde a uno de la pluralidad de atributos;
ponderar cada uno de dichos factores de confianza; y
obtener el primer nivel de confianza de los factores de confianza ponderados.

8. El método de la reivindicación 7, que comprende además:

elegir un valor por defecto para un atributo faltante; y
utilizar el valor por defecto como parte de la determinación del primer nivel de confianza.

9. El método de la reivindicación 8, en el que dicha elección de un valor por defecto comprende:
representar el valor por defecto mediante una contribución promedio.

10. El método de la reivindicación 1, en el que determinar un primer nivel de confianza incluye analizar al menos un atributo técnico asociado a la primera operación de comunicación.

11. El método de la reivindicación 10, que comprende:

recibir una opción para la primera operación de comunicación; y
ajustar el primer nivel de confianza basándose en la opción.

12. El método de la reivindicación 10, en el que determinar el primer nivel de confianza comprende:

recibir información sobre el procesamiento de la primera operación de comunicación a través de una red; y
calcular el primer nivel de confianza basándose en la información.

13. El método de la reivindicación 1, que comprende:

iniciar la primera operación de comunicación durante una sesión de terminal;
visualizar un indicador que es indicativo del primer nivel de confianza en una pantalla de usuario de un terminal (202); y
recibir una entrada para aceptar o rechazar la primera operación de comunicación basándose en el indicador visualizado.

14. El método de la reivindicación 13, que comprende:
mostrar el indicador para un marco asociado de una página web que se muestra, en donde la página web comprende una pluralidad de marcos.

15. El método de la reivindicación 13, en el que mostrar un indicador comprende:

mostrar una presentación gráfica del primer nivel de confianza en la pantalla del usuario; o
mostrar una presentación numérica del primer nivel de confianza en la pantalla del usuario.

16. Un programa informático que comprende medios de código de programa adaptados para realizar al menos una de las reivindicaciones 1-12 cuando el programa se ejecuta en un ordenador.

17. Un aparato que comprende:

una interfaz de comunicación configurada para recibir una solicitud de análisis de una primera operación de comunicación desde un terminal (202) durante una sesión de terminal, en donde el aparato está situado separado del terminal (202); y
un procesador configurado para determinar un primer nivel de confianza en respuesta a la solicitud recibida, en donde el primer nivel de confianza es indicativo de un nivel de seguridad asociado a la primera operación de comunicación si un usuario permite que se lleve a cabo la primera operación de comunicación, y provocar el envío al terminal (202), a través de la interfaz de comunicación, de la primera información de confianza que es indicativa del primer nivel de confianza .

18. El aparato de la reivindicación 17, en el que:

la solicitud comprende una pluralidad de atributos; y
el procesador está configurado además para:

determinar factores de confianza, en donde cada factor de confianza corresponde a uno de la pluralidad de atributos;
ponderar cada uno de dichos factores de confianza; y
obtener el primer nivel de confianza de los factores de confianza ponderados.

19. El aparato de la reivindicación 17, en el que el procesador está configurado adicionalmente para:
determinar el primer nivel de confianza en función de un atributo utilizado para la primera operación de comunicación.

20. El aparato de la reivindicación 19, en el que el atributo se basa
en un tipo de tecnología de red utilizada para la primera operación de comunicación; o
en la fiabilidad de un operador de un servidor de aplicaciones (212) que proporciona un servicio que utiliza la primera operación de comunicación.

21. El aparato de la reivindicación 19, en el que el atributo se basa en la tecnología utilizada por el terminal (202) durante la operación de comunicación o en la viabilidad comercial de una oferta de servicio durante una sesión de terminal.

22. El aparato de la reivindicación 17, en el que el procesador se configura adicionalmente para:

recibir una segunda solicitud de una segunda operación de comunicación desde el terminal (202);
determinar por separado un segundo nivel de confianza para la segunda operación de comunicación durante la sesión de terminal; y
enviar segunda información de confianza que sea indicativa del segundo nivel de confianza.

23. El aparato de la reivindicación 18, en el que el procesador está configurado adicionalmente para:

elegir un valor por defecto para un atributo faltante; y
utilizar el valor por defecto como parte de la determinación del primer nivel de confianza.

24. El aparato de la reivindicación 23, en el que el procesador está configurado adicionalmente para: representar el valor por defecto mediante una contribución promedio.

25. Un sistema (200), que comprende:

un aparato como se reivindica en al menos una de las reivindicaciones 17 a 24; y
un terminal (202) que comprende:

una pantalla de usuario; y
un procesador configurado para:

iniciar una operación de comunicación durante una sesión de terminal;
provocar la visualización de un indicador que sea indicativo del nivel de confianza en la pantalla del usuario; y
recibir una entrada para aceptar o rechazar la operación de comunicación basándose en el indicador visualizado.

26. Un sistema (200) de acuerdo con la reivindicación 25, en el que el procesador del terminal está configurado para provocar la visualización del indicador para un marco asociado de una página web que se muestra, en donde la página web comprende una pluralidad de marcos.

27. Un sistema (200) de acuerdo con la reivindicación 25, en el que el procesador del terminal está configurado para provocar la presentación de una presentación gráfica del primer nivel de confianza o una presentación numérica del nivel de confianza.

