(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 027**

(51) Int. CI.:

H04L 29/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.06.2002 E 02741045 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 1405482**

(54) Título: **Proximidad temporal para verificar proximidad física**

(30) Prioridad:

28.06.2001 US 894391

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.04.2013

(73) Titular/es:

KONINKLIJKE PHILIPS ELECTRONICS N.V. (100.0%)
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN, NL

(72) Inventor/es:

EPSTEIN, MICHAEL

(74) Agente/Representante:

ZUAZO ARALUZE, Alexander

DESCRIPCIÓN

Proximidad temporal para verificar proximidad física

Antecedentes de la invención

1. Campo de la invención

Esta invención se refiere al campo de la protección de datos, y en particular a proteger datos de la copia ilícita desde una ubicación remota.

2. Descripción de la técnica relacionada

La protección de datos se está volviendo un área de seguridad cada vez más importante. En muchas situaciones, la autoridad para copiar o procesar de otro modo información está correlacionada con la proximidad física de la información al dispositivo que está efectuando la copia u otro procesamiento. Por ejemplo, las representaciones de audio y vídeo se graban en CD, DVD y similares. Si una persona adquiere un CD o DVD, la persona tiene tradicionalmente el derecho de copiar o procesar de otro modo el material, con fines de copia de seguridad, facilitar su uso, etc. Cuando la persona que adquirió el material desea usar el material, no es poco razonable suponer que la persona tenga el CD o DVD dentro de la proximidad física del dispositivo que usará el material. Si, por otro lado, la persona no tiene la propiedad apropiada del material, es probable que la persona no tenga posesión física del material, y por lo tanto, el material estará situado de manera físicamente remota con respecto al dispositivo que pretende usar el material. Por ejemplo, la copia o reproducción ilícita de material a partir de un sitio de internet u otra ubicación remota corresponde a material que está situado de manera físicamente remota con respecto al dispositivo que se usa para copiar el material.

De manera similar, los sistemas de seguridad están configurados a menudo para verificar la información asociada con un usuario, tal como verificar parámetros biométricos, tales como huellas dactilares, escáneres de pupila, y similares. En un ejemplo más simple, los sistemas de seguridad están configurados a menudo para procesar información proporcionada por un usuario, tal como información contenida en una etiqueta de identificación, tarjeta inteligente, etc. Generalmente, la información o los parámetros pueden proporcionarse fácilmente por un usuario autorizado, debido a que el usuario autorizado está en posesión de los medios que contienen la información. Por otro lado, un usuario no autorizado a menudo no tendrá los medios originales que contienen la información de verificación, pero puede tener un sistema que pueda generar/regenerar la información o los parámetros de seguridad desde una ubicación remota.

De manera similar, algunos sistemas, tales como una LAN de oficina, u ordenadores en un laboratorio, están configurados para protegerse controlando el acceso físico a terminales que se usan para acceder al sistema. Si el usuario tiene acceso al sistema, se supone que el usuario está autorizado para acceder al sistema. A veces se emplean algunas medidas de seguridad, tales como una verificación de identificación, pero normalmente no tan exhaustivamente como las medidas de seguridad para los sistemas que carecen de aislamiento físico.

El documento FR 2781076 describe un sistema de bloqueo para un coche que realiza autentificación. Se mide el tiempo de una señal de respuesta de un identificador, tiempo que debe ser muy corto para asegurarse de que el identificador está dentro de unos pocos metros del vehículo.

Breve sumario de la invención

Es un objeto de esta invención proporcionar un sistema o método para impedir el uso de material en ausencia del indicio de que el material está en posesión física del usuario. Es un objeto adicional de esta invención impedir el uso de material en presencia del indicio de que el material está situado de manera remota con respecto al dispositivo que pretende usar el material. Es un objeto adicional de esta invención impedir el acceso a sistemas en presencia del indicio de que el usuario está situado de manera remota con respecto al sistema.

