(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 741 513**

(51) Int. CI.:

H04L 12/22 (2006.01)
G06F 21/62 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.09.2008 PCT/US2008/075557**

(87) Fecha y número de publicación internacional: **12.03.2009 WO09033137**

(96) Fecha de presentación y número de la solicitud europea: **08.09.2008 E 08799288 (9)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 2191610**

(54) Título: **Ofuscación de datos polimórfica multicanal basada en software**

(30) Prioridad:

07.09.2007 US 970722 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2020

(73) Titular/es:

DIS-ENT, LLC (100.0%)
5465 Desert Point Drive
Las Vegas, Nevada 89118, US

(72) Inventor/es:

JOHNSTON II, RICHARD, FENDALL;
STRAUSS, WILLIAM, J. y
PIERCE, DEAN

(74) Agente/Representante:

DÍAZ DE BUSTAMANTE TERMINEL, Isidro

DESCRIPCIÓN

Ofuscación de datos polimórfica multicanal basada en software.

Esta invención se refiere a una red de comunicación segura, un método para proporcionar comunicación segura dentro de una red de comunicaciones y un método de autenticación de usuarios para una red de comunicaciones.

AVISO DE DERECHOS DE AUTOR

ANTECEDENTES DE LA INVENCIÓN

Esta divulgación se refiere al cifrado, más específicamente, la divulgación se refiere a un sistema para un dispositivo implementado por ordenador y un método para neutralizar métodos para obtener datos confidenciales de un flujo de datos. La introducción de medidas de seguridad más complejas para proteger las cuentas financieras en línea solo ha dado como resultado esquemas más inteligentes para robar las credenciales personales necesarias para cometer fraude. Armados con un software de registro de pulsaciones de teclas o simplemente usando un malware inteligente, virus y spyware de clonación de formularios, los delincuentes en línea pueden robar las credenciales de identificación necesarias para apropiarse de cuentas e información confidencial.

El malware y los virus y spyware de clonación de formularios están destinados principalmente a robar información de usuarios en línea. Sin embargo, los indicios indican que el número de intentos de pirateo de cuentas financieras está aumentando sustancialmente. Por esta razón, las empresas con presencia en línea deben emplear una sólida autenticación de usuarios, entrada de datos y capacidades de almacenamiento, así como una transmisión de datos de usuario más segura.

La autenticación de usuarios durante las transacciones en línea basadas en Internet debe actualizarse a partir del proceso de autenticación de factor único generalmente aceptado actualmente, generalmente solo basado en el nombre de usuario y contraseñas, con una autenticación de usuarios de múltiples formas más segura. Los sitios web también deben dejar de transmitir datos confidenciales a través de texto sin formato que pueden ser capturados fácilmente a través de Internet.

En el documento US 2006/104446 A1, se describe un sistema y un método para proporcionar una comunicación segura dentro de una red de comunicaciones usando cifrado y descifrado de datos transmitidos en una red implementada por ordenador, preferentemente datos de identificación de autenticación de usuarios, tales como una contraseña, en el punto de entrada en el ordenador del usuario. Estos sistemas y métodos conocidos permiten a un usuario final seleccionar mentalmente un marcador de entre uno de los elementos dispuestos aleatoriamente en una primera parte de una imagen gráfica e incitan al usuario a introducir cada elemento del identificador moviendo el marcador seleccionado y la primera parte según sea necesario para alinear sustancialmente el marcador seleccionado con un elemento elegido de una disposición de elementos de una secuencia de identificador de autenticación individual que aparece en la segunda parte de la imagen gráfica. Por lo tanto, estos sistemas y métodos conocidos usan imágenes gráficas que se distorsionan antes de la transmisión al cliente y requieren la manipulación por parte del cliente de la información presentada al cliente.

Es contra el contexto, y las limitaciones y problemas asociados con el mismo, que se ha desarrollado la presente invención.

Para lograr esto, la red de comunicación segura de la invención comprende las características reivindicadas en la reivindicación 1, el método para proporcionar comunicación segura dentro de una red de comunicaciones de la invención comprende las características reivindicadas en la reivindicación 9 y el método de autenticación de usuarios para una red de comunicaciones de la invención comprende las características reivindicadas en la reivindicación 18.

En las reivindicaciones dependientes se reivindican realizaciones ventajosas de la invención.

Esta divulgación proporciona soluciones que son esencialmente de instalación inmediata y, por lo tanto, no requieren una minuciosa adaptación para añadirlas a la infraestructura técnica existente. La metodología descrita en lo sucesivo implementa múltiples capas de autenticación de usuarios de manera que reducen el impacto sobre la experiencia del usuario, es decir, pretende ser muy intuitiva y fácil de usar, al tiempo que defiende adecuadamente contra ataques a transacciones que son altamente vulnerables a fraude o ataque con los sistemas actuales.

BREVE RESUMEN DE LA INVENCIÓN

Dicho brevemente, la presente divulgación incluye software polimórfico que cambia cada vez que se ejecuta mientras mantiene intacto el algoritmo original.

Más particularmente, en diversas realizaciones, la presente divulgación proporciona una red de comunicación segura, en la que la red puede incluir al menos un dispositivo cliente conectable de forma comunicativa a un servidor anfitrión para comunicar datos entre el dispositivo cliente y el servidor anfitrión. En diversas implementaciones, el servidor anfitrión puede incluir un medio asociado con el servidor anfitrión para generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos y un medio asociado con el servidor anfitrión para transmitir el código fuente para el formulario de entrada de datos al dispositivo cliente. Además, en diversas implementaciones, el dispositivo cliente puede incluir un medio asociado con el dispositivo cliente para establecer una conexión de comunicaciones con el dispositivo anfitrión y un medio asociado con el dispositivo cliente para interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos para generar un página de entrada de datos interactiva que incluye una pluralidad de campos de entrada de datos interactivos y un teclado virtual, la página de entrada de datos interactiva presentada en una pantalla del dispositivo cliente. El dispositivo cliente puede incluir, además, un medio asociado con el dispositivo cliente para interpretar y ejecutar el código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente y transmutar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario.

En diversas otras realizaciones, la presente divulgación proporciona un método para proporcionar comunicación segura dentro de una red de comunicaciones, en el que el método incluye establecer una conexión de comunicaciones con un dispositivo cliente y un dispositivo anfitrión de la red de comunicaciones. El método puede incluir, además, generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos en el servidor anfitrión y transmitir el código fuente para el formulario de entrada de datos al dispositivo cliente. Además, el método puede incluir ejecutar un programa de interfaz almacenado en el dispositivo cliente para interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos y generar una página de entrada de datos interactiva presentada en una pantalla del dispositivo cliente utilizando los datos de ofuscación, incluyendo la página de entrada de datos interactiva una pluralidad de campos de entrada de datos interactivos y un teclado virtual. La ejecución de la interfaz puede afectar, además, a la interpretación y ejecución del código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente y transmutar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario.

En aún otras realizaciones, la presente divulgación proporciona un método de autenticación de usuarios para una red de comunicaciones, en el que el método incluye establecer una conexión de comunicaciones con un dispositivo cliente y un dispositivo anfitrión de la red de comunicaciones, a través del enrutador de comunicaciones de la red de comunicaciones. El método puede incluir, además, generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos en el servidor anfitrión y transmitir el código fuente para el formulario de entrada de datos al dispositivo cliente. Además, el método puede incluir ejecutar un programa de interfaz de enrutador almacenado en el dispositivo cliente para interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos y generar una página de entrada de datos interactiva presentada en una pantalla del dispositivo cliente utilizando los datos de ofuscación, incluyendo al página de entrada de datos interactiva una pluralidad de campos de entrada de datos interactivos y un teclado virtual. La ejecución de la interfaz de enrutador puede afectar, además, a la interpretación y ejecución del código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente y transmutar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario.

La ejecución de la interfaz de enrutador puede afectar aún más a la concatenación de los datos introducidos usando los dispositivos de interfaz de usuario primero y segundo, la aplicación de una sal aleatoria a los datos concatenados, la sal aleatoria generada en el servidor anfitrión e incorporada en el código fuente del formulario de entrada de datos, troceo (*hashing*) de los datos salados y pase de los datos troceados (*hashed*) al servidor anfitrión. Finalmente, el método puede incluir descifrar los datos troceados (*hashed*) en el servidor anfitrión, comparar los datos descifrados con los datos de credenciales de usuario almacenados en una base de datos de almacenamiento masivo electrónica del dispositivo anfitrión y autenticar un usuario del dispositivo cliente basándose en la comparación de datos.