28. Un método, que comprende:

enviar, a un servidor (210), una primera solicitud para un análisis de una primera operación de comunicación desde un terminal (202) durante una sesión de terminal para determinar un primer nivel de confianza;
recibir, del servidor (210), una primera información de confianza, determinada por el servidor, que es indicativa del primer nivel de confianza, en donde el primer nivel de confianza es indicativo de un primer nivel de seguridad asociado a la primera operación de comunicación si un usuario permite que se lleve a cabo la primera operación de comunicación;
visualizar un indicador que es indicativo del primer nivel de confianza en una pantalla del terminal (202).

29. Un terminal, que comprende:

un procesador; y
una memoria que incluye el código del programa informático;
la al menos una memoria y el código del programa informático configurados para, con el procesador, hacer que el terminal al menos realice:

enviar, a un servidor (210), una primera solicitud para un análisis de una primera operación de comunicación desde el terminal (202) durante una sesión de terminal para determinar un primer nivel de confianza; recibir, del servidor (210), una primera información de confianza, determinada por el servidor, que es indicativa del primer nivel de confianza, en donde el primer nivel de confianza es indicativo de un primer nivel de seguridad asociado a la primera operación de comunicación si un usuario permite que se lleve a cabo la primera operación de comunicación;
visualizar en una pantalla del terminal (202) un indicador que es indicativo del primer nivel de confianza.

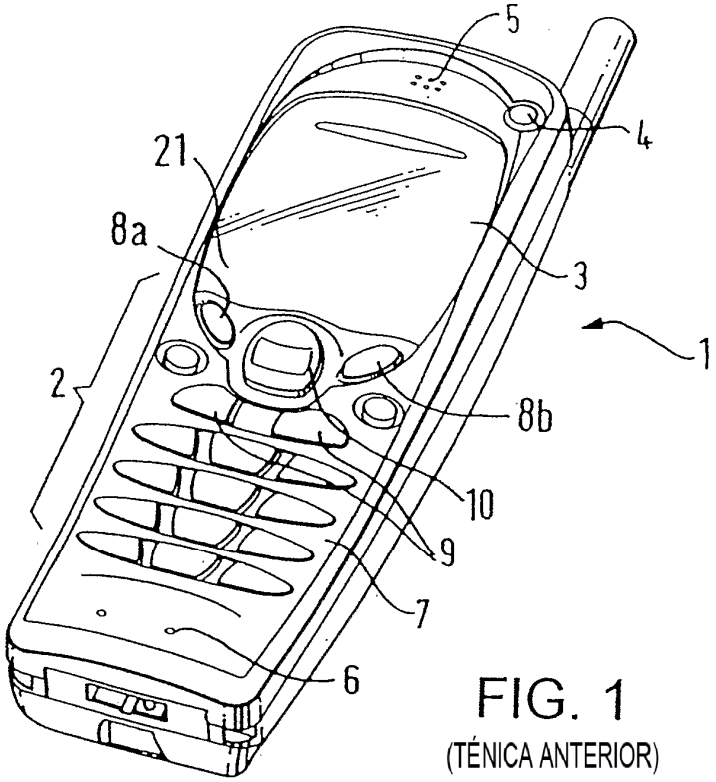


FIG. 1
(TÉNICA ANTERIOR)

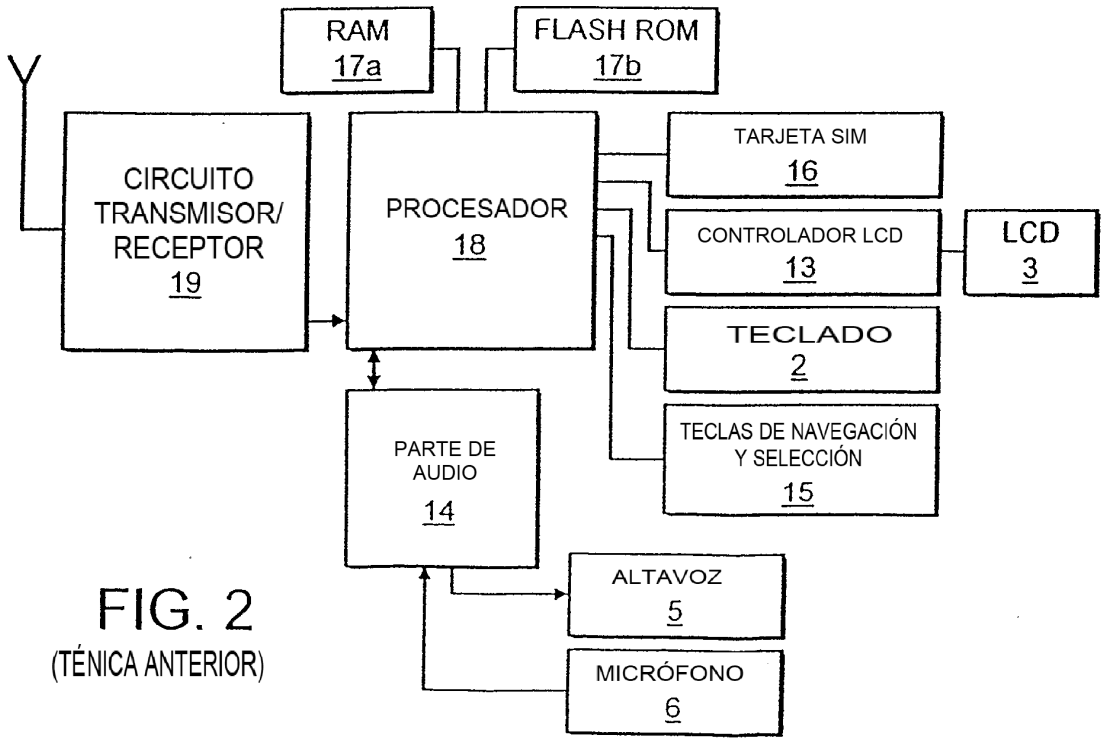


FIG. 2
(TÉNICA ANTERIOR)