Estos objetos y otros se logran proporcionando un sistema de seguridad tal como se define en la reivindicación 1. Generalmente, la proximidad física corresponde a la proximidad temporal. Si el tiempo de respuesta indica un retraso sustancial o anómalo entre solicitud y respuesta, el sistema supone que el retraso está provocado por la solicitud y la respuesta que tienen que desplazarse una distancia física sustancial o anómala, o provocado por la solicitud que se procesa para generar una respuesta, en lugar de contestarse por una respuesta existente en la posesión física de un usuario. Si se detecta un retraso sustancial o anómalo, el sistema está configurado para limitar el acceso posterior al material protegido por el usuario actual, y/o notificar al personal de seguridad del retraso de respuesta anómalo.

Breve descripción de los dibujos

La invención se explica en más detalle, y a modo de ejemplo, con referencia al dibujo adjunto en el que:

la figura 1 ilustra un sistema de acceso de control de ejemplo según esta invención.

En todo el dibujo, los mismos números de referencia indican características o funciones similares o correspondientes.

Descripción detallada de la invención

Para facilitar la referencia y el entendimiento, la invención se presenta en el presente documento en el contexto de un esquema de protección contra copia, en el que el procesamiento de material protegido contra copia se controla a través de una verificación en la que el usuario del material está en posesión física del material protegido contra copia.

La figura 1 ilustra un sistema 100 de acceso de control de ejemplo según esta invención. El sistema 100 de acceso de control incluye un procesador 120 que está configurado para procesar material a partir de medios físicos, tales como un CD 130, a través de un dispositivo 132 de acceso, tal como un lector. El medio 125 de almacenamiento tal como un procesador 120 puede ser un dispositivo de grabación que graba una o más canciones desde el CD 130 en una tarjeta de memoria, en un CD recopilatorio, etc. El procesador 120 también puede ser un dispositivo de reproducción que está configurado para proporcionar una salida adecuada para la percepción humana, tal como imágenes en una pantalla, sonidos de un altavoz 127, etc. El término “reproducción” se usa en el presente documento para incluir un procesamiento, transformación, almacenamiento, etc., del material recibido por el procesador 120. Usando este contexto y terminología, el procesador 120 de ejemplo incluye un reproductor 122 que proporciona la interfaz con el dispositivo 132 de acceso, y un verificador 126 que está configurado para verificar la presencia de material 130 autorizado.

Cuando un usuario da comienzo a la reproducción de material a partir de los medios 130, el procesador 120 está configurado para verificar la presencia de los medios 130. Un método para efectuar esta verificación es solicitar al dispositivo 132 de acceso que proporcione el indicio de que los medios 130 están disponibles para proporcionar material o información que difiere del material que el usuario está intentando reproducir. Por ejemplo, si el usuario da comienzo a la reproducción de una canción, el verificador 126 puede dirigirse al reproductor 122 para solicitar una parte de una canción diferente del dispositivo 132 de acceso. Si el dispositivo de acceso no puede proporcionar la parte solicitada de una canción diferente, el verificador 126 puede concluir que los medios 130 no están presentes realmente para la reproducción, y terminará la reproducción posterior del material que el usuario pretendió reproducir, a través de la puerta 124.

Por ejemplo, un usuario puede descargar de manera ilícita una selección de diferentes canciones protegidas contra copia desde un sitio 140 remoto en internet 144, y a continuación intentar crear un CD recopilatorio que contiene estas canciones seleccionadas por el usuario. Normalmente, el tamaño de un álbum completo de material disuade de la descarga de cada álbum que contiene las canciones seleccionadas por el usuario. Cuando el verificador 126 solicita una parte de una canción diferente del álbum correspondiente a un CD 130 real, se impedirá que el usuario que sólo descargó del álbum la canción seleccionada por el usuario reproduzca adicionalmente el material descargado.