BREVE DESCRIPCIÓN DE LAS VARIAS VISTAS DE LOS DIBUJOS

En los dibujos adjuntos que forman parte de la memoria descriptiva:

La figura 1 es un diagrama de bloques de una red informatizada para administrar un mecanismo de ofuscación de datos polimórfica multicanal basada en software, de acuerdo con diversas realizaciones de la presente divulgación;

Las figuras 2 y 2A proporcionan un diagrama de flujo que ilustra un método de implementación del mecanismo de ofuscación de datos polimórfica multicanal basada en software administrado por el sistema mostrado en la figura 1, de acuerdo con diversas realizaciones de la presente divulgación; y

La figura 3 es una vista esquemática de un teclado basado en software que permite la entrada de datos al sistema de la figura 1, de acuerdo con diversas realizaciones de la presente divulgación.

Los números de referencia correspondientes indican partes correspondientes en todas las varias figuras de los dibujos.

DESCRIPCIÓN

La siguiente descripción detallada ilustra la invención a modo de ejemplo y no a modo de limitación. La descripción claramente permite a un experto en la materia elaborar y usar la invención, describe varias realizaciones, adaptaciones, variaciones, alternativas y usos de la invención, incluyendo lo que actualmente se cree que es el mejor modo de llevar a cabo la invención.

Aunque aspectos de esta divulgación son susceptibles de realizaciones en muchas formas diferentes que se muestran en los dibujos y se describirán en el presente documento en detalle, diversas realizaciones se describen en detalle con el entendimiento de que las presentes divulgaciones deben considerarse como ejemplos de los principios de la divulgación y no pretenden limitar los aspectos generales de la divulgación a las realizaciones ilustradas.

La presente divulgación puede materializarse en forma de procesos implementados por ordenador y aparatos para poner en práctica esos procesos. La presente divulgación también puede materializarse en forma de código de programa informático que contiene instrucciones materializadas en medios tangibles, tales como disquetes, CD-ROM, discos duros o cualquier otro medio de almacenamiento legible por ordenador, en el que, cuando el código de programa informático se carga en, y es ejecutado por, un dispositivo electrónico tal como un ordenador, microprocesador o circuito lógico, el dispositivo se convierte en un aparato para poner en práctica la invención expuesta en las reivindicaciones adjuntas.

La presente divulgación también puede materializarse en forma de código de programa informático, por ejemplo, ya sea almacenado en un medio de almacenamiento, cargado en y/o ejecutado por un ordenador, o transmitido a través de algún medio de transmisión, tal como por alambres o cableado eléctrico, a través de fibra óptica, o mediante radiación electromagnética, en el que, cuando el código de programa informático se carga en y es ejecutado por un ordenador, el ordenador se convierte en un aparato para poner en práctica la invención. Cuando se implementa en un microprocesador de uso general, los segmentos de código de programa informático configuran el microprocesador para crear circuitos lógicos específicos.

La figura 1 es una ilustración de una red informatizada 10 ejemplar, tal como una red de área local (LAN) o una red de área amplia (WAN) que está estructurada y operable para implementar un mecanismo de ofuscación de datos polimórfica multicanal basada en software, como se describe a continuación. En diversas realizaciones, la red 10 puede incluir al menos un dispositivo cliente 14 conectable de forma comunicativa a un servidor anfitrión 18, por ejemplo, un servidor web, a través de un enrutador de comunicación 22, por ejemplo, Internet, para comunicar datos entre el dispositivo cliente 14 y el servidor anfitrión 18.

Aunque la red 10 puede incluir una pluralidad de dispositivos cliente 14 conectados de forma operativa al servidor anfitrión 18, por simplicidad y claridad, la red 10 se describirá en el presente documento con referencia a un solo dispositivo cliente 14. Sin embargo, debe entenderse que las disposiciones de la presente divulgación son igualmente aplicables a realizaciones que incluyen una pluralidad de dispositivos cliente 14, cada uno configurado para funcionar sustancialmente igual que el dispositivo cliente único descrito a continuación, y dichas realizaciones permanecen dentro del alcance de la presente divulgación.

En diversas implementaciones, el dispositivo cliente 14 puede ser un ordenador que incluye un procesador 30 adecuado para ejecutar todas las funciones y programas del dispositivo cliente 14. El dispositivo cliente 14 puede incluir, además, al menos un dispositivo de almacenamiento electrónico 34 que comprende un medio legible por ordenador, tal como un disco duro o cualquier otro dispositivo de almacenamiento electrónico de datos para almacenar cosas tales como paquetes de software o programas, algoritmos e información digital, datos, tablas de búsqueda, hojas de cálculo electrónicas y bases de datos, etc. El dispositivo cliente 14 puede incluir, además, una pantalla 38 para visualizar elementos tales como información, datos y/o representaciones gráficas, y una pluralidad de dispositivos de interfaz de usuario 42, por ejemplo, un primer dispositivo de interfaz de usuario 42A y un segundo dispositivo de interfaz de usuario 42B. Cada dispositivo de interfaz de usuario 42 puede ser cualquier dispositivo de interfaz adecuado, tal como un teclado, ratón, lápiz óptico, micrófono, escáner y/o una pantalla táctil interactiva en la

pantalla 38, y el dispositivo cliente 14 puede incluir cualquier combinación de dos o más de dichos dispositivos de interfaz de usuario 42.

En diversas realizaciones, el dispositivo cliente 14 puede incluir además un lector 46 de medios extraíbles para leer información y datos de, y/o escribir información y datos en, medios de almacenamiento electrónico extraíbles tales como disquetes, discos compactos, discos DVD, discos Zip, o cualquier otro medio de almacenamiento electrónico extraíble y portátil legible por ordenador. Como alternativa, el lector 46 de medios extraíbles puede ser un puerto de E/S utilizado para comunicarse con dispositivos de memoria externos o periféricos tales como memorias USB, lápices/tarjetas de memoria o discos duros externos. Aún más, el dispositivo cliente 14 puede incluir un dispositivo de interfaz de enrutador 50 para comunicar datos con el enrutador de comunicaciones 22, tal como un módem de acceso telefónico, un módem de cable, una conexión por satélite, una conexión DSL (línea de abonado digital), un puerto de Ethernet o similar.

Las realizaciones alternativas del dispositivo cliente 14 pueden incluir cualquier dispositivo eléctrico o electrónico capaz de comunicarse con el servidor anfitrión 18 a través del enrutador de comunicaciones 22, tal como, por ejemplo, un asistente digital personal (PDA), un teléfono móvil, un teléfono que funciona con un sistema de voz interactivo, o un televisor que funciona con un sistema interactivo de televisión por cable o satélite.

Aunque, como se ha descrito anteriormente, en diversas realizaciones, la red 10 puede ser cualquier red informatizada, tal como una LAN o una WAN, por simplicidad y claridad, la red 10 se describirá a continuación con respecto a diversas realizaciones de WAN. Sin embargo, debe entenderse que las disposiciones de la presente divulgación son igualmente aplicables a cualquier otra red informatizada donde se deseen comunicaciones seguras entre el dispositivo cliente 14 y el servidor anfitrión 18, y que dichas realizaciones permanecen dentro del alcance de la presente divulgación.

Por consiguiente, en diversas realizaciones, el procesador 30 es capaz de ejecutar un programa 52 de interfaz de enrutador, tal como un programa de navegador web y en lo sucesivo denominado el navegador web 52, para comunicarse con el servidor anfitrión 18, de forma ejemplar, un servidor web y en lo sucesivo denominado el servidor web 18, a través del enrutador de comunicaciones 22, de forma ejemplar, Internet y en lo sucesivo denominada Internet 22. Generalmente, en dichas realizaciones, un usuario puede interactuar con el dispositivo cliente 14 visualizando datos, a través de la pantalla 38, e introduciendo datos, a través de los dispositivos de interfaz de usuario 42. El navegador web 52 permite al usuario introducir direcciones de páginas web específicas a recuperar, que se denominan localizadores de recursos uniformes o URL. Las páginas web pueden contener diversos tipos de contenido, desde información textual simple hasta contenido multimedia e interactivo más complejo, tal como programas de software, gráficos, señales de audio, videos, etc. Un conjunto de páginas web interconectadas, que generalmente incluyen una página de inicio, se gestionan en el servidor web 18 como una colección denominada colectivamente como sitio web. El contenido y el funcionamiento de dichos sitios web son gestionados por el servidor web 18. Más particularmente, como se describe a continuación, el servidor web 18 ejecuta e implementa un programa 54 de ofuscación de datos polimórfico multicanal (MCPDO) para ofuscar los datos transmitidos entre el dispositivo cliente 14 y el servidor web 18, proporcionando de este modo comunicaciones seguras entre el dispositivo cliente 14 y el servidor web 18. Además, en diversas realizaciones, el servidor web 18 ejecuta e implementa el programa MCPDO 54 para ofuscar los datos transmitidos entre el dispositivo cliente 14 y el servidor web 18 para proporcionar autenticación de usuarios y comunicación de datos seguras durante transacciones en línea basadas en Internet.