FIG. 3A
(TÉNICA ANTERIOR)

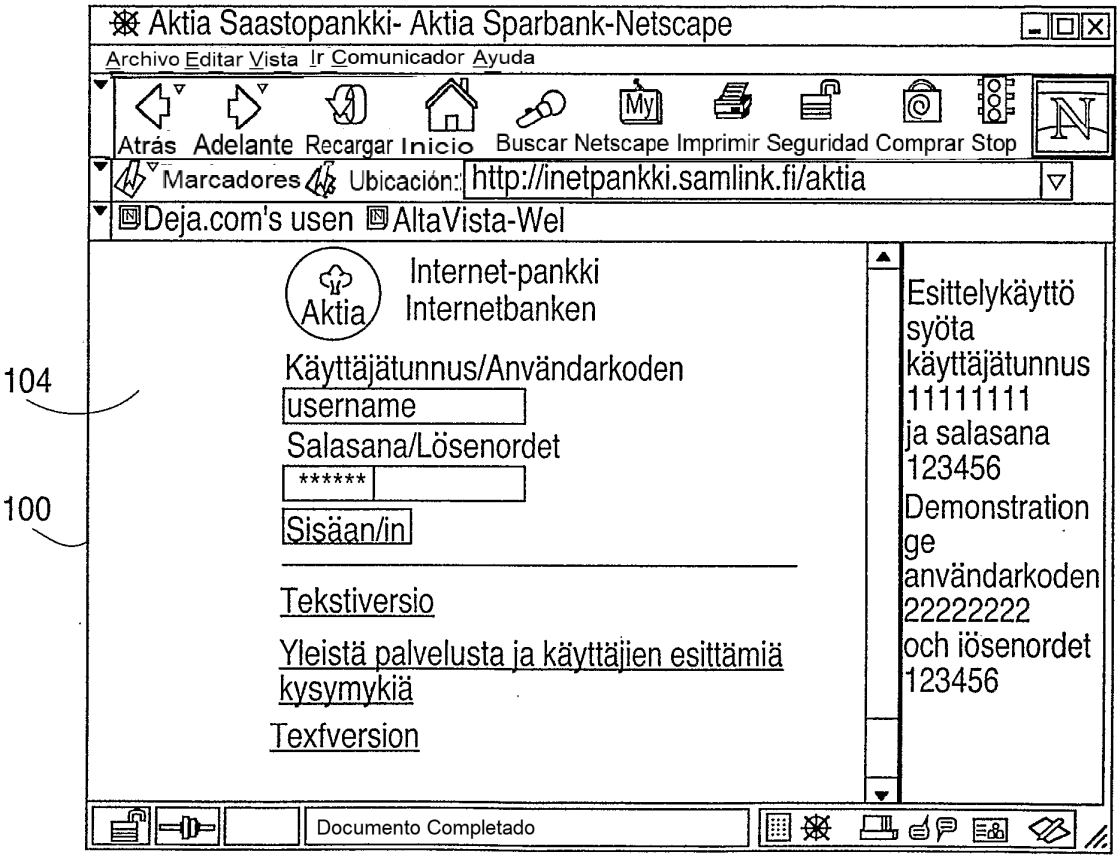


FIG. 3B

(TÉNICA ANTERIOR)