Pueden emplearse una variedad de técnicas para garantizar que el material proporcionado en respuesta a la solicitud corresponde al material que está contenido en el CD 130 real. Por ejemplo, la solicitud de patente internacional WO 01/59705 (expediente del agente US000040) enseña un conjunto de datos autorreferencial en el que cada sección de un conjunto de datos, tal como un álbum protegido contra copia, se identifica de manera unívoca mediante un identificador de sección que está asociado de manera segura con cada sección. Para garantizar que una recopilación de secciones son todas del mismo conjunto de datos, un identificador del conjunto de datos también se codifica de manera segura con cada sección. Usando un muestreo exhaustivo o aleatorio, se determina la presencia de la totalidad del conjunto de datos, o bien de manera absoluta o bien con certeza estadística, comprobando los identificadores de sección y conjunto de datos de secciones seleccionadas.

Sin embargo, puede rechazarse la verificación proporcionada por el verificador 126 tal como se describió anteriormente, respondiendo a las solicitudes del reproductor 122 del sitio 140 remoto que contiene la totalidad del álbum. Es decir, en lugar de descargar todo el álbum del sitio 140 remoto, el usuario ilícito necesita descargar sólo la canción deseada, e imitar la presencia del CD 130 real proporcionando un imitador 142 de CD que proporciona acceso al material solicitado o a partes del material solicitadas a través de internet 144. Cuando el verificador 126 solicita una parte de una canción, o sección de un conjunto de datos, el imitador 142 de CD transforma la solicitud en una solicitud de descarga del sitio 140 remoto, y se proporciona la sección solicitada al reproductor 122, como si se proporcionara del CD 130. Suponiendo que, con fines prácticos, el verificador 126 se configurara sólo para comprobar unas pocas secciones en un álbum, el uso del imitador 142 de CD dará como resultado una cantidad sustancialmente reducida de transferencia de datos, en comparación con la descarga de todo el álbum, y por tanto preferible para la descarga ilícita de canciones seleccionadas.

Según esta invención, el procesador 120 incluye un temporizador 128 que está configurado para medir el tiempo

entre una solicitud del verificador 126 y una respuesta de una fuente externa, o bien el CD 130 real, o la fuente 140 remota, para facilitar una evaluación mediante el verificador 126 de la proximidad física de la fuente de la respuesta. En una realización preferida, el verificador 126 está configurado para filtrar o promediar los tiempos de respuesta, para permitir perturbaciones menores en el tiempo de respuesta de una fuente 130 autorizada, mientras que todavía puede distinguir una respuesta de una fuente 140 físicamente remota. Por ejemplo, usando técnicas estadísticas convencionales, el verificador 126 puede continuar solicitando secciones de la fuente desconocida hasta que se detecta una diferencia estadísticamente significativa del tiempo de respuesta esperado de una fuente 130 local. En una realización más simple, si el tiempo de respuesta está por debajo de un umbral de retardo N de M veces, el verificador 126 está configurado para concluir que la fuente debe ser local. Estas y otras técnicas para evaluar la proximidad física basándose en proximidad temporal serán evidentes para un experto habitual en la técnica en vista de esta descripción.

Los principios de esta invención también son aplicables a otras aplicaciones. En una aplicación análoga, por ejemplo, el reproductor 122 y el dispositivo 132 de acceso pueden ser dispositivos de desafío-respuesta que están configurados para intercambiar claves de seguridad, usando por ejemplo, una tarjeta inteligente como los medios 130. Si un usuario no autorizado intenta intercambiar claves procesando los desafíos-respuestas a través del acceso a un sistema que puede superar potencialmente la seguridad del intercambio, el temporizador 128 podrá detectar el retraso anómalo entre el desafío y la respuesta, y terminar el intercambio de clave. De manera similar, si un sistema espera que todos los accesos sean desde terminales que están en un área protegida físicamente común, el temporizador 128 podrá detectar retrasos anómalos si el sistema se convierte en el objetivo de un “hacker” de acceso remoto u otros accesos intentados desde el exterior del área protegida físicamente.