Internet 22 puede utilizar cualquier protocolo de comunicaciones adecuado, tal como el protocolo de transferencia de hipertexto (HTTP), para comunicar datos entre el dispositivo cliente 14 y el servidor web 18. Sin embargo, como se ha descrito anteriormente, el enrutador de comunicaciones 22 puede ser cualquier red de intercambio de datos que implemente un protocolo de comunicaciones adecuado respectivo, tal como FTP (Protocolo de transferencia de archivos), SNMP (Protocolo simple de administración de red), TELNET (Red telefónica) y similares.

En diversas realizaciones, el servidor anfitrión 18, por ejemplo, el servidor web 18 comprende un sistema informático que incluye un procesador 58 y un dispositivo de almacenamiento masivo electrónico 62 que tiene el programa MCPDO 54 almacenado en él. Además, el servidor web 18 incluye al menos una base de datos 64 que reside en el dispositivo de almacenamiento masivo 62. El servidor web 18 está equipado adecuadamente con un dispositivo 66 de interfaz de enrutador para comunicar datos con el dispositivo cliente 14, tal como un módem de acceso telefónico, un módem de cable, una conexión por satélite, una conexión DSL, un puerto de Ethernet o similar. Generalmente, cuando el dispositivo cliente 14 inicia las comunicaciones con el servidor web 18, a través de Internet 22, el servidor web 18 ejecuta el programa MCPDO 54 para generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en el código fuente de un formulario de entrada de datos que se transmite al dispositivo cliente 14. Al recibir el formulario de entrada de datos, el navegador web 52 del dispositivo cliente interpreta los datos de ofuscación y el código de programa, presenta una página de entrada de datos interactiva 200 (mostrada en la figura 3) utilizando los datos de ofuscación, e implementa el código de programa de ofuscación.

Con referencia ahora a las figuras 1, 2, 2A y 3, las figuras 2 y 2A proporcionan un diagrama de flujo 100 que ilustra el funcionamiento y la funcionalidad de la red 10 durante la ejecución e implementación del programa MCPDO 54,

de acuerdo con diversas realizaciones de la presente divulgación. Inicialmente, un usuario utiliza uno o más de los dispositivos de interfaz de usuario 42 para ejecutar el navegador web 52 y establecer la conexión entre el dispositivo cliente 14 y el servidor web 18, a través de Internet 22, como se indica en 102. Al conectarse con el dispositivo cliente 14, el servidor web 18 ejecuta el programa MCPDO 54.

Debe entenderse que la siguiente descripción de la funcionalidad del servidor web 18 resulta de la ejecución del programa MCPDO 54 por el procesador 58 del servidor web. Es decir, aunque la siguiente descripción hará referencia al servidor web 18 que realiza diversas funciones, debe entenderse que, en última instancia, es la ejecución del programa MCPDO 54 por el procesador 58 del servidor web y los procesos y operaciones resultantes, según están controlados por el procesador 58 del servidor web, lo que afecta a la siguiente funcionalidad del servidor web 18.

En el momento de la ejecución del programa MCPDO 54, el servidor web 18 genera aleatoriamente un mapa de caracteres transmutado y almacena el mapa de caracteres transmutado en la base de datos 64, como se indica en 104 y 106. El servidor web 18 inicia, a continuación, la generación del formulario de entrada de datos y el código fuente asociado que se pasará o transmitirá posteriormente al dispositivo cliente 14 y será ejecutado por el navegador web 52 para proporcionar una página de entrada de datos interactiva visualizada en la pantalla 38 del dispositivo cliente. Una página de entrada de datos interactiva ejemplar 200, por ejemplo, un formulario de inicio de sesión, que puede ser generada por el navegador web 52 basándose en el código fuente del formulario generado por el servidor web, se ilustra en la figura 3. En diversas realizaciones, la página de entrada de datos interactiva 200 puede incluir una pluralidad de campos de entrada de datos interactivos 204, por ejemplo, un campo de nombre de usuario 204A, un campo de contraseña 204B, un campo de PIN 204C, un campo de clave 204D y cualquier otro campo deseado. La página de entrada de datos interactiva 200 incluye además una etiqueta de campo 206 asociada con cada campo interactivo 204, por ejemplo, una etiqueta de nombre de usuario 206A, una etiqueta de contraseña 206B, una etiqueta de PIN 206C y una etiqueta de clave 206D. Cabe destacar que, en diversas realizaciones, cada etiqueta de campo 206 se presenta como una imagen, en lugar de texto, por ejemplo, texto HTML, que es identificado fácilmente por spyware, malware, virus, etc., en este documento denominado software de ataque. Además, en diversas realizaciones, la página de entrada de datos interactiva 200 puede incluir un gráfico, por ejemplo, virtual o en línea, un teclado 208 y una imagen de prevención contra robots alfa/numérica aleatoria 212.

Debe entenderse que cada conexión entre el dispositivo cliente 14 y el servidor web 18, como se describe en el presente documento, generará un código fuente del formulario de entrada de datos que es completamente aleatorio y diferente de cualquier código fuente generado anterior o posteriormente, pero cuando lo utiliza el navegador web 52 del dispositivo cliente, generará gráficamente la misma página de entrada de datos interactiva 200.

A continuación, el servidor web 18 incorpora el mapa de caracteres transmutado en el código fuente del formulario de entrada de datos y asigna el mapa de caracteres transmutado al teclado virtual 208 que será generado por el navegador web 52 del dispositivo cliente al recibir el formulario de entrada de datos, como se indica en 108 y 110.

El servidor genera, a continuación, una pluralidad de etiquetas de identificación (ID) de elementos de formularios aleatorios, almacena las etiquetas ID de elementos de formularios generadas aleatoriamente en la base de datos 64 e incorpora las etiquetas ID de elementos de formularios generadas aleatoriamente en el código fuente del formulario de entrada de datos, como se indica en 112, 114 y 116. A continuación, el servidor web 18 genera una pluralidad de elementos de formulario señuelo asociados con cada etiqueta ID de elementos e incorpora los elementos de formulario señuelo en el código fuente del formulario de entrada de datos, como se indica en 118 y 120. Posteriormente, el servidor web 18 generará nombres aleatorios para asociarlos con nombres de archivos de imagen y ubicaciones almacenadas en el dispositivo de almacenamiento masivo 62 del servidor web 18 e incorpora nombres en el código fuente del formulario de entrada de datos, como se indica en 122 y 124. Los archivos de imagen asociados que se identifican por los nombres generados aleatoriamente se pasan posteriormente al dispositivo cliente 14 y el navegador web 52 los utiliza para generar las imágenes para las etiquetas de campo 206 de cada campo interactivo 204. Por lo tanto, aunque el navegador web 52 del dispositivo cliente utilizará las etiquetas ID de elemento y los nombres de archivo de imagen incorporados en el código fuente del formulario de entrada de datos para generar gráficamente los mismos campos interactivos 204 y etiquetas de campo 206 de la página de entrada de datos interactiva 200, cada vez que el programa MCPDO 54 se ejecuta, las etiquetas ID de elementos de formulario y los nombres de archivo de imagen pasados del servidor web 18 al dispositivo cliente 14, a través del código fuente del formulario de entrada de datos, se generarán aleatoriamente y serán diferentes cada vez que se ejecute el programa MCPDO 54. Por lo tanto, será difícil para el software atacante capturar, rastrear o descifrar las etiquetas ID del elemento. Además, los elementos del formulario señuelo se pasarán al navegador web 52 del dispositivo cliente y después se pasarán de vuelta al servidor web 18 como datos POST inválidos o señuelo junto con la entrada de datos POST válidos a la página de entrada de datos interactiva 200 por el usuario. Por lo tanto, será difícil para el software atacante capturar, rastrear o descifrar los datos POST válidos.