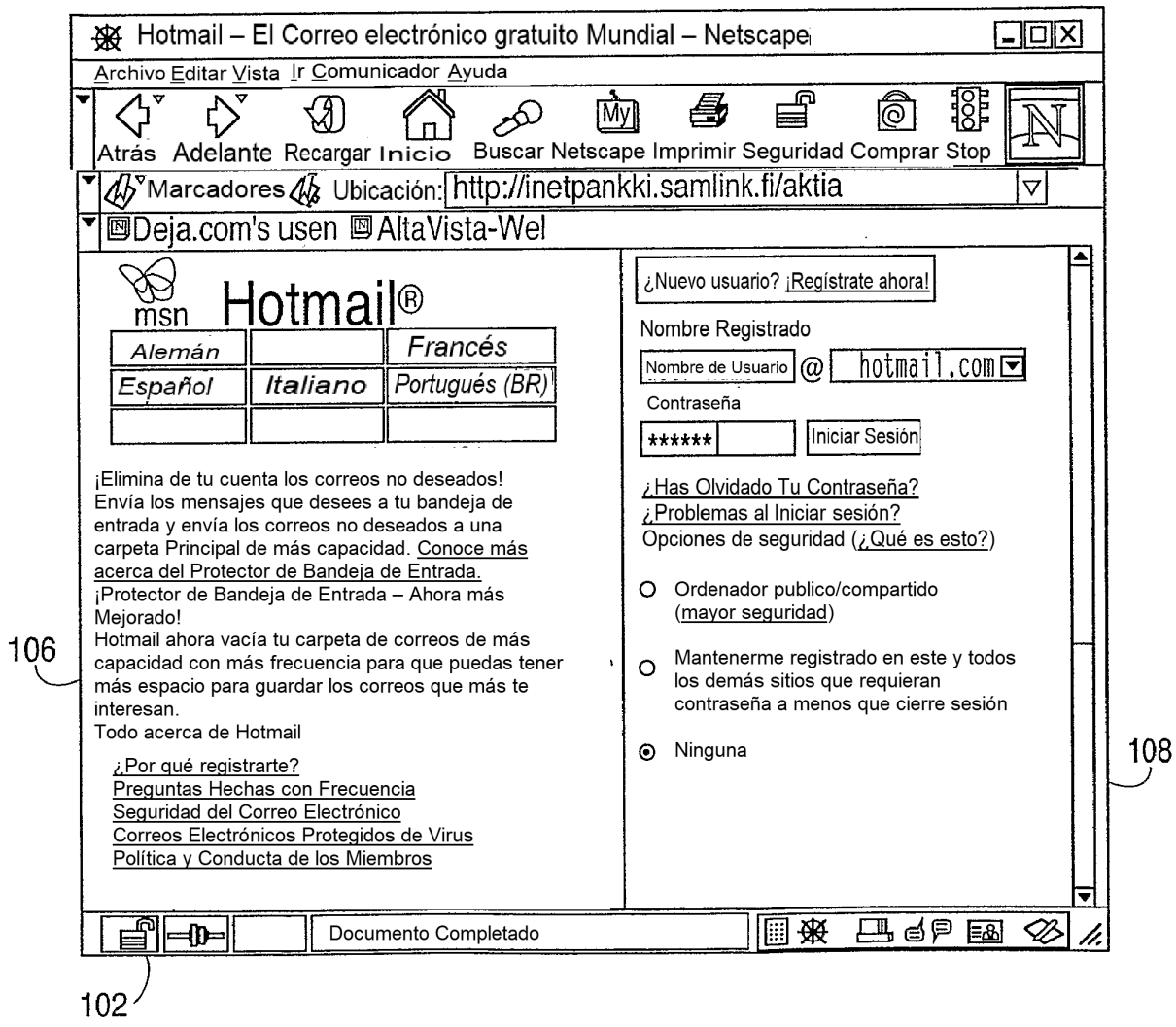


FIG. 4A

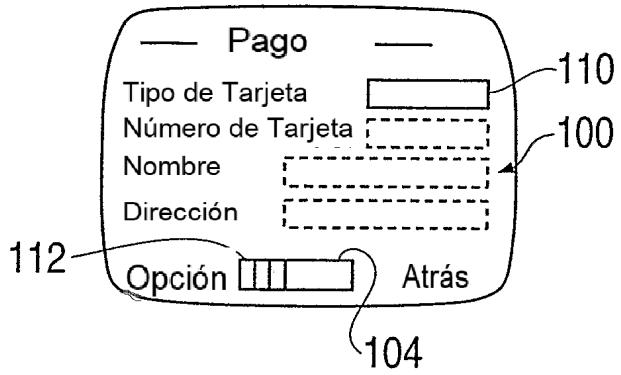

Pago
Tipo de Tarjeta
Número de Tarjeta
Nombre
Dirección
Opción
Atrás
110
100
112
104