Preferiblemente, el verificador 126 está configurado para solicitar información de fuente aleatoria. En el ejemplo de los medios 130 de CD, el verificador 126 está configurado para solicitar acceso a secciones seleccionadas aleatoriamente en los medios 130 hasta que se consigue la confianza suficiente ya sea la fuente local o remota. En otras aplicaciones, el verificador 126 está configurado simplemente para monitorizar, y contar, las transacciones que se producen de manera rutinaria entre un dispositivo 122 de solicitud y un dispositivo 132 de acceso, para detectar tiempos de respuesta largos de manera anómala. En otras aplicaciones, el verificador 126 simplemente puede controlar el orden de aparición de solicitudes de acceso a datos de rutina. Por ejemplo, cuando se lee información a partir de un dispositivo de identificación del usuario, el verificador 126 puede configurarse para a veces preguntar el nombre del usuario en primer lugar, después el número de identificación, después la huella dactilar, etc.; en una sesión posterior, el verificador 126 puede preguntar en primer lugar el número de identificación, después un reconocimiento de voz, etc., impidiendo de este modo una secuencia pregrabada de respuestas.

De manera similar, en una aplicación prevista para impedir la descarga de datos desde un sitio remoto, el verificador 126 en el ejemplo de la figura 1 puede simplemente solicitar partes de los datos solicitados en una secuencia de orden diferente, para determinar si los datos solicitados son locales o remotos. De manera similar, para impedir la descarga no autorizada de información de una red, el verificador y el tiempo pueden situarse en el sitio remoto, y configurarse para medir el tiempo de transporte de los datos. Por ejemplo, en una red convencional que tiene capacidades de detección de errores, el verificador puede configurarse para transmitir intencionadamente datos erróneos, o una secuencia errónea de datos, y medir la duración de tiempo hasta que se produce una solicitud de retransmisión. Si el sitio de recepción es local, la solicitud de retransmisión debe producirse sustancialmente más rápido que si el sitio de recepción fuera remoto. En este ejemplo, la transmisión errónea constituye una “solicitud” de una “respuesta” del sistema de recepción. Estos y otros esquemas de temporización serán evidentes para un experto habitual en la técnica.

Lo anterior simplemente ilustra los principios de la invención. Por tanto se apreciará que los expertos en la técnica puedan concebir diversas disposiciones que, aunque no se describan o muestren explícitamente en el presente documento, implementan los principios de la invención y por tanto están dentro de su alcance. Por ejemplo, aunque la invención se presenta en el contexto de detectar respuestas que son bajas de manera anómala, los principios de la invención pueden aplicarse también para detectar respuestas que son rápidas de manera anómala. Por ejemplo, si un sistema está configurado para leer información a partir de una banda magnética en una tarjeta, existe un retraso esperado asociado con el paso de la tarjeta. Si la información se proporciona sin este retraso, por ejemplo, de un ordenador que está configurado para evitar el lector de banda magnética, puede garantizarse una alerta de seguridad. Estas y otras características de configuración y optimización de sistema serán evidentes para un experto habitual en la técnica en vista de esta descripción, y se incluyen dentro del alcance de las siguientes reivindicaciones.

La invención puede implementarse por medio de hardware que comprende varios elementos distintos, y por medio de un ordenador programado de manera adecuada.

REIVINDICACIONES

1. Sistema (100) de seguridad que comprende:

un verificador (126) que está configurado para determinar una autorización basándose en una o más respuestas a una o más solicitudes, y

un temporizador (128) que está configurado para medir tiempos de respuesta asociados con la una o más respuestas a la una o más solicitudes;

estando configurado el verificador (126) para determinar la autorización basándose al menos en parte en una evaluación de los tiempos de respuesta, en el que los tiempos de respuesta se correlacionan con una proximidad física entre una primera fuente de la una o más solicitudes y una segunda fuente de la una o más respuestas,

caracterizado porque

el sistema de seguridad comprende un procesador (120) para procesar información dependiendo de la autorización, y un dispositivo (132) de acceso configurado para ejecutar un protocolo de desafío-respuesta entre el procesador y el dispositivo de acceso para dicha determinación de la autorización, protocolo durante el que se intercambia una clave de seguridad, el temporizador (128) está configurado para medir un retraso entre un desafío enviado durante dicho protocolo y una respuesta al desafío, y

el verificador (126) está configurado para provocar que el protocolo se termine si el retraso medido difiere de un tiempo de respuesta esperado.