Seguidamente, el servidor web 18 genera sal aleatoria para el troceo (*hashing*) de datos POST, almacena la sal generada aleatoriamente en la base de datos 64 del servidor web e incorpora la sal en el código fuente del formulario de entrada de datos, como se indica en 126, 128 y 130. A continuación, el servidor web 18 genera una cadena alfa/numérica de prevención contra robots aleatoria y almacena la cadena de prevención contra robots

aleatoria en la base de datos 64 del servidor web, como se indica en 132 y 134. La cadena aleatoria de prevención contra robots se presentará como la imagen de prevención contra robots 212 por el navegador web 52, al recibir el formulario de entrada de datos desde el servidor web 18 por el dispositivo cliente 14. Cabe destacar que la imagen de prevención contra robots 212 se presenta como una imagen, en lugar de texto, por ejemplo, texto HTML, que es identificado fácilmente por software atacante. A continuación, el servidor web 18 genera un nombre aleatorio para la imagen de prevención contra robots e incorpora el nombre de la imagen de prevención contra robots aleatoria en el código fuente del formulario de entrada de datos, como se indica en 136 y 138. Por lo tanto, la imagen y el nombre de prevención contra robots se generarán aleatoriamente y serán diferentes cada vez que se ejecuta el programa MCPDO 54, lo que hace que sea difícil para el software atacante capturar, rastrear o descifrar la imagen de prevención contra robots y los datos POST asociados.

Una vez que el servidor web 18 ha compilado el código fuente para el formulario de entrada de datos para incluir los diversos datos generados aleatoriamente, como se ha descrito anteriormente, el servidor web 18 pasa, o transmite, el formulario de entrada de datos y el código fuente respectivo al dispositivo cliente 14, como se indica en 140. Cabe destacar que, aunque se ha descrito anteriormente una secuencia ejemplar de datos generados aleatoriamente, cualquier secuencia adecuada de generación de datos aleatorios puede implementarse mediante la ejecución del programa MCPDO 54 y permanecer dentro del alcance de la presente divulgación.

Al recibir el formulario de entrada de datos y el código fuente respectivo, el navegador web 52 que se ejecuta en el dispositivo cliente 14 interpretará el código fuente, presentará la página de entrada de datos interactiva 200 en la pantalla 38 del dispositivo cliente y ejecutará la siguiente funcionalidad basándose en el código fuente, como se indica en 142. Es decir, la interpretación del código fuente proporciona un programa de ofuscación de datos polimórfica multicanal 'del lado del cliente' (csMCPDO), que no se muestra, pero que un experto en la materia entiende fácilmente que reside temporalmente en el dispositivo de almacenamiento electrónico 34 del dispositivo cliente y ejecutable por el procesador 30 del dispositivo cliente. Además, debe entenderse que la siguiente descripción de la funcionalidad del dispositivo cliente 14 resulta de la ejecución del csMCPDO por el procesador 30 del dispositivo cliente. Es decir, aunque la siguiente descripción hará referencia al dispositivo cliente 14 realizando diversas funciones, debe entenderse que, en última instancia, es la ejecución del programa csMCPDO por el procesador 30 del dispositivo cliente y los procesos y operaciones resultantes, controlados por el procesador 30 del dispositivo cliente, lo que afecta a la siguiente funcionalidad del dispositivo cliente 14. Además, debe entenderse que la siguiente funcionalidad se describirá en referencia a la página de entrada de datos interactiva ejemplar 200, por ejemplo, un formulario de inicio de sesión, que se muestra en la figura 3, pero es igualmente aplicable a otras páginas interactivas presentadas, mientras permanece dentro del alcance de la presente divulgación.

En diversas realizaciones, los campos interactivos 204 de la página de entrada de datos interactiva 200 se completan, es decir, los datos son introducidos por el usuario utilizando una pluralidad de dispositivos de interfaz de usuario 42, también denominados en el presente documento entrada de datos multicanal. Por ejemplo, se le puede solicitar al usuario que introduzca algunos datos usando el teclado 42A y otros datos usando el ratón 42B en combinación con el teclado virtual 208. La utilización de la entrada multicanal dificulta que el software del atacante monitorice, rastree o lea los datos introducidos del usuario. Además, los diversos campos interactivos 204 pueden completarse usando cualquier combinación o secuencia para el dispositivo de interfaz de usuario 204. Por ejemplo, una vez que se presenta la página de entrada de datos interactiva 200, a través del navegador web 52, el usuario puede introducir datos de nombre de usuario en el campo interactivo de nombre de usuario 204A, usando un teclado físico 42A del dispositivo cliente 14, como se indica en 144. Posteriormente, en diversas realizaciones, el dispositivo cliente 14 almacenará los datos de nombre de usuario introducidos en una Cookie para permitir que los datos POST se correlacionen con los datos en la base de datos 64 del servidor web, como se indica en 146. Es decir, la Cookie se usa como un identificador en los datos POST para permitir que el servidor web 18 busque en la base de datos 64 la credencial asociada con el usuario, es decir, asociada con los datos POST proporcionados por la entrada del usuario en los campos interactivos 204.

A continuación, el usuario puede introducir datos de contraseña en el campo interactivo de contraseña 204B, usando el teclado físico 42A del dispositivo cliente 14, como se indica en 148. Más particularmente, la entrada de datos al campo interactivo de contraseña 204B se transmuta mediante la ejecución del programa csMCPDO y se almacena temporalmente en el dispositivo de almacenamiento electrónico 34 del dispositivo cliente. Después de que se introducen los datos de contraseña, el usuario puede introducir datos de PIN en el campo interactivo de PIN 204C, usando un ratón 42B del dispositivo cliente 14 y el único teclado transmutado 208, como se indica en 150. Por consiguiente, la entrada de datos en el campo interactivo de PIN 204C se transmuta y se almacena temporalmente en el dispositivo de almacenamiento electrónico 34 del dispositivo cliente. Posteriormente, el usuario puede introducir la imagen de prevención contra robots alfa/numérica visualizada 212 utilizando el teclado 42A del dispositivo cliente 14, como se indica en 152. Además, la entrada de datos alfa/numéricos de la imagen de prevención contra robots 212 se transmuta mediante la ejecución del programa csMCPDO y se almacena de temporalmente en el dispositivo de almacenamiento electrónico 34 del dispositivo cliente. El usuario puede seleccionar, a continuación, un botón de inicio de sesión 214, a través de cualquiera de los dispositivos de interfaz de usuario 42, para enviar el formulario de inicio de sesión completado, es decir, la página de entrada de datos interactiva 200, como se indica en 154. Posteriormente, el dispositivo cliente 14 concatena la entrada transmutada de contraseña, PIN y datos de imagen de prevención contra robots, adjunta la sal a los datos concatenados, trocea

(*hash*) los datos concatenados salados y pasa la Cookie de nombre de usuario, los datos señuelo (descritos anteriormente) y el bloque de datos troceados (*hashed*), es decir, datos POST, de vuelta al servidor web 18, como se indica en 156, 158, 160 y 162.

Una vez que el servidor web 18 recibe la Cookie de nombre de usuario, los datos señuelo y el bloque de datos POST troceados (*hashed*), el servidor utiliza el mapa de caracteres transmutado, las etiquetas ID de elementos aleatorios y la sal aleatoria almacenada en la base de datos 64 del servidor web (descrita anteriormente) para descifrar el bloque de datos POST troceados (*hashed*).

Posteriormente, en diversas realizaciones, el servidor web 18 usa la Cookie para identificar los datos de credenciales de usuario almacenados en la base de datos 64 del servidor web y después compara los datos descifrados con las credenciales de usuario correspondientes, como se indica en 164. El servidor web 18 elimina a continuación el bloque de datos POST troceados (*hashed*), la Cookie de nombre de usuario y los datos señuelo recibidos desde el dispositivo cliente 14, como se indica en 166. Si los datos descifrados coinciden con las credenciales de usuario almacenadas en la base de datos 64 del servidor web, el servidor web 18 permite el acceso del usuario, a través del dispositivo cliente 14, como se indica en 168.

Por lo tanto, a través de la aplicación de la red 10 y la implementación del programa MCPDO 54, como se describe en el presente documento, no hay dos sesiones de usuario, incluso si las realiza el mismo usuario usando el mismo dispositivo cliente 14, que generen los mismos datos POST. Por lo tanto, es muy difícil para cualquier virus, spyware, malware y similar, es decir, el software atacante, interpretar, rastrear o descifrar los datos transmitidos entre el dispositivo cliente 14 y el servidor web 18.

Debe entenderse que, aunque la red 10 y la implementación del programa MCPDO 54 se han descrito anteriormente de manera ejemplar con respecto a la autenticación de un usuario para permitir que el usuario acceda al servidor web 18, la red 10 y la implementación del programa MCPDO 54 son igualmente aplicables a realizaciones en las que es deseable transmitir datos de forma segura desde un usuario, pero no necesariamente autenticar al usuario. Es decir, se prevé que la red 10 y el programa MCPDO 54 se puedan implementar y utilizar, como se ha descrito anteriormente, en ausencia de la funcionalidad de comparación de datos indicada en 146, 160 y 164, para transmitir de forma segura cualquier tipo de datos entre el dispositivo cliente 14 y el servidor web 18 sin el riesgo de que un atacante intercepte dichos datos.