FIG. 4B

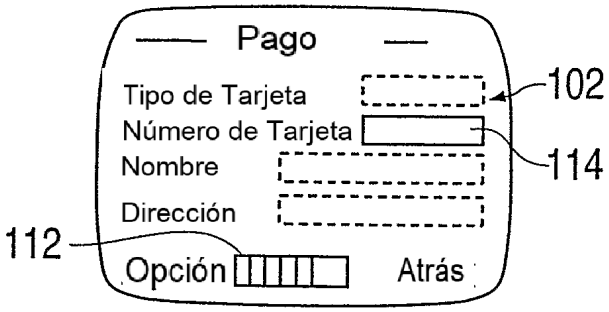

Pago
Tipo de Tarjeta
Número de Tarjeta
Nombre
Dirección
Opción
Atrás
102
114
112

FIG. 4C

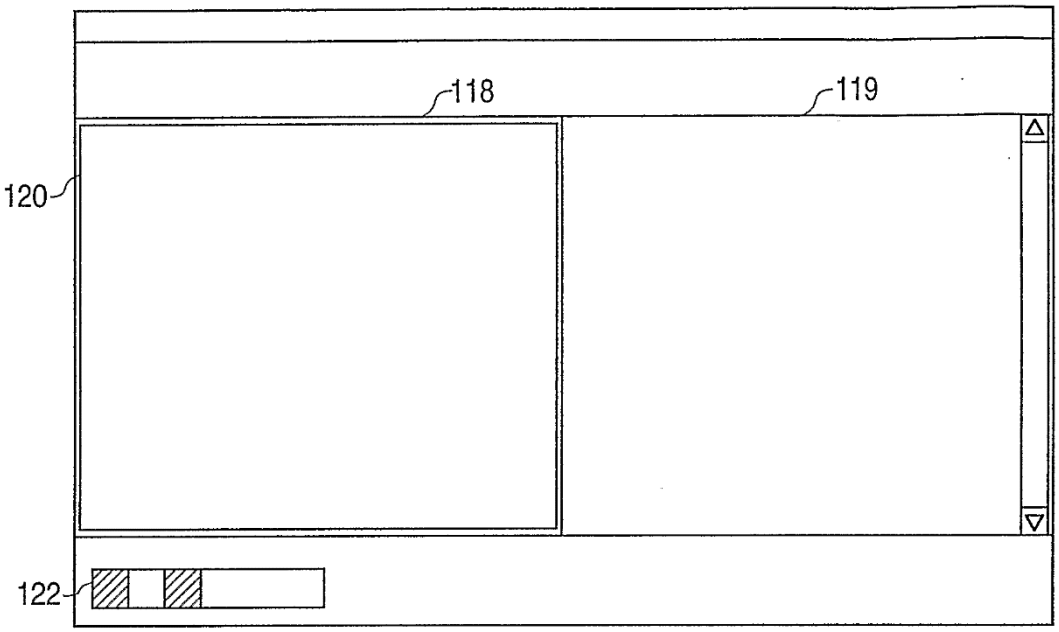


FIG. 4D

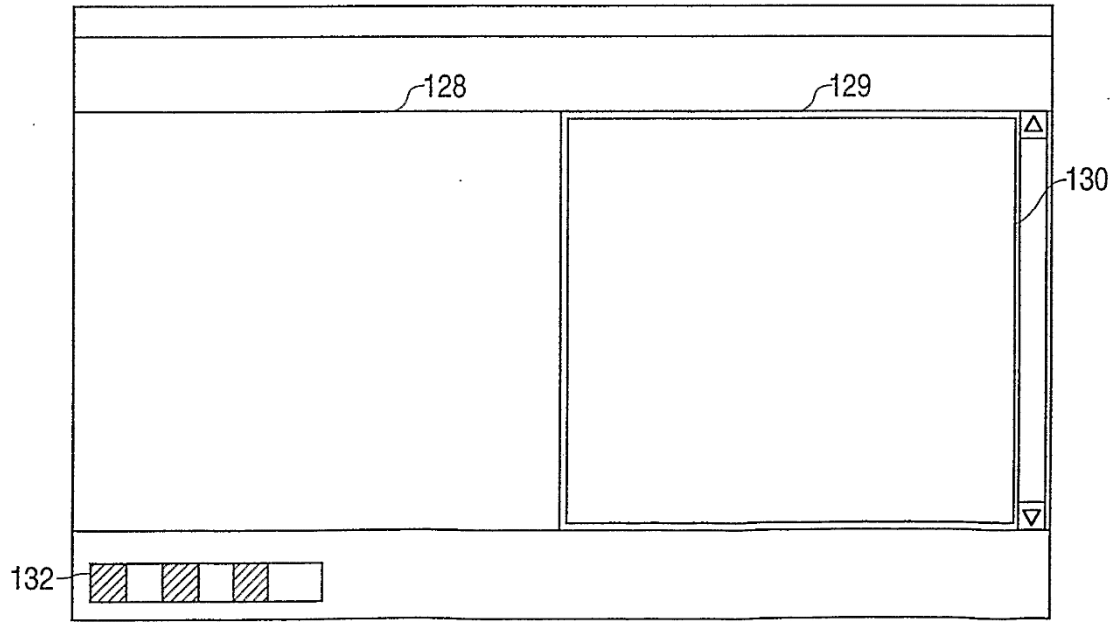


FIG. 4E

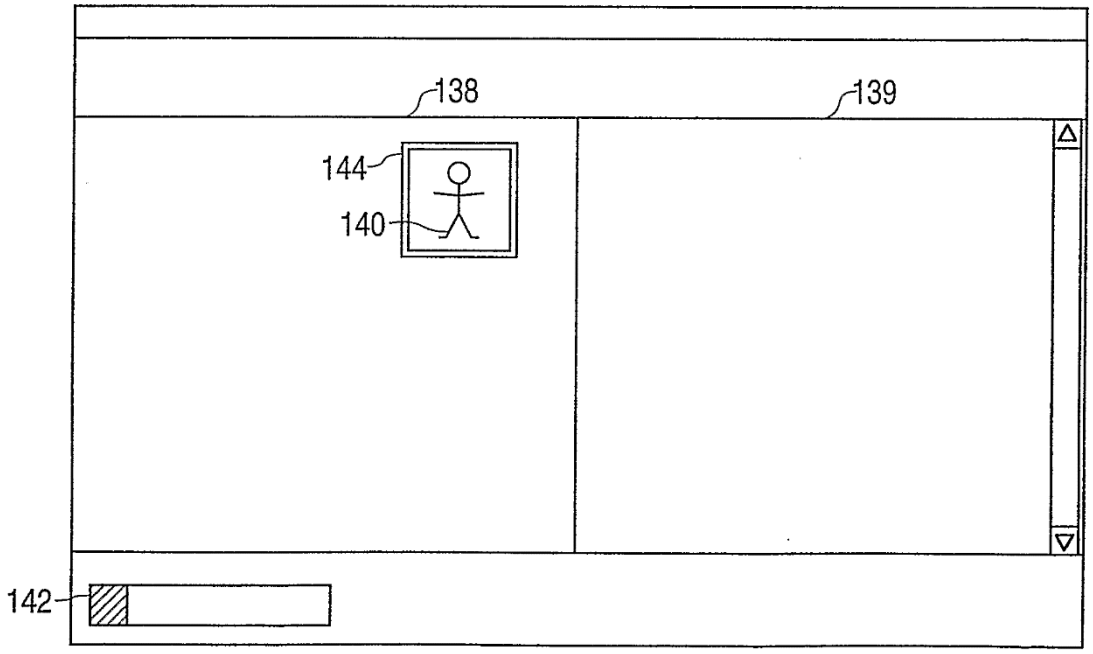


FIG. 5

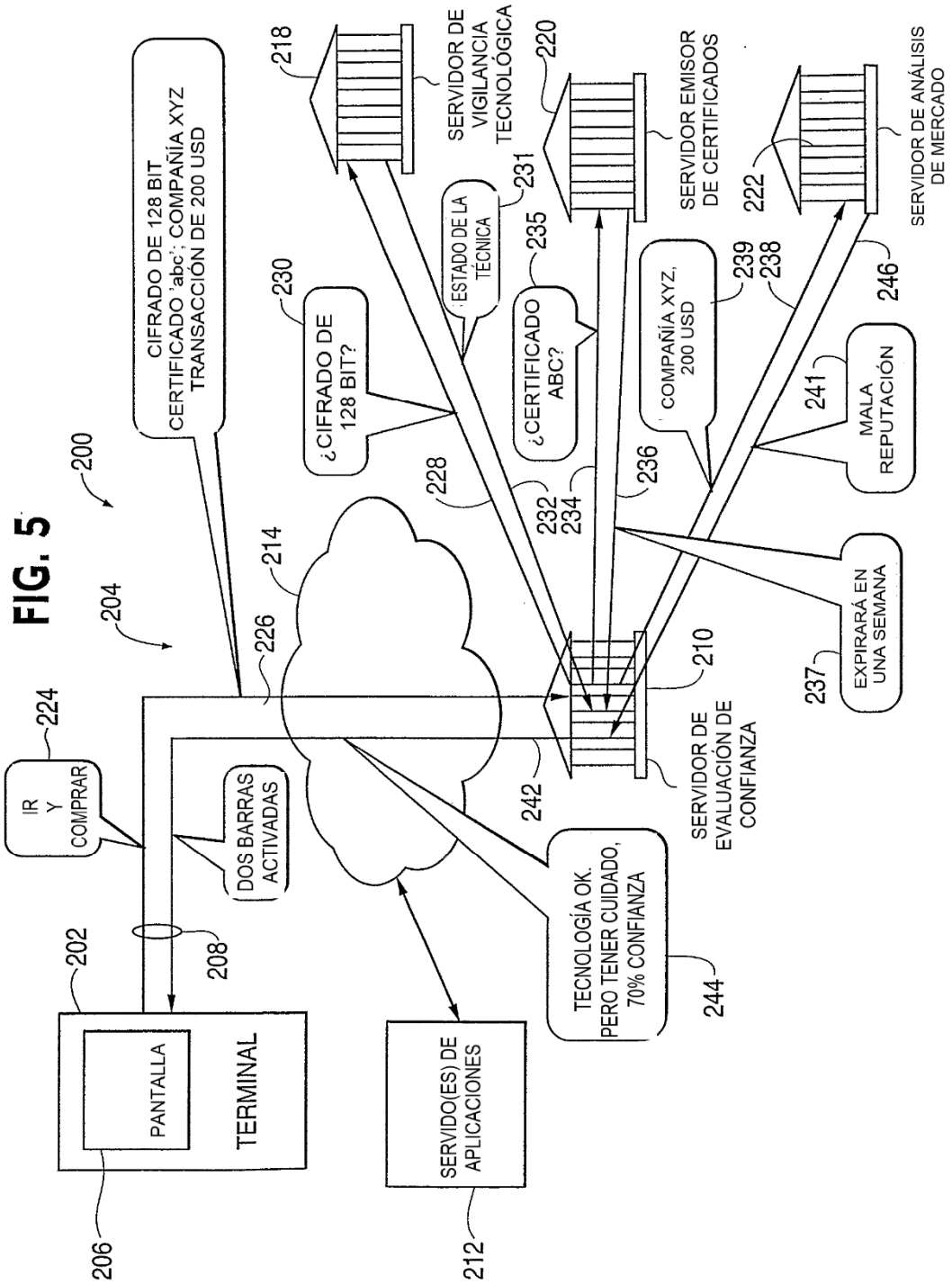

200
204
206
TERMINAL
PANTALLA
202
208
IR Y COMPRAR
224
DOS BARRAS ACTIVADAS
CIFRADO DE 128 BIT CERTIFICADO 'abc'; COMPAÑÍA XYZ TRANSACCIÓN DE 200 USD
226
214
SERVIDOR(ES) DE APLICACIONES
212
218
SERVIDOR DE VIGILANCIA TECNOLÓGICA
¿CIFRADO DE 128 BIT?
230
228
ESTADO DE LA TÉCNICA
231
220
SERVIDOR EMISOR DE CERTIFICADOS
¿CERTIFICADO ABC?
235
232
234
236
COMPAÑÍA XYZ, 200 USD
239
238
222
SERVIDOR DE ANÁLISIS DE MERCADO
MALA REPUTACIÓN
241
246
EXPIRARÁ EN UNA SEMANA
237
210
SERVIDOR DE EVALUACIÓN DE CONFIANZA
242
TECNOLOGÍA OK. PERO TENER CUIDADO, 70% CONFIANZA
244