2. Sistema (100) de seguridad según la reivindicación 1, en el que el verificador (126) está configurado para formar la evaluación basándose en al menos uno de:

un promedio de los tiempos de respuesta,

una comparación de los tiempos de respuesta a uno o más tiempos umbral, y

una prueba estadística basándose en los tiempos de respuesta.

3. Sistema (100) de seguridad según la reivindicación 1, en el que el verificador (126) está configurado para proporcionar la una o más solicitudes, basándose en una selección aleatoria de uno o más elementos a solicitar.

4. Sistema (100) de seguridad según la reivindicación 1, en el que la evaluación de los tiempos de respuesta forma una evaluación de si la una o más respuestas se comunicaron a través de una conexión de red.

5. Sistema de seguridad según la reivindicación 1, que comprende además:

un reproductor (122) que está configurado para recibir una pluralidad de elementos de datos correspondientes a un conjunto de datos, y para producir a partir de los mismos una reproducción correspondiente a un elemento de datos seleccionado,

estando acoplado de manera operativa el verificador (126) al reproductor (122), y configurado para excluir la reproducción correspondiente al elemento de datos seleccionado dependiendo de si otros elementos de datos de la pluralidad de elementos de datos están disponibles para el reproductor (122), y

estando acoplado de manera operativa el temporizador (128) al verificador (126) y al reproductor (122), y configurado para medir tiempos de respuesta asociados con respuestas a solicitudes para los otros elementos de datos del reproductor (122).

6. Método para determinar una autorización entre un receptor y una fuente de una pluralidad de elementos de datos en un sistema (100) de seguridad, comprendiendo el método:

determinar una autorización basándose en una o más respuestas a una o más solicitudes, y

medir tiempos de respuesta asociados con la una o más respuestas a la una o más solicitudes;

determinar la autorización basándose al menos en parte en una evaluación de los tiempos de respuesta, en el que los tiempos de respuesta se correlacionan con una proximidad física entre una primera fuente de la una o más solicitudes y una segunda fuente de la una o más respuestas, estando el método caracterizado

porque comprende

procesar información dependiendo de la autorización,

ejecutar un protocolo de desafío-respuesta entre el receptor y la fuente para dicha determinación de la autorización, protocolo durante el que se intercambia una clave de seguridad,

medir un retraso entre un desafío enviado durante dicho protocolo y una respuesta al desafío, y

terminar el protocolo si el retraso medido difiere de un tiempo de respuesta esperado.

7. Método según la reivindicación 6, en el que medir el tiempo de respuesta incluye, para cada elemento de datos de un subconjunto de la pluralidad de elementos de datos:

solicitar el elemento de datos de la fuente en un primer tiempo,

recibir el elemento de datos en un receptor en un segundo tiempo, y

acumular una medida de tiempo de respuesta correspondiente a una diferencia entre el segundo tiempo y el primer tiempo; y

determinar el tiempo de respuesta basándose en la medida de tiempo de respuesta.

8. Método según la reivindicación 7, en el que la medida de tiempo de respuesta corresponde a al menos uno de:

un promedio de las diferencias entre cada tiempo segundo y primero,

un recuento basándose en una comparación de cada diferencia con uno o más tiempos umbral, y

un parámetro estadístico basándose en las diferencias.

9. Producto de programa informático dispuesto para provocar que un procesador ejecute el método según la reivindicación 6.