Por lo tanto, la red 10 y su implementación del programa MCPDO 54, como se han descrito anteriormente, proporciona diversas características que afectan a la comunicación altamente segura entre el dispositivo cliente 14 y el servidor anfitrión 18, por ejemplo, el servidor web 18. Por ejemplo, entre las características proporcionadas se encuentra un teclado virtual basado en software que permite la entrada de datos a través de un ratón y que usa la transmutación de caracteres y el oscurecimiento de ventanas para evitar que un demonio de clonación de pantallas capture el contenido de la ventana. Otra característica de las proporcionadas es una página interactiva presentada en el dispositivo cliente que requiere entradas de campo multicanal, por ejemplo, ciertas entradas de campo a través del teclado y otras entradas de campo a través del ratón. Aún otra característica proporcionada es la provisión de envío de datos de método mixto en el que ciertos valores se transmiten usando Cookies de corta duración y que se destruyen inmediatamente al enviarlas, mientras que otros valores se envían usando entrada de datos POST. Aún otra característica más proporcionó el uso del intercambio de datos basado en troceo (*hash*).

Otra característica proporcionada es el uso de nombres de campo sin sentido en los que a todos los campos del formulario y nombres de imagen se les asigna una etiqueta aleatoria que solo es significativa para el servidor anfitrión 18 que generó el formulario de entrada de datos. Aún otra característica es el uso de datos de envío sin sentido o inválidos generados aleatoriamente incluidos con entradas de datos válidos de los datos POST. Otra característica proporcionada más es el uso de imágenes generadas aleatoriamente para evitar el envío automático del formulario de entrada de datos. Aún otra característica proporcionada más es la implementación de una tabla de credenciales estándar en la base de datos del dispositivo anfitrión 64 junto con una segunda tabla utilizada para gestionar los datos POST temporales recibidos desde el dispositivo cliente 14.

En vista de lo anterior, se verá que se han descrito diversas características de la invención y se han obtenido diversos resultados ventajosos. Dado que se podrían realizar diversos cambios en las construcciones anteriores sin apartarse del alcance de la invención, se pretende que toda la materia contenida en la descripción anterior o mostrada en los dibujos adjuntos se interprete como ilustrativa y no en un sentido limitante.

REIVINDICACIONES

1. Una red de comunicación segura que comprende: al menos un dispositivo cliente conectable de forma comunicativa a un servidor anfitrión para comunicar datos entre el dispositivo cliente y el servidor anfitrión; comprendiendo el servidor anfitrión:

un medio asociado con el servidor anfitrión para generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos que incluye generar una pluralidad de elementos de formulario señuelo e incorporar los elementos de formulario señuelo en el código fuente del formulario de entrada de datos; y

un medio asociado con el servidor anfitrión para transmitir el código fuente para el formulario de entrada de datos al dispositivo cliente; y

comprendiendo el dispositivo cliente:

un medio asociado con el dispositivo cliente para establecer una conexión de comunicaciones con el servidor anfitrión;

un medio asociado con el dispositivo cliente para interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos para generar una página de entrada de datos interactiva visualizada de manera consistente que incluye una pluralidad de campos de entrada de datos interactivos y un teclado virtual, la página de entrada de datos interactiva presentada en una pantalla del dispositivo cliente; y

un medio asociado con el dispositivo cliente para interpretar y ejecutar el código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar los datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente, para transmutar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario y para pasar datos señuelo basados en los elementos de formulario señuelo de vuelta al servidor anfitrión como datos POST inválidos junto con la entrada de datos POST válidos en los campos de entrada de datos interactivos.

2. La red de la reivindicación 1, en la que la primera interfaz de usuario comprende

un teclado físico y el segundo dispositivo de interfaz de usuario comprende un ratón informático.

3. La red de la reivindicación 1, que comprende además:

un medio asociado con el servidor anfitrión para generar un mapa de caracteres transmutado, almacenar el mapa de caracteres transmutado en una base de datos del servidor anfitrión e incorporar el mapa de caracteres transmutado en el código fuente del formulario de entrada de datos; y

un medio asociado con el servidor anfitrión para asignar el mapa de caracteres transmutado al teclado virtual.

4. La red de la reivindicación 1, que comprende además un medio asociado con el servidor anfitrión para generar una pluralidad de etiquetas ID de elementos de formularios aleatorios, almacenar las etiquetas ID de elementos de formularios aleatorios en una base de datos del servidor anfitrión e incorporar las etiquetas ID de elementos de formularios aleatorios en el código fuente del formulario de entrada de datos.

5. La red de la reivindicación 1, que comprende además un medio asociado con el servidor anfitrión para generar nombres aleatorios para nombres de archivos de imagen y ubicaciones almacenadas en un dispositivo de almacenamiento masivo electrónico del servidor anfitrión e incorporar nombres y ubicaciones de archivos de imagen aleatorios en el código fuente del formulario de entrada de datos.

6. La red de la reivindicación 1, que comprende además un medio asociado con el servidor anfitrión para generar una sal aleatoria para el troceo (*hashing*) de datos POST, almacenar la sal aleatoria en una base de datos

del servidor anfitrión e incorporar la sal aleatoria en el código fuente del formulario de entrada de datos.

7. La red de la reivindicación 1, que comprende además:

un medio asociado con el servidor anfitrión para generar una cadena aleatoria de imagen de prevención contra robots y almacenar la cadena aleatoria de imagen de prevención en una base de datos del servidor anfitrión; y

un medio asociado con el servidor anfitrión para generar un nombre aleatorio para la imagen de prevención contra robots e incorporar el nombre aleatorio para la imagen de prevención contra robots en el código fuente del formulario de entrada de datos.

8. La red de la reivindicación 1, que comprende además un enrutador de comunicaciones estructurado y operable para enrutar los datos entre el dispositivo cliente y el servidor anfitrión, en el que:

el servidor anfitrión comprende un servidor web;

el enrutador de comunicación comprende Internet; y

el medio asociado con el dispositivo cliente para establecer una conexión de comunicaciones con el servidor anfitrión, interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos para generar una página de entrada de datos interactiva e interpretar y ejecutar el código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente y transmutar los datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario, comprende un programa navegador web almacenado en un dispositivo de almacenamiento electrónico del dispositivo cliente y ejecutado por un procesador del dispositivo cliente.

9. Un método para proporcionar comunicación segura dentro de una red de comunicaciones, comprendiendo dicho método:

establecer una conexión de comunicaciones entre un dispositivo cliente y un servidor anfitrión de la red de comunicaciones;

generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos en el servidor anfitrión mientras se mantiene intacto el algoritmo original del servidor anfitrión, en el que generar e incorporar una pluralidad de datos de ofuscación y código de programa en un el código fuente para un formulario de entrada de datos comprende generar una pluralidad de elementos de formulario señuelo e incorporar los elementos de formulario señuelo en el código fuente del formulario de entrada de datos;

transmitir el código fuente para el formulario de entrada de datos al dispositivo cliente; y

ejecutar un programa de interfaz almacenado en el dispositivo cliente para:

interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos y generar una página de entrada de datos interactiva presentada en una pantalla del dispositivo cliente utilizando los datos de ofuscación, incluyendo la página de entrada de datos interactiva una pluralidad de campos de entrada de datos interactivos y un teclado virtual; e

interpretar y ejecutar el código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente, transmutar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario y pasar datos señuelo basados en los elementos de formulario señuelo de vuelta al servidor anfitrión como datos POST inválidos junto con datos POST válidos introducidos en los campos de entrada de datos interactivos.

10. El método de la reivindicación 9, en el que generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos comprende:

generar un mapa de caracteres transmutado, almacenar el mapa de caracteres transmutado en una base de datos del servidor anfitrión e incorporar el mapa de caracteres transmutado en el código fuente del formulario de entrada de datos; y

asignar el mapa de caracteres transmutado al teclado virtual.

11. El método de la reivindicación 9, en el que generar e incorporar una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos comprende generar una pluralidad de etiquetas ID de elementos de formularios aleatorios, almacenar las etiquetas ID de elementos de formularios aleatorios en una base de datos del servidor anfitrión e incorporar las etiquetas ID de elementos de formularios aleatorios en el código fuente del formulario de entrada de datos.

