(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 669 536**

(51) Int. CI.:

G06F 21/46 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.02.2013 E 13155372 (9)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 2767922**

(54) Título: **Sistema de auditoría de contraseñas**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.05.2018

(73) Titular/es:

PRAETORS AG (100.0%)
Obere Allmend 12
6375 Beckenried, CH

(72) Inventor/es:

ENACHE, COSTIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de auditoría de contraseñas

La presente invención se refiere a un sistema de auditoría de contraseñas para determinar la solidez de las contraseñas de usuario en un sistema, aplicación o red informáticos a la que tienen acceso una pluralidad de usuarios a través de una identificación de usuario y contraseña.

Antecedentes de la invención

Las contraseñas son el mecanismo de autenticación usado más ampliamente en entornos informáticos. En los sistemas, aplicaciones y redes informáticas mencionados anteriormente, las contraseñas se usan para proteger la identidad de los usuarios y para permitir el acceso autenticado a recursos y datos. Para la autenticación de los usuarios, sus datos de contraseña tienen que ser almacenados dentro del entorno protegido, de modo que se pueda verificar si coincide la contraseña introducida por el usuario cuando se accede al sistema. Todos de tales sistemas protegidos típicamente tienen administradores de sistema, que son usuarios privilegiados y pueden acceder a los datos sin estar limitados como lo están los usuarios normales. Técnicamente, los administradores son capaces de extraer y ver los datos de contraseña de otros usuarios.

Con el fin de evitar la exposición de las contraseñas, los sistemas informáticos normalmente implementan cifrado de contraseñas (también llamado comprobación aleatoria de contraseñas). Esta operación transforma la contraseña de usuario reales (llamada contraseña de texto plano) en datos codificados (llamada contraseña de texto cifrado). El texto cifrado se puede usar para verificar si la contraseña introducida es correcta, pero no se puede usar para determinar el texto plano, debido a que el algoritmo de cifrado empleado es una operación matemática irreversible. Cuando el usuario introduce la contraseña, el texto plano se codifica y se compara con el texto cifrado almacenado – si coincide, la contraseña es correcta.

En un compromiso típico de seguridad informática, los datos de texto cifrado llegan a estar expuestos y el atacante intenta determinar el texto plano a partir del texto cifrado, con el fin de encontrar las contraseñas reales. Como la operación matemática de codificación es irreversible, el atacante tiene que probar diferentes textos planos, codificarlos y encontrar uno que coincida con el texto cifrado. Se emplean distintas estrategias: fuerza bruta (donde se prueban todas las combinaciones de letras, números y caracteres especiales), diccionario (donde se prueban todas las palabras de una lista) y varias combinaciones basadas en las anteriores. Este proceso se llama comúnmente “recuperación de contraseña”.

Con el fin de hacer que este proceso lleve mucho tiempo, las operaciones matemáticas usadas para codificar emplean algoritmos de cifrado y comprobación aleatoria complejos. El objetivo de este diseño es proteger las contraseñas haciendo que el proceso de recuperación de contraseña lleve demasiado tiempo para ser eficaz en la recuperación de los datos de contraseña de texto plano.

En los últimos años, los ordenadores han llegado a ser más y más poderosos, siendo capaces de ejecutar mucho más rápido las operaciones de cifrado. Los algoritmos de cifrado también se han actualizado para que sean más difíciles de recuperar. El resultado de este proceso es que actualmente las contraseñas son relativamente fáciles de recuperar si la complejidad de la contraseña es baja, y de difícil a imposible si la complejidad de la contraseña es alta. Las empresas y organizaciones típicamente definen políticas de contraseñas, que especifican cuán complejas tienen que ser las contraseñas que se usan en su sistema, aplicación o red informáticos.