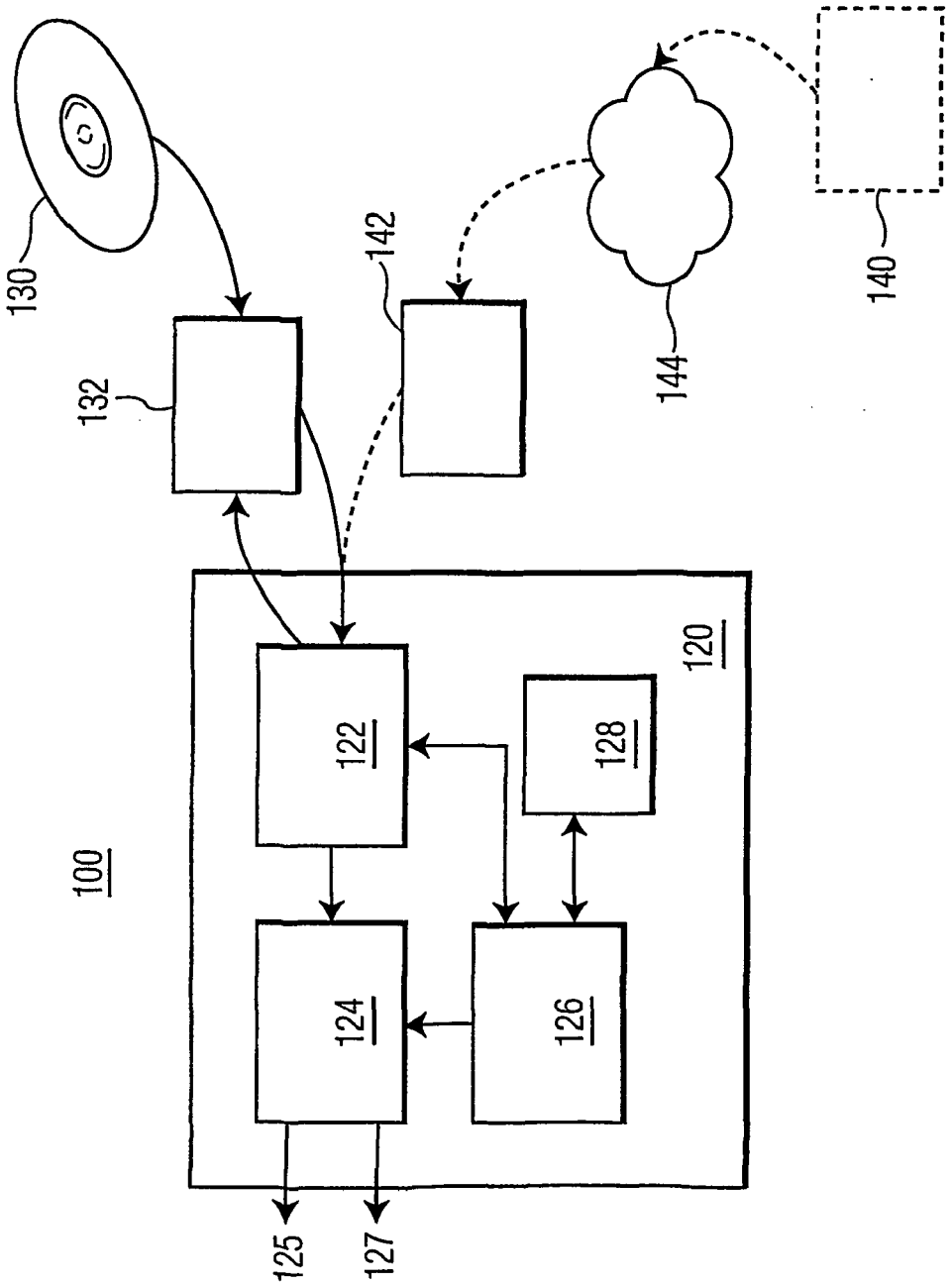

FIG. 1