12. El método de la reivindicación 9, en el que generar e incorporar una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos comprende un medio asociado con el servidor anfitrión para generar nombres aleatorios para nombres de archivos de imagen y ubicaciones almacenadas en un dispositivo de almacenamiento masivo electrónico del servidor anfitrión, e incorporar nombres y ubicaciones de archivos de imagen aleatorios en el código fuente del formulario de entrada de datos.

13. El método de la reivindicación 9, en el que generar e incorporar una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos comprende generar una sal aleatoria para el troceo (*hashing*) de datos POST, almacenar la sal aleatoria en una base de datos del servidor anfitrión e incorporar la sal aleatoria en el código fuente del formulario de entrada de datos.

14. El método de la reivindicación 9, en el que generar e incorporar una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos comprende:

generar una cadena de imagen de prevención contra robots aleatoria y almacenar la cadena de imagen de prevención aleatoria en una base de datos del servidor anfitrión; y

generar un nombre aleatorio para la imagen de prevención contra robots e incorporar el nombre aleatorio para la imagen de prevención contra robots en el código fuente del formulario de entrada de datos.

15. El método de la reivindicación 9, en el que la red de comunicaciones incluye un enrutador de comunicaciones estructurado y operable para enrutar los datos entre el dispositivo cliente y el servidor anfitrión, y en el que el servidor anfitrión comprende un servidor web, el enrutador de comunicación comprende Internet, y en el que ejecutar un programa de interfaz almacenado en el dispositivo cliente comprende ejecutar un programa de navegador web almacenado en el dispositivo cliente.

16. El método de la reivindicación 9, en el que ejecutar el programa de interfaz comprende además ejecutar el código de programa incorporado en el código fuente del formulario de entrada de datos para:

concatenar los datos introducidos usando los dispositivos de interfaz de usuario primero y segundo;

aplicar una sal aleatoria a los datos concatenados, la sal aleatoria generada en el servidor anfitrión e incorporada en el código fuente del formulario de entrada de datos; trocear (*hash*) los datos salados; y pasar los datos troceados (*hashed*) al servidor anfitrión.

17. El método de la reivindicación 16, que comprende además:

descifrar los datos troceados (*hashed*) en el servidor anfitrión;

comparar los datos descifrados con los datos de credenciales de usuario almacenados en una base de datos de almacenamiento masivo electrónica del servidor anfitrión;

autenticar un usuario del dispositivo cliente basándose en la comparación de datos; y

eliminar los datos descifrados de un dispositivo de memoria del servidor anfitrión al finalizar la comparación de los datos descifrados con los datos de credenciales de usuario.

18. Un método de autenticación de usuarios para una red de comunicaciones, comprendiendo dicho método:

establecer una conexión de comunicaciones con un dispositivo cliente y un servidor anfitrión de la red de comunicaciones, a través de un enrutador de comunicaciones de la red de comunicaciones;

generar e incorporar de forma polimórfica una pluralidad de datos de ofuscación y código de programa en un código fuente para un formulario de entrada de datos en el servidor anfitrión mientras se mantiene intacto el algoritmo original del servidor anfitrión, incluyendo generar una pluralidad de elementos de formulario señuelo e incorporar los elementos de formulario señuelo en el código fuente del formulario de entrada de datos;

transmitir el código fuente para el formulario de entrada de datos al dispositivo cliente; y

ejecutar un programa de interfaz de enrutador almacenado en el dispositivo cliente para:

interpretar los datos de ofuscación incorporados en el código fuente del formulario de entrada de datos y generar una página de entrada de datos interactiva presentada en una pantalla del dispositivo cliente utilizando los datos de ofuscación, incluyendo la página de entrada de datos interactiva una pluralidad de campos de entrada de datos interactivos y un teclado virtual;

interpretar y ejecutar el código de programa incorporado en el código fuente del formulario de entrada de datos para ofuscar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un primer dispositivo de interfaz de usuario del dispositivo cliente, transmutar datos introducidos en al menos uno de los campos de entrada de datos interactivos usando un segundo dispositivo de interfaz de usuario, y pasar datos señuelo basados en los elementos de formulario señuelo de vuelta al servidor anfitrión como datos POST inválidos junto con datos POST válidos introducidos en los campos de entrada de datos interactivos;

concatenar los datos introducidos usando los dispositivos de interfaz de usuario primero y segundo;

aplicar una sal aleatoria a los datos concatenados, la sal aleatoria generada en el servidor anfitrión e incorporada en el código fuente del formulario de entrada de datos; trocear (*hash*) los datos salados; pasar los datos troceados (*hashed*) al servidor anfitrión; descifrar los datos troceados (*hashed*) en el servidor anfitrión;

comparar los datos descifrados con los datos de credenciales de usuario almacenados en una base de datos de almacenamiento masivo electrónica del servidor anfitrión; y

autenticar un usuario del dispositivo cliente basándose en la comparación de datos.

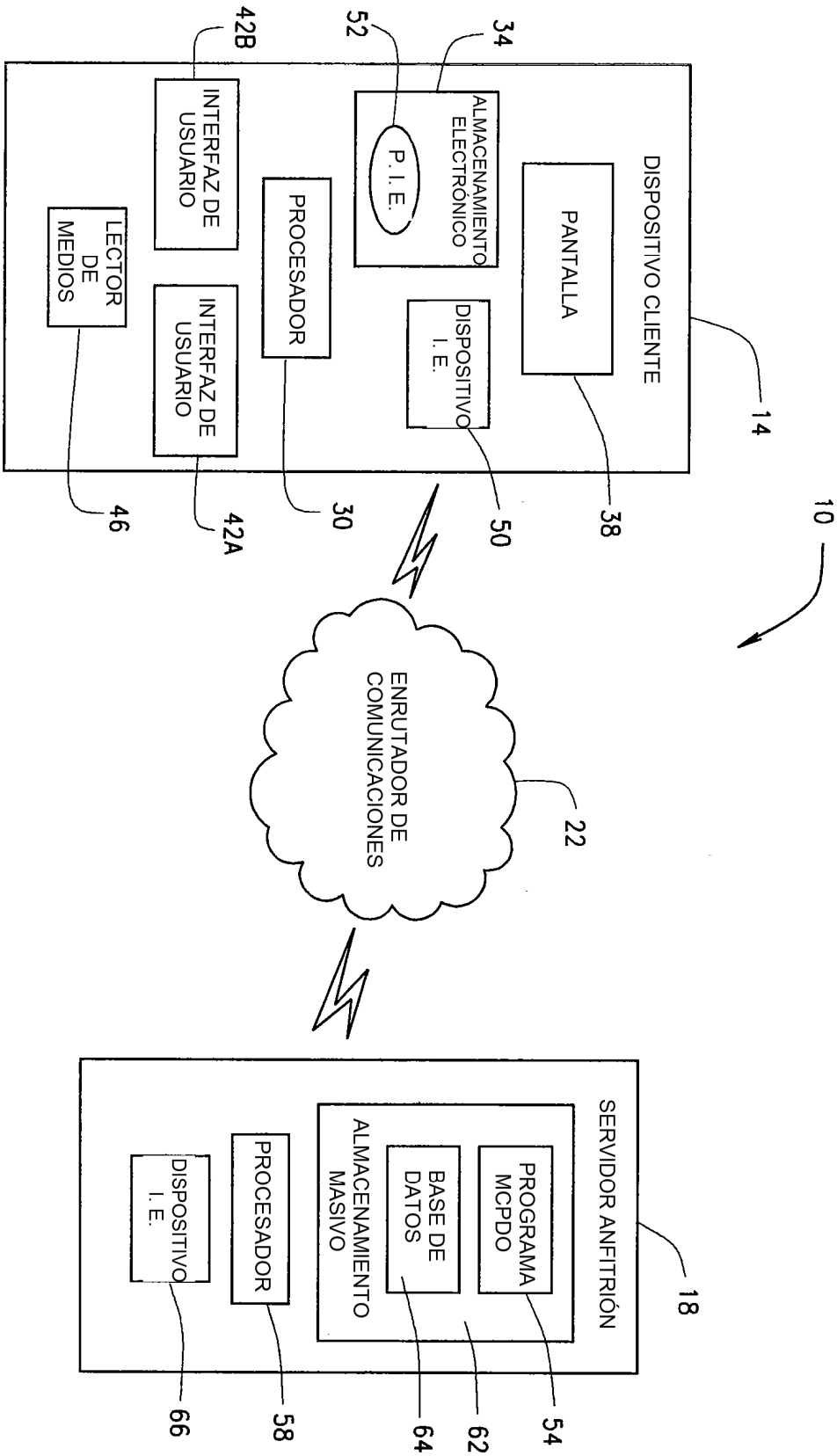
10
DISPOSITIVO CLIENTE
14
PANTALLA
38
ALMACENAMIENTO ELECTRÓNICO
34
P. I. E.
52
DISPOSITIVO I. E.
50
PROCESADOR
30
INTERFAZ DE USUARIO
42B
INTERFAZ DE USUARIO
42A
LECTOR DE MEDIOS
46
ENRUTADOR DE COMUNICACIONES
22
SERVIDOR ANFITRIÓN
18
PROGRAMA MCPDO
54
ALMACENAMIENTO MASIVO
BASE DE DATOS
62
64
PROCESADOR
58
DISPOSITIVO I. E.
66