Distintos factores pueden conducir a la exposición de contraseñas de texto plano, tales como usar la misma contraseña de inicialización en una empresa dada cuando se crean nuevas cuentas, usar contraseñas predecibles o fáciles de recordar, usar la misma contraseña en múltiples sistemas, etc. Las empresas y organizaciones típicamente imponen sus políticas de contraseñas con el fin de evitar tal exposición. No obstante, estas políticas no se pueden hacer demasiado estrictas, debido a que entonces los usuarios comenzarán a olvidar sus contraseñas. Un sistema ideal impondría contraseñas sólidas, que son lo suficientemente complejas pero posibles de memorizar, siendo cada usuario capaz de elegir: por ejemplo, uno usará una contraseña más corta pero completamente aleatoria, mientras que otro usará una contraseña muy larga pero relativamente fácil de recordar; ambas serían suficientemente sólidas.

El gran número de ataques con éxito que eligen como objetivo contraseñas en los últimos años indica que la tecnología actual, o la forma en que se emplea, no tiene éxito en evitar el uso de contraseñas débiles y predecibles.

Básicamente, hay dos posibilidades para el propietario o el administrador, respectivamente, de un sistema, una aplicación o una red informáticos para asegurarse de que los usuarios en la empresa u organización dada usen contraseñas sólidas: en primer lugar imponiendo una política de contraseñas sólida cuando se cambia la contraseña, y en segundo lugar comprobando activamente las contraseñas de texto cifrado almacenadas para identificar las contraseñas débiles y predecibles. El primer método proporciona la protección más básica, pero muy a menudo no es eficaz, en la medida que los usuarios intentarán usar contraseñas fáciles de memorizar, incluso con una política sólida. El segundo método podría compensar las debilidades del primero, simulando activamente un ataque real y detectando, de esta manera, cualquier contraseña débil o predecible de los usuarios. No obstante, este método a

menudo no se puede emplear debido a restricciones legales, debido a que revela las contraseñas de texto plano al administrador de sistema, o al menos hace posible tal revelación. Esto se considera como que contraviene la protección de privacidad de datos y, por lo tanto, es ilegal en la mayoría de los países.

El documento US2005/0198537A1 proporciona una técnica para evaluar contraseñas.

Es el objeto subyacente de la invención proporcionar un sistema que permita determinar la solidez de las contraseñas de usuarios y proporcionar esta información al administrador del sistema, aplicación o red informáticos, sin revelar las contraseñas en sí mismas al administrador o a cualquier otra persona.

Compendio de la invención

Según la presente invención, este problema se resuelve mediante un sistema de auditoría de contraseñas como se ha mencionado al principio. La invención es como se define en las reivindicaciones adjuntas.

El sistema de auditoría de contraseñas inventivo es una entidad física separada, que recupera los datos de texto cifrado del sistema para ser auditados, realiza un proceso de recuperación de contraseñas como se conoce de manera general a partir de la técnica y almacena solamente la información pertinente relativa a la solidez de las contraseñas, de modo que esta información se pueda proporcionar a y evaluar por el administrador o propietario, respectivamente, del sistema informático. No obstante, las contraseñas de usuarios no están comprometidas, debido a que las contraseñas de texto plano recuperadas no son accesibles en ningún momento.

Para asegurar la protección de privacidad mediante el sistema de auditoría de contraseñas, es más preferido si el sistema se configura de manera que una contraseña de texto plano para la que se ha encontrado una coincidencia no se almacena en los medios de almacenamiento de datos, o solamente se almacena de una forma que no sea asignable a la identificación del usuario correspondiente. En el primer caso, la contraseña de texto plano se descarta instantáneamente después de que se haya identificado y se hayan almacenado los datos relativos a su solidez, de modo que cualquier acceso al texto plano en sí mismo es imposible. En el segundo caso, la contraseña de texto plano se almacena, pero no de una forma personalizada, por ejemplo, añadiéndola a un diccionario usado para el proceso de recuperación de contraseña, para hacer que este proceso sea más eficaz para futuras auditorías.

