(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 556 345**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/31 (2013.01)
G06F 21/44 (2013.01)
H04L 9/08 (2006.01)
H04N 7/16 (2011.01)
H04N 21/25 (2011.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.06.2010 E 10725768 (5)**

(97) Fecha y número de publicación de la concesión europea: **07.10.2015 EP 2454699**

(54) Título: **Método para detectar el uso de unidades de usuario clonadas que se comunican con un servidor**

(30) Prioridad:

15.07.2009 EP 09165496

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.01.2016

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

BAROFFIO, IVAN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para detectar el uso de unidades de usuario clonadas que se comunican con un servidor

Campo de la invención

[0001] La presente invención se refiere a un método para detectar unidades multimedia con usuarios no autorizados para compartir los derechos de acceso a un contenido distribuido por un servidor a través de una red de comunicación.
En particular, cuando se detecta una unidad no autorizada o clonada, se prevé la activación de contramedidas para limitar o deshabilitar el acceso al servidor.

Antecedentes técnicos

[0002] Desde las recientes mejoras técnicas en el ámbito de las redes de banda ancha de alto rendimiento y en los dispositivos de procesamiento de datos, se han desarrollado numerosas soluciones para luchar contra los intentos fraudulentos de acceder a los datos con contenido de carga útil disponibles en los servidores de la red.

[0003] El contenido se explota por unidades de usuario o unidades multimedia definidas aquí como ordenadores de escritorio u ordenadores portátiles personales, decodificadores de televisión digital, conjuntos de televisores, terminales inalámbricos tales como teléfonos móviles, etc. Un uso específico de cliente, como por ejemplo instalar un reproductor de contenido multimedia en la unidad de usuario para escuchar o ver contenidos de audio/video distribuidos por un servidor en la red.
El acceso condicional y el software de descodificado y/o los módulos de hardware completan el uso para asegurar el procesamiento de datos seguro en la unidad.

[0004] Las soluciones adoptadas para evitar el acceso no autorizado a los datos con contenido de carga útil en una red se basan principalmente en una autentificación mutua del la unidad de usuario con el servidor de distribución de contenido.

[0005] El documento US20070283162A1 divulga un sistema y un método para detectar un dispositivo de reproducción no autorizada.
En un servidor de gestión, una unidad de procesamiento de recepción adquiere un identificador de terminal de usuario y un primer número aleatorio de un terminal de usuario previsto para detectar un dispositivo de reproducción no autorizada.
La unidad de procesamiento de recepción determina si un segundo número aleatorio del servidor de gestión, que se almacena en una unidad de almacenamiento correspondiente al identificador del terminal de usuario, coincide con el primer número aleatorio del terminal de usuario.
Si los dos números aleatorios no coinciden, se muestra un mensaje que indica que existe un clon.
Si los dos números aleatorios coinciden, una unidad terminal generadora de información del servidor de gestión genera un nuevo número aleatorio y escribe este nuevo número aleatorio como un segundo número aleatorio en la unidad de almacenamiento.
El servidor de gestión manda el segundo número aleatorio al terminal de usuario que actualiza el primer número aleatorio de terminal de usuario al segundo número aleatorio.

[0006] El documento WO2006055545A2 divulga un sistema y un método para proporcionar comunicaciones seguras entre dispositivos de comunicación de cliente y servidores.
Un servidor genera una compensación aleatoria, altera una credencial dinámica del dispositivo de comunicación de servidor aplicando la compensación aleatoria y almacena la credencial dinámica así modificada.
El servidor manda, por medio de una red, una señal con la compensación aleatoria a un dispositivo de comunicación de cliente.
El dispositivo de comunicación de cliente devuelve al servidor una señal que incluye una credencial dinámica para verificar mediante la determinación de una diferencia entre la credencial dinámica de servidor y la credencial dinámica recibida.
Se detecta una presencia de un dispositivo de comunicaciones de cliente clonado basándose en la diferencia.

[0007] El documento WO2007096735A2 se refiere a teléfonos móviles que comprenden cada uno una señal personal o tarjeta de SIM usada para autentificarse en una red de telecomunicaciones de telefonía móvil.
La tarjeta de SIM comprende un microprocesador, una memoria, una clave secreta almacenada y un conjunto de instrucciones para el control del microprocesador realizando un cálculo de autentificación basado en un número aleatorio recibido y en la clave secreta almacenada.
La tarjeta de SIM incluye además una ubicación de memoria dedicada al almacenamiento de un valor de contador e instrucciones para que el valor de contador se desarrolle cada vez que se realice el cálculo de autentificación.
El valor de contador almacenado en la tarjeta de SIM se compara con el valor de contador tal como se ha recibido de un servidor remoto que realiza el mismo cálculo de autentificación que la tarjeta SIM.

En caso de incompatibilidad entre los dos valores de contador, la tarjeta de SIM se deshabilita y así no puede volver a conectar el teléfono móvil a la red de telecomunicaciones.

[0008] El documento US2005239440A1 divulga un sistema que comprende una pluralidad de dispositivos de cliente y un proveedor de servicios.
Un dispositivo de cliente se autentifica usando una tabla de libreta de un solo uso almacenada en el dispositivo de cliente, y una tabla de coincidencias mantenida por el proveedor de servicio.
Cuando el cliente envía una solicitud de servicio al proveedor de éste, la siguiente libreta sin usar se cambia y verifica con el estado actual de la copia de la tabla del proveedor de servicios.
Si la libreta de un solo uso es el siguiente código sin usar, el servicio es concedido incluso si el usuario se tiene que identificar a sí mismo, que cuando los resultados se completan exitosamente en el dispositivo de cliente siendo descargados con una nueva tabla de libreta de un solo uso, sustitución de la tabla comprometida.
El uso del servicio por un dispositivo clonado produce que la tabla de libreta de un solo uso se de sincronice en el proveedor de servicios con la copia autenticada del dispositivo copia de la tabla, estableciendo así la capacidad de detectar el fraude, detener el consumo de servicios por el clon, y reprogramar el dispositivo autenticado para permitir la interrupción del servicio.

[0009] En caso de interferencias en la transmisión de datos a través de la red entre el servidor y las unidades de usuario u otra corrupción de datos que proceden de errores de cálculo en un gran volumen de datos y alto rendimiento, los métodos anteriores de autenticación mutua o de detección de dispositivos clonados pueden estar