FIG. 1

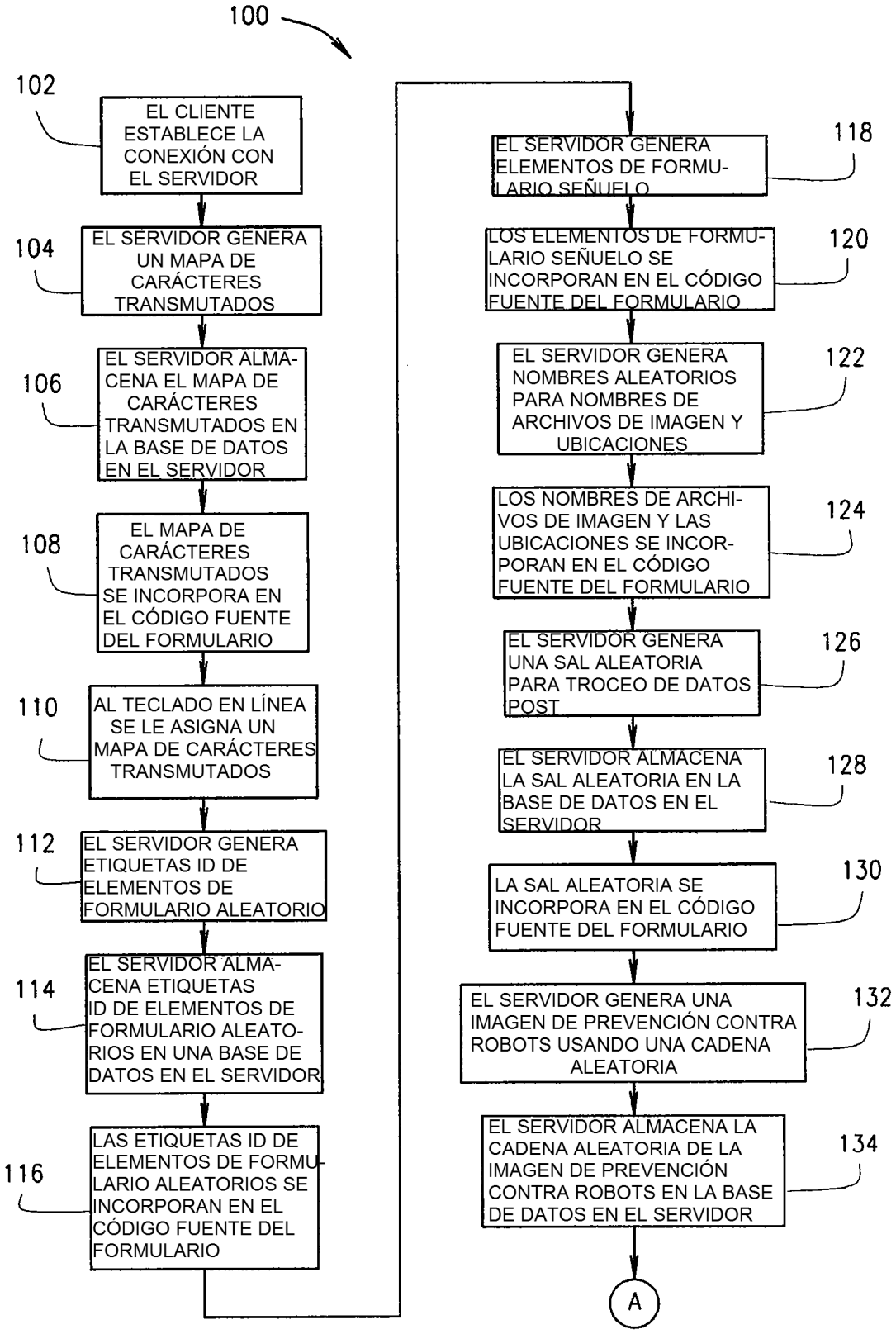
100
102
EL CLIENTE ESTABLECE LA CONEXIÓN CON EL SERVIDOR
104
EL SERVIDOR GENERA UN MAPA DE CARÁCTERES TRANSMUTADOS
106
EL SERVIDOR ALMACENA EL MAPA DE CARÁCTERES TRANSMUTADOS EN LA BASE DE DATOS EN EL SERVIDOR
108
EL MAPA DE CARÁCTERES TRANSMUTADOS SE INCORPORA EN EL CÓDIGO FUENTE DEL FORMULARIO
110
AL TECLADO EN LÍNEA SE LE ASIGNA UN MAPA DE CARÁCTERES TRANSMUTADOS
112
EL SERVIDOR GENERA ETIQUETAS ID DE ELEMENTOS DE FORMULARIO ALEATORIO
114
EL SERVIDOR ALMACENA ETIQUETAS ID DE ELEMENTOS DE FORMULARIO ALEATORIOS EN UNA BASE DE DATOS EN EL SERVIDOR
116
LAS ETIQUETAS ID DE ELEMENTOS DE FORMULARIO ALEATORIOS SE INCORPORAN EN EL CÓDIGO FUENTE DEL FORMULARIO
118
EL SERVIDOR GENERA ELEMENTOS DE FORMULARIO SEÑUELO
120
LOS ELEMENTOS DE FORMULARIO SEÑUELO SE INCORPORAN EN EL CÓDIGO FUENTE DEL FORMULARIO
122
EL SERVIDOR GENERA NOMBRES ALEATORIOS PARA NOMBRES DE ARCHIVOS DE IMAGEN Y UBICACIONES
124
LOS NOMBRES DE ARCHIVOS DE IMAGEN Y LAS UBICACIONES SE INCORPORAN EN EL CÓDIGO FUENTE DEL FORMULARIO
126
EL SERVIDOR GENERA UNA SAL ALEATORIA PARA TROCEO DE DATOS POST
128
EL SERVIDOR ALMACENA LA SAL ALEATORIA EN LA BASE DE DATOS EN EL SERVIDOR
130
LA SAL ALEATORIA SE INCORPORA EN EL CÓDIGO FUENTE DEL FORMULARIO
132
EL SERVIDOR GENERA UNA IMAGEN DE PREVENCIÓN CONTRA ROBOTS USANDO UNA CADENA ALEATORIA
134
EL SERVIDOR ALMACENA LA CADENA ALEATORIA DE LA IMAGEN DE PREVENCIÓN CONTRA ROBOTS EN LA BASE DE DATOS EN EL SERVIDOR
A