En una realización preferida, el sistema se configura para generar una lista que comprende las identificaciones de usuario y los valores asignados relativos a la solidez de las contraseñas de usuario. Esta lista se puede generar a partir de los datos almacenados relativos a la solidez de las contraseñas, después de la terminación del proceso de recuperación de contraseña o en cualquier punto posterior en el tiempo. Los valores asignados a cada identificación de usuario pueden ser binarios en el caso más simple, es decir, el valor es “débil” si se ha encontrado una coincidencia por el proceso de recuperación de contraseñas dentro del tiempo predeterminado y, de otro modo, el valor es “sólido”. Además, el valor puede estar en una escala numérica, en donde las contraseñas débiles se clasifican además según lo rápido que se encontró una coincidencia.

Se ha de señalar que el valor relativo a la solidez de una contraseña es dependiente del tiempo predeterminado que se da para el proceso de recuperación de contraseña. Se prefiere si la duración de este tiempo se puede variar por el administrador de sistema, dependiendo del nivel deseado de seguridad de la contraseña en la empresa u organización.

El valor relativo a la solidez de las contraseñas de usuario también puede tener en cuenta una política de contraseñas dada del sistema, aplicación o red informáticos. Tal política puede prescribir, por ejemplo, que una contraseña debería tener una longitud mínima, constar de diferentes tipos de caracteres (letras, números, etc.), o no ser una palabra conocida de un diccionario. El sistema inventivo puede analizar las contraseñas recuperadas en vista de esta política y asignar un valor que indique una contraseña más débil si no se cumplen una o más disposiciones. Alternativamente o además, la lista puede incluir también una información explícita acerca de cuáles de las disposiciones no se cumplen por la contraseña.

La interfaz del sistema inventivo está configurada preferiblemente para proporcionar la lista generada al sistema, aplicación o red informáticos a través de la conexión de datos. Allí, se puede acceder por el administrador de sistema y llevarla a cualquier formato deseado. En base a esta información, el administrador u otra persona autorizada en nombre de la empresa u organización puede tomar medidas preventivas para aumentar la seguridad de la contraseña, en particular informando a los usuarios con contraseñas débiles y pidiéndoles que cambien su contraseña según la política de contraseñas.

En otra realización de la invención, el sistema está configurado para generar un mensaje electrónico al usuario correspondiente si la solidez de su contraseña es insuficiente, es decir, si se ha recuperado dentro del tiempo predeterminado. El mensaje puede ser un correo electrónico o una información de sistema tras el próximo inicio de sesión del usuario. Tal notificación automática de los usuarios asegura que las contraseñas débiles se sustituyan tan pronto como sea posible, y también facilita el proceso para el administrador de sistema, en particular en sistemas grandes con muchos usuarios.

La interfaz es capaz preferiblemente de recuperar datos de diferentes plataformas de software que se ejecutan en el

sistema, la aplicación o la red informáticos. Esto significa que el sistema inventivo se puede emplear universalmente en conexión con diferentes plataformas tales como Microsoft Windows, Apple Mac OS X o UNIX.

Además, la unidad central de procesamiento del sistema inventivo es capaz idealmente de usar diferentes algoritmos de cifrado que se almacenan en los medios de almacenamiento de datos, dependiendo del algoritmo de cifrado usado por el sistema, la aplicación o la red informáticos. Con el fin de asegurar la compatibilidad con todos los sistemas usados comúnmente, se deberían almacenar los algoritmos de cifrado correspondientes de todos estos sistemas, en donde el algoritmo aplicable se selecciona automática o manualmente tras la configuración del sistema inventivo.