FIG. 6

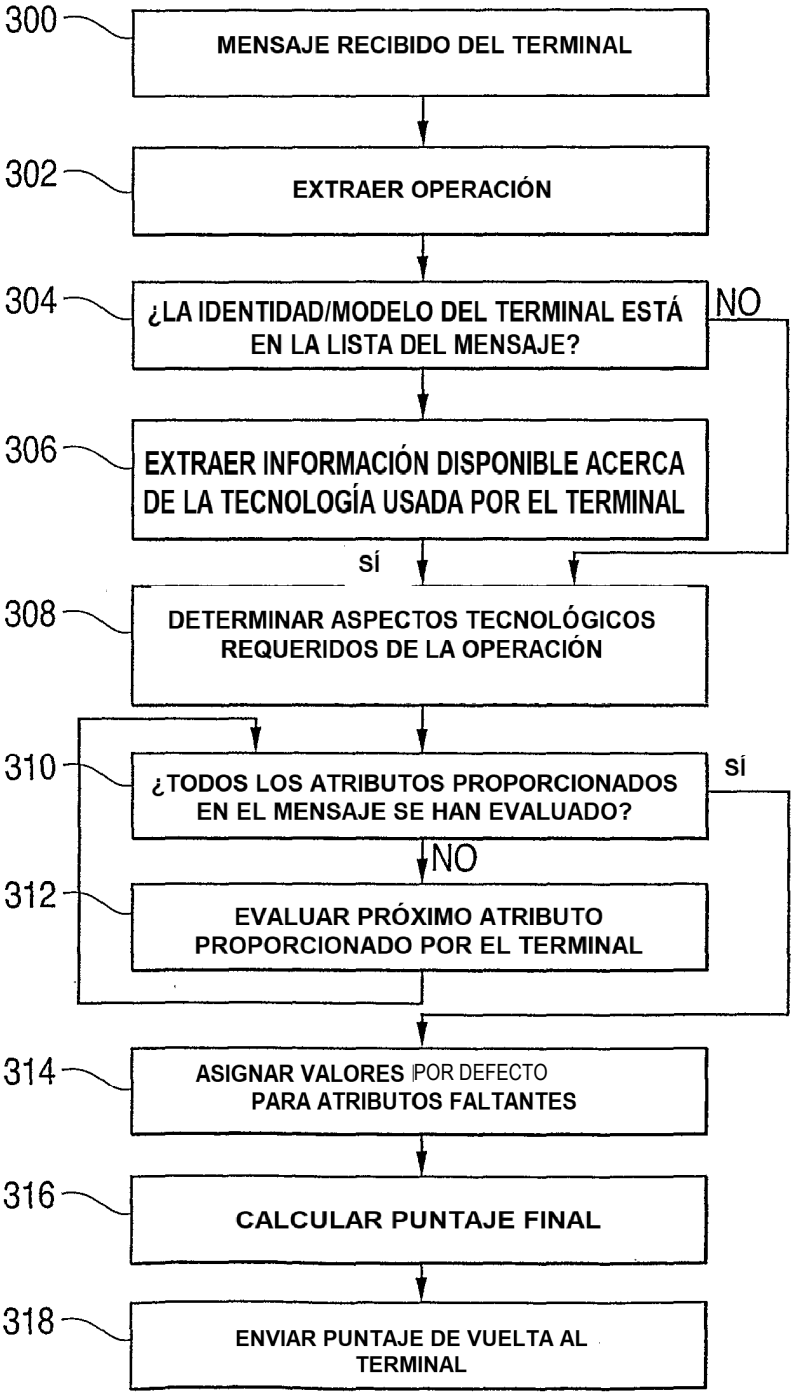
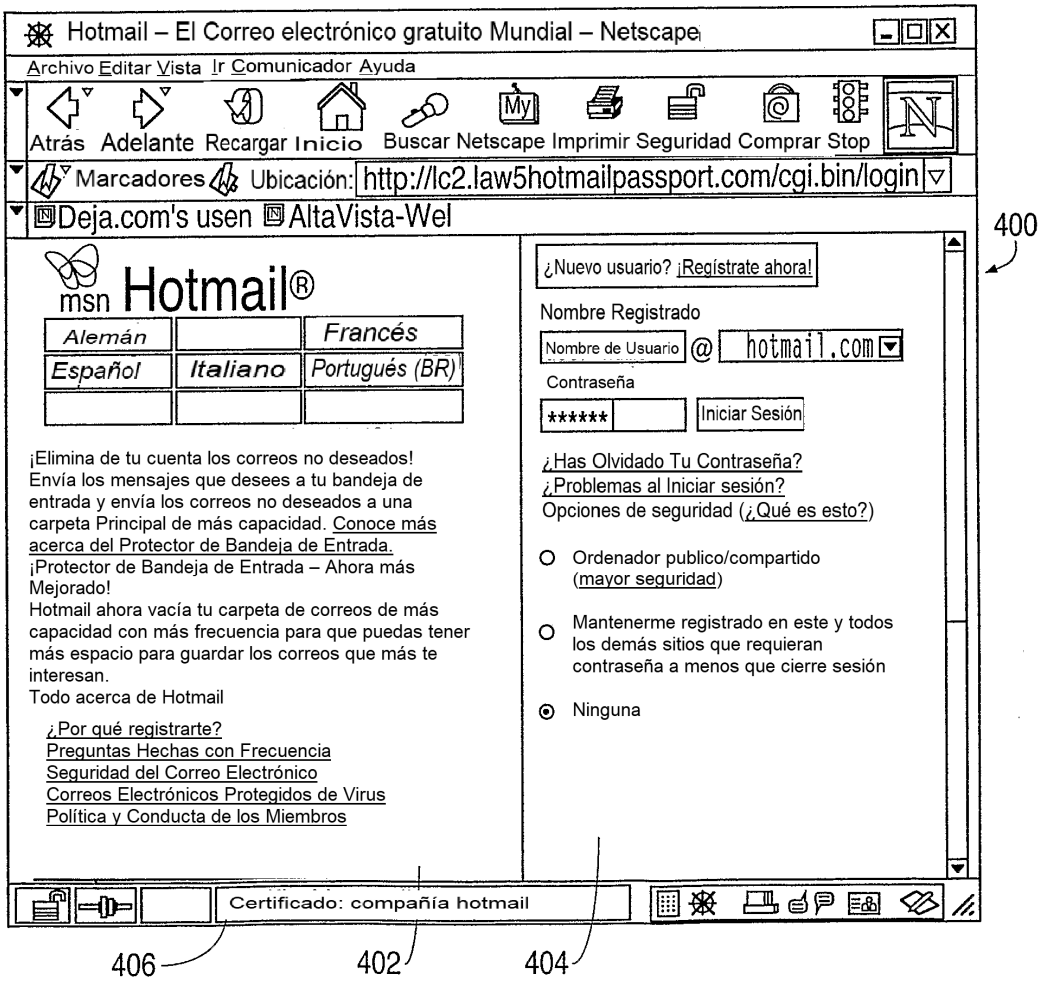