FIG. 2

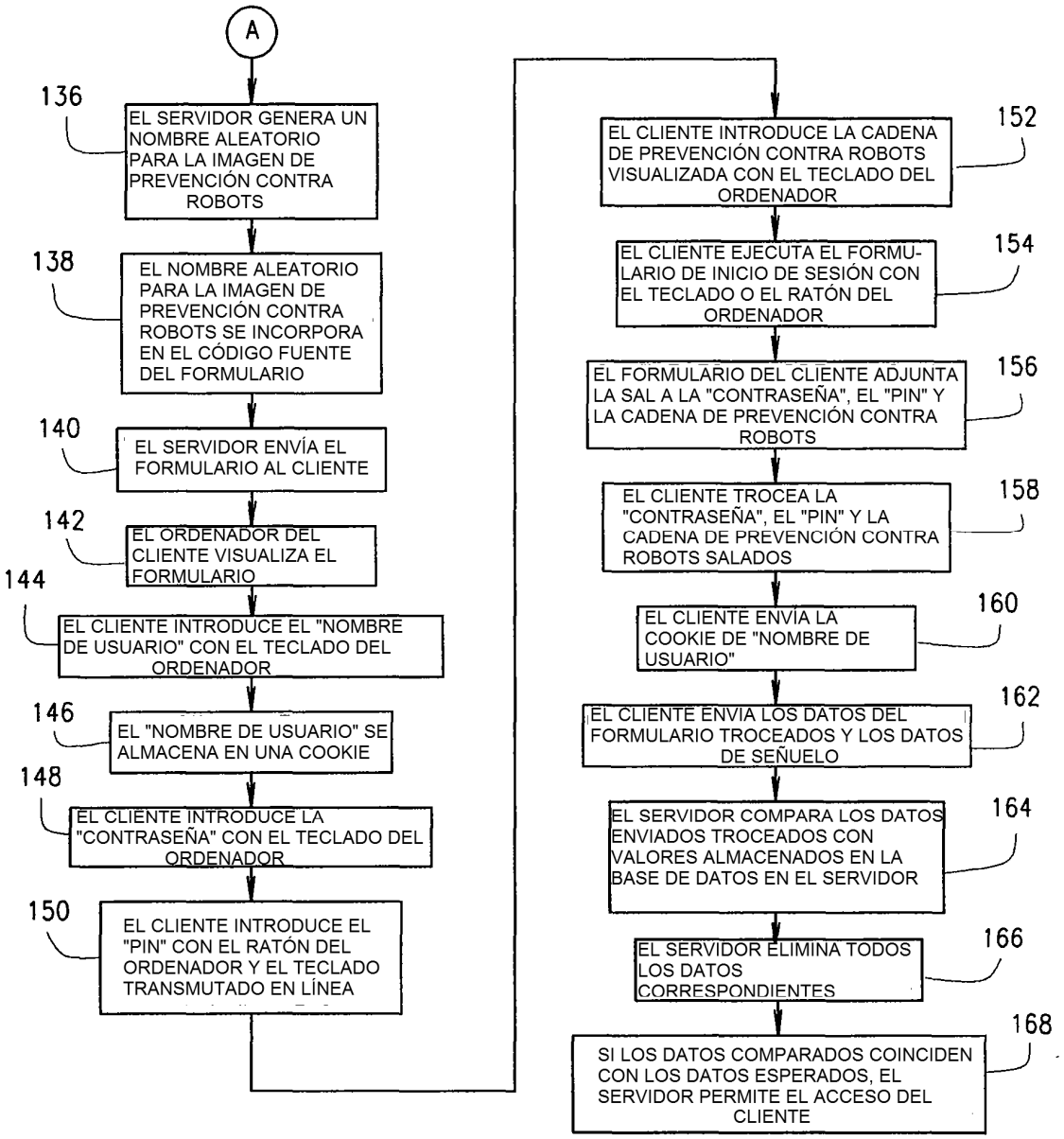
A
136
EL SERVIDOR GENERA UN NOMBRE ALEATORIO PARA LA IMAGEN DE PREVENCIÓN CONTRA ROBOTS
138
EL NOMBRE ALEATORIO PARA LA IMAGEN DE PREVENCIÓN CONTRA ROBOTS SE INCORPORA EN EL CÓDIGO FUENTE DEL FORMULARIO
140
EL SERVIDOR ENVÍA EL FORMULARIO AL CLIENTE
142
EL ORDENADOR DEL CLIENTE VISUALIZA EL FORMULARIO
144
EL CLIENTE INTRODUCE EL "NOMBRE DE USUARIO" CON EL TECLADO DEL ORDENADOR
146
EL "NOMBRE DE USUARIO" SE ALMACENA EN UNA COOKIE
148
EL CLIENTE INTRODUCE LA "CONTRASEÑA" CON EL TECLADO DEL ORDENADOR
150
EL CLIENTE INTRODUCE EL "PIN" CON EL RATÓN DEL ORDENADOR Y EL TECLADO TRANSMUTADO EN LÍNEA
152
EL CLIENTE INTRODUCE LA CADENA DE PREVENCIÓN CONTRA ROBOTS VISUALIZADA CON EL TECLADO DEL ORDENADOR
154
EL CLIENTE EJECUTA EL FORMULARIO DE INICIO DE SESIÓN CON EL TECLADO O EL RATÓN DEL ORDENADOR
156
EL FORMULARIO DEL CLIENTE ADJUNTA LA SAL A LA "CONTRASEÑA", EL "PIN" Y LA CADENA DE PREVENCIÓN CONTRA ROBOTS
158
EL CLIENTE TROCEA LA "CONTRASEÑA", EL "PIN" Y LA CADENA DE PREVENCIÓN CONTRA ROBOTS SALADOS
160
EL CLIENTE ENVÍA LA COOKIE DE "NOMBRE DE USUARIO"
162
EL CLIENTE ENVÍA LOS DATOS DEL FORMULARIO TROCEADOS Y LOS DATOS DE SEÑUELO
164
EL SERVIDOR COMPARA LOS DATOS ENVIADOS TROCEADOS CON VALORES ALMACENADOS EN LA BASE DE DATOS EN EL SERVIDOR
166
EL SERVIDOR ELIMINA TODOS LOS DATOS CORRESPONDIENTES
168
SI LOS DATOS COMPARADOS COINCIDEN CON LOS DATOS ESPERADOS, EL SERVIDOR PERMITE EL ACCESO DEL CLIENTE

FIG. 2A

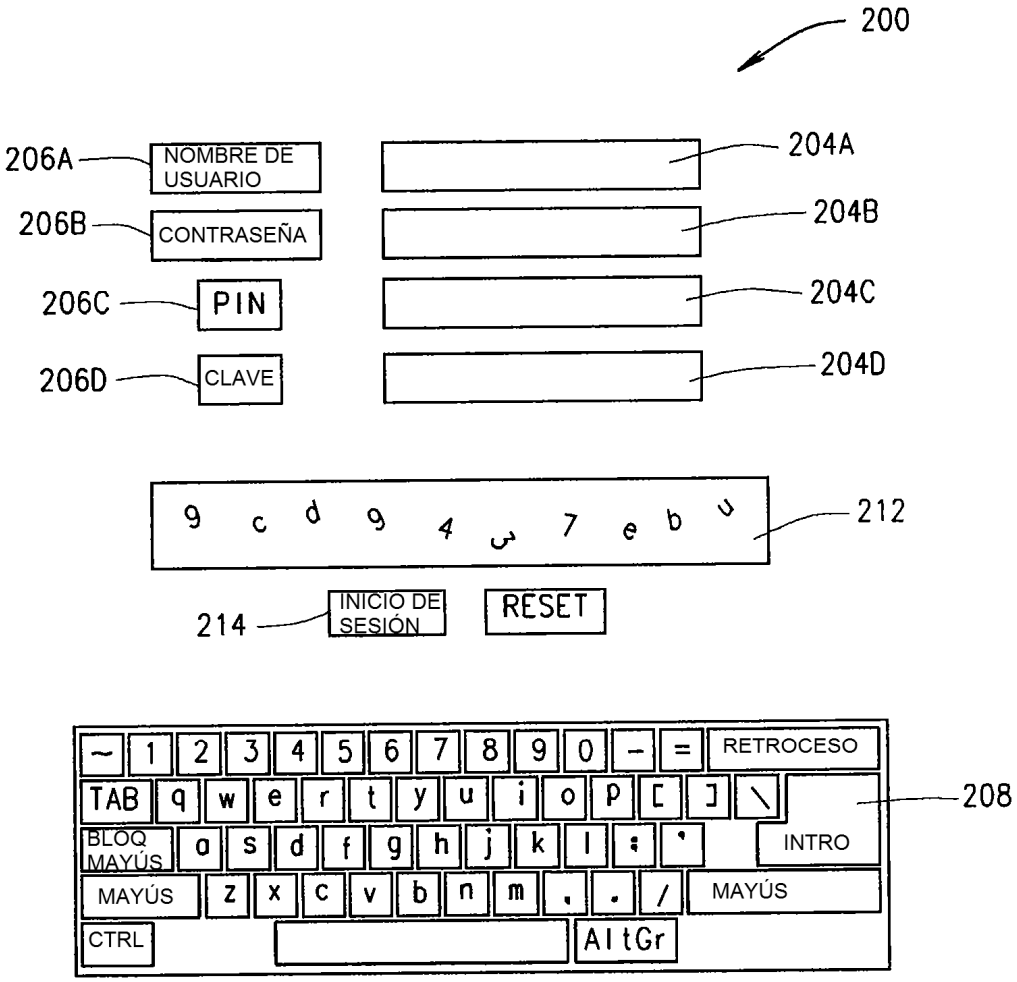
200
206A
NOMBRE DE USUARIO
204A
206B
CONTRASEÑA
204B
206C
PIN
204C
206D
CLAVE
204D
9 c d 9 4 3 7 e b v
212
214
INICIO DE SESIÓN
RESET
~ 1 2 3 4 5 6 7 8 9 0 - = RETROCESO
TAB q w e r t y u i o p [ ] \
BLOQ MAYÚS a s d f g h j k l ; '
INTRO
MAYÚS z x c v b n m , . / MAYÚS
CTRL
AltGr
208

FIG. 3