Para el proceso de recuperación de contraseña, la unidad central de procesamiento puede emplear cualquier método conocido para generar las diferentes contraseñas de texto plano. En particular, se generan por medio de uno o más diccionarios almacenados en los medios de almacenamiento de datos, y/o mediante una combinación aleatoria de caracteres (fuerza bruta). Un planteamiento común es probar primero las palabras del diccionario, luego una serie de modificaciones de las palabras del diccionario y finalmente el método de fuerza bruta. El tiempo predeterminado, que se da para el intento de recuperar cada contraseña de usuario, generalmente es suficiente para probar todas las palabras del diccionario y sus modificaciones, y para iniciar el método de fuerza bruta si los dos primeros métodos no tuvieran éxito. Si la contraseña coincidente se ha encontrado en un diccionario, esta información también se puede incluir en la lista de resultados y proporcionar al usuario respectivo, de modo que sepa la razón de por qué su contraseña es débil.

Como ya se ha mencionado anteriormente, el sistema inventivo se puede configurar para incluir contraseñas de texto plano, para las cuales se ha encontrado una coincidencia, en un diccionario. Mediante este método, las contraseñas relativamente débiles que se han recuperado mediante el método de fuerza bruta se recuperarán incluso más rápido en la próxima auditoría y se identificarán como incluso más débiles, en caso de que el mismo u otro usuario use de nuevo esta contraseña. No obstante, tiene que ser asegurado que las contraseñas añadidas al diccionario no estén asignadas a usuarios específicos, y que no se puedan acceder desde fuera del sistema inventivo.

Con el fin de aumentar la potencia de cálculo del sistema inventivo para generar las diferentes contraseñas de texto plano y codificarlas en contraseñas de texto cifrado, se prefiere si el sistema comprende además un coprocesador para soportar las funciones de la unidad central de procesamiento. En particular, las unidades de procesamiento gráfico (GPU) se pueden usar ventajosamente como coprocesadores, ya que son muy potentes en la recuperación de contraseñas.

En otra realización preferida de la invención, el sistema de auditoría de contraseñas comprende además uno o más sensores para detectar impactos físicos sobre la carcasa, tales como vibración, inclinación o choque. En la medida que la carcasa no se pretende que sea abierta durante la configuración y la operación normal del sistema inventivo, cualquier intento de abrirla se puede considerar como una intervención no autorizada, contra la cual se deberían tomar medidas de protección.

Preferiblemente, el sistema inventivo se puede configurar (después de que se haya colocado y conectado al sistema informático) para apagarse y evitar cualquier acceso a los datos almacenados si se detecta un impacto físico en la carcasa. Más preferiblemente, los datos almacenados se eliminan en tal caso, lo cual proporciona el nivel más alto de protección contra cualquier intento de acceder a datos de contraseña almacenados por el sistema.

De manera similar, el sistema inventivo también se puede configurar para apagarse y evitar cualquier acceso a los datos almacenados si se detecta un acceso no autorizado a través de la interfaz. Es decir, el sistema de auditoría de contraseñas también se protege a sí mismo contra ataques lógicos a través del sistema, la aplicación o la red informáticos.

Breve descripción de los dibujos

Estas y otras ventajas de la invención se explicarán en conexión con las siguientes realizaciones preferidas, haciendo referencia a las figuras.

Las figuras muestran:

FIG. 1: una ilustración esquemática del despliegue de un sistema de auditoría de contraseñas inventivo en una configuración de agrupación; y

FIG. 2: una ilustración esquemática de los componentes de un sistema de auditoría de contraseñas inventivo.

Descripción detallada de la invención

El sistema de auditoría de contraseñas inventivo se puede desplegar en una configuración de agrupación dentro de una red de cliente típica, donde residen los operadores del sistema de auditoría de contraseñas y del objetivo de la auditoría. Una configuración ejemplar de tal agrupación se muestra esquemáticamente en la Figura 1.

En esta configuración, una consola 1-1 de operador está conectada a través de una red 1-3 de auditoría a varios objetivos 1-2 para la auditoría de contraseñas, es decir, sistemas, aplicaciones o redes informáticos. También conectados a través de la red 1-3 de auditoría están múltiples ejemplos del sistema 1-4 de auditoría de contraseñas inventivo, comprendiendo una unidad 1-5 maestra/controladora y varias unidades 1-6 esclavas, que cooperan en la realización de las operaciones descritas a continuación. Esta configuración permite un escalado del sistema 1-4 inventivo, en donde los múltiples ejemplos 1-5 y 1-6 realizan operaciones simultáneas al auditar uno o más de los objetivos 1-2.

Una ilustración esquemática de un sistema de auditoría de contraseñas inventivo o un ejemplo del mismo, respectivamente, se muestra en la Figura 2 como realización ejemplar. Este sistema comprende una carcasa 2-1, que encierra los siguientes componentes: una unidad 2-2 central de procesamiento, un coprocesador 2-3 que es una unidad de procesamiento gráfico (GPU) como acelerador de cifrado, un sensor 2-4 de impacto físico, un sensor 2-5 de intrusión de carcasa, un módulo de plataforma de confianza (TPM) 2-6, discos duros como medios de almacenamiento de datos que comprenden un almacenamiento 2-7 cifrado, un almacenamiento 2-8 sin cifrar y un módulo de actualización, así como una interfaz para establecer una conexión de datos a un sistema, aplicación o red informáticos y una interfaz para establecer una conexión de datos a una red de auditoría según la Figura 1.

El sistema inventivo es una entidad separada del sistema, la aplicación o la red informáticos a ser auditado. Cualquier intento de abrir o acceder a la carcasa 2-1 durante la operación del sistema será detectado por los sensores 2-4 y 2-5, conduciendo al apagado del sistema y la prevención de cualquier acceso a los datos almacenados. Además, el sistema de auditoría de contraseñas almacena todos los datos de la aplicación y del usuario, incluyendo información operacional y de personalización, solamente en un formato cifrado, que proporciona una protección adicional contra cualquier revelación de datos sensibles, en particular de datos de contraseñas.

Las operaciones que se realizan por el sistema inventivo, según la realización descrita en la presente memoria, se pueden resumir como sigue:

- En la puesta en marcha, el sistema primero emplea funciones de TPM con el fin de asegurar que el entorno de software y de hardware no haya sido saboteado mientras el sistema no estaba encendido; si se ha detectado un sabotaje, el sistema no se iniciará;

- después de que se ha superado con éxito la prueba de sabotaje, el sistema recupera del TPM la primera mitad de la clave de cifrado (clave de hardware) usada para protección de almacenamiento de datos y sugiere al operador la segunda mitad;

- después de que el operador proporciona la segunda mitad de la clave (clave de usuario), se combina con la clave de hardware y el resultado se usa para descifrar el almacenamiento e iniciar el sistema operativo y el software de la aplicación; el sistema ahora está operativo;

- el sistema inicia las aplicaciones que monitorizan el entorno: se monitorizan los ataques lógicos y la intrusión de hardware, y si se detecta, el evento se registra y se apaga el sistema;

- el operador del sistema ahora puede autenticar y usar la funcionalidad del sistema: después de que el sistema se ha inicializado, el operador puede definir objetivos para la auditoría de contraseñas; el sistema almacenará la información y, en el tiempo programado, realizará la operación de auditoría, entonces generará un informe e informará al operador o a otros usuarios definidos;

- el operador del sistema primero define un nuevo objetivo para la auditoría de contraseñas, especificando la dirección de red, el tipo de sistema, el método de recuperación de contraseñas de texto cifrado; se verifica la información y se guarda el objetivo;

- el operador del sistema entonces define una nueva operación de auditoría, especificando el objetivo, los detalles de la auditoría, tales como qué diccionarios han de ser usados, si ha de ser empleada aceleración de GPU, cuánto debería ser el tiempo predeterminado para encontrar una coincidencia y cuál es la política de contraseñas; el operador también especifica cuándo tendrá lugar la auditoría y si se repite sobre una base regular, quién debería ser informado acerca de los resultados, y si los usuarios afectados por contraseñas débiles deberían ser informados automáticamente; se guarda la información del proceso de auditoría;

- en el tiempo programado, el sistema iniciará la operación de auditoría recuperando las contraseñas de texto cifrado del objetivo, iniciará el proceso de recuperación de contraseñas como se define por los parámetros del operador y esperará hasta su terminación; se evaluará cualquier contraseña débil detectada, determinando por qué se encontró la contraseña y por qué es débil la contraseña (por ejemplo, la contraseña es demasiado corta o está presente en un diccionario); los datos relacionados con la solidez de la contraseña se guardan junto con la identificación de usuario, mientras que la contraseña de texto plano en sí misma no se guardará en conexión con el usuario;

- después de la terminación del proceso de auditoría, el sistema genera un informe con los resultados,

incluyendo una lista con las identificaciones de usuario afectadas y un valor relativo a la solidez de las contraseñas detectadas; el informe se envía o se pone a disposición del operador del sistema; opcionalmente, si se elige, los usuarios afectados son informados automáticamente por correo electrónico;

- después de la generación del informe, se destruyen todas las contraseñas de texto cifrado recuperadas; el informe permanece en el almacenamiento;

- se pueden definir múltiples objetivos y operaciones de auditoría en el mismo sistema de auditoría de contraseñas; los objetivos pueden ser diferentes, correspondientes a sistemas, aplicaciones y redes informáticos de varios proveedores diferentes, incluyendo aplicaciones personalizadas.

Lista de números de referencia

1-1	consola de operador
1-2	objetivos (sistemas, aplicaciones o redes informáticos)
1-3	red de auditoría
1-4	sistema de auditoría de contraseñas
1-5	unidad maestra/controladora
1-6	unidades esclavas
2-1	carcasas
2-2	unidad central de procesamiento
2-3	coprocesador (unidad de procesamiento gráfico)
2-4	sensor de impacto físico
2-5	sensor de intrusión de carcasa
2-6	módulo de plataforma de confianza (TPM)
2-7	almacenamiento cifrado (disco duro)
2-8	almacenamiento sin cifrar (disco duro)
2-9	módulo de actualización (disco duro)
2-10	interfaz a sistema, aplicación o red informáticos
2-11	interfaz a red de auditoria

REIVINDICACIONES

1. Un sistema de auditoría de contraseñas para determinar la solidez de las contraseñas de usuarios en un sistema, aplicación o red informáticos al que tienen acceso una pluralidad de usuarios a través de una identificación de usuario y contraseña, comprendiendo el sistema de auditoría de contraseñas:

- una interfaz para establece una conexión de datos entre el sistema de auditoría de contraseñas y el sistema, la aplicación o la red informáticos, estando configurada para recuperar contraseñas de usuario de texto cifrado almacenadas en el sistema, la aplicación o la red informáticos;

- una unidad central de procesamiento, estando configurada para generar sucesivamente diferentes contraseñas de texto plano por medio de uno o más diccionarios y mediante combinaciones aleatorias de caracteres, codificar las contraseñas de texto plano en contraseñas de texto cifrado correspondientes con un algoritmo de cifrado, y comparar las contraseñas de texto cifrado codificadas con una dada de las contraseñas de texto cifrado recuperadas, hasta que se encuentre una coincidencia o haya transcurrido un tiempo predeterminado; y

- medios de almacenamiento de datos para almacenar datos relativos a la solidez de cada una de las contraseñas de usuario, siendo la solidez dependiente del método empleado para generar las diferentes contraseñas de texto plano y el tiempo necesario para encontrar una coincidencia, en donde la unidad central de procesamiento está configurada además para descartar instantáneamente cada contraseña de usuario para la cual se ha encontrado una coincidencia,

en donde los componentes del sistema de auditoría de contraseñas están encerrados en una carcasa que está separada del sistema, aplicación o red informáticos.

2. El sistema de la reivindicación 1, en donde el sistema está configurado para generar una lista que comprende las identificaciones de usuario y los valores asignados relativos a la solidez de las contraseñas de usuario.

3. El sistema de la reivindicación 2, en donde el valor relativo a la solidez de las contraseñas de usuario también tiene en cuenta una política de contraseñas dada del sistema, aplicación o red informáticos.

4. El sistema de la reivindicación 2 o la reivindicación 3, en donde la interfaz está configurada para proporcionar la lista generada al sistema, aplicación o red informáticos a través de la conexión de datos.

5. El sistema de una cualquiera de las reivindicaciones precedentes, en donde el sistema está configurado para generar un mensaje electrónico al usuario correspondiente si la solidez de su contraseña es insuficiente.

6. El sistema de una cualquiera de las reivindicaciones precedentes, en donde la unidad central de procesamiento es capaz de usar diferentes algoritmos de cifrado que se almacenan en los medios de almacenamiento de datos, dependiendo del algoritmo de cifrado usado por el sistema, aplicación o red informáticos.

7. El sistema de cualquiera de las reivindicaciones precedentes, en donde el sistema está configurado para incluir contraseñas de texto plano, para las cuales se ha encontrado una coincidencia, en un diccionario.

8. El sistema de una cualquiera de las reivindicaciones precedentes, comprendiendo además uno o más sensores para detectar impactos físicos en la carcasa, tales como vibración, inclinación o choque, en donde el sistema se puede configurar para apagarse y evitar cualquier acceso a los datos almacenados si se detecta un impacto físico en la carcasa.

9. El sistema de una cualquiera de las reivindicaciones precedentes, en donde el sistema se puede configurar para apagarse y evitar cualquier acceso a los datos almacenados si se detecta un acceso no autorizado a través de la interfaz.

10. Un método para determinar la solidez de las contraseñas de usuario en un sistema, aplicación o red informáticos a los que tienen acceso una pluralidad de usuarios a través de una identificación de usuario y contraseña, comprendiendo el método:

- recuperar contraseñas de usuario de texto cifrado almacenadas en el sistema, aplicación o red informáticos;

- generar sucesivamente diferentes contraseñas de texto plano por medio de uno o más diccionarios y mediante combinaciones aleatorias de caracteres, codificar las contraseñas de texto plano en contraseñas de texto cifrado correspondientes con un algoritmo de cifrado, y comparar las contraseñas de texto cifrado codificadas con una dada de las contraseñas de texto cifrado recuperadas, hasta que se encuentre una coincidencia o haya transcurrido un tiempo predeterminado; y

- almacenar datos relativos a la solidez de cada una de las contraseñas de usuario, siendo la solidez dependiente del método empleado para generar las diferentes contraseñas de texto plano y el tiempo necesario para encontrar una coincidencia, y descartar instantáneamente cada contraseña de usuario para

la cual se ha encontrado una coincidencia.

11. El método de la reivindicación 10, comprendiendo además generar una lista que comprende las identificaciones de usuario y los valores asignados relativos a la solidez de las contraseñas de usuario.

12. El método de la reivindicación 11, en donde el valor relativo a la solidez de las contraseñas de usuario también tiene en cuenta una política de contraseñas dada del sistema, aplicación o red informáticos.

13. El método de la reivindicación 11 o la reivindicación 12, comprendiendo además proporcionar la lista generada al sistema, aplicación o red informáticos a través de la conexión de datos.

14. El método de una cualquiera de las reivindicaciones 10 a 13, comprendiendo además generar un mensaje electrónico al usuario correspondiente si la solidez de su contraseña es insuficiente.

15. El método de una cualquiera de las reivindicaciones 10 a 14, comprendiendo además incluir contraseñas de texto plano, para las cuales se ha encontrado una coincidencia, en un diccionario.

FIG. 1

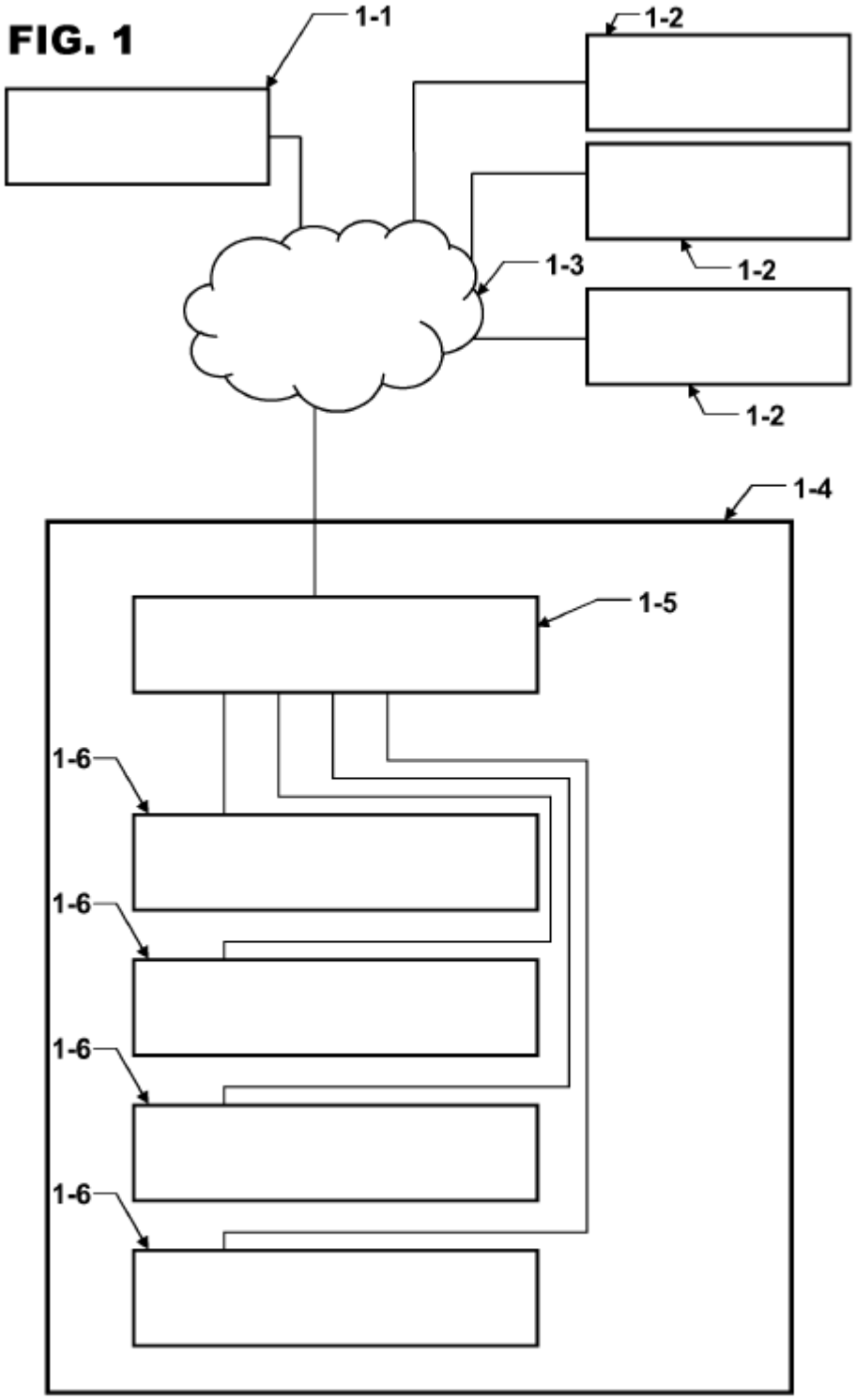

FIG. 2