300
MENSAJE RECIBIDO DEL TERMINAL
302
EXTRAER OPERACIÓN
304
¿LA IDENTIDAD/MODELO DEL TERMINAL ESTÁ EN LA LISTA DEL MENSAJE?
NO
306
EXTRAER INFORMACIÓN DISPONIBLE ACERCA DE LA TECNOLOGÍA USADA POR EL TERMINAL
SÍ
308
DETERMINAR ASPECTOS TECNOLÓGICOS REQUERIDOS DE LA OPERACIÓN
310
¿TODOS LOS ATRIBUTOS PROPORCIONADOS EN EL MENSAJE SE HAN EVALUADO?
SÍ
NO
312
EVALUAR PRÓXIMO ATRIBUTO PROPORCIONADO POR EL TERMINAL
314
ASIGNAR VALORES POR DEFECTO PARA ATRIBUTOS FALTANTES
316
CALCULAR PUNTAJE FINAL
318
ENVIAR PUNTAJE DE VUELTA AL TERMINAL

FIG. 7


Hotmail – El Correo electrónico gratuito Mundial – Netscape
Archivo Editar Vista Ir Comunicador Ayuda
Atrás Adelante Recargar Inicio Buscar Netscape Imprimir Seguridad Comprar Stop
Marcadores Ubicación: http://lc2.law5hotmailpassport.com/cgi.bin/login
Deja.com's usen AltaVista-Wel
msn Hotmail®
Alemán
Francés
Español
Italiano
Portugués (BR)
¡Elimina de tu cuenta los correos no deseados!
Envía los mensajes que desees a tu bandeja de entrada y envía los correos no deseados a una carpeta Principal de más capacidad. Conoce más acerca del Protector de Bandeja de Entrada.
¡Protector de Bandeja de Entrada – Ahora más Mejorado!
Hotmail ahora vacía tu carpeta de correos de más capacidad con más frecuencia para que puedas tener más espacio para guardar los correos que más te interesan.
Todo acerca de Hotmail
¿Por qué registrarte?
Preguntas Hechas con Frecuencia
Seguridad del Correo Electrónico
Correos Electrónicos Protegidos de Virus
Política y Conducta de los Miembros
¿Nuevo usuario? ¡Regístrate ahora!
Nombre Registrado
Nombre de Usuario @ hotmail.com
Contraseña
******
Iniciar Sesión
¿Has Olvidado Tu Contraseña?
¿Problemas al Iniciar sesión?
Opciones de seguridad (¿Qué es esto?)
Ordenador publico/compartido (mayor seguridad)
Mantenerme registrado en este y todos los demás sitios que requieran contraseña a menos que cierre sesión
Ninguna
Certificado: compañía hotmail
400
406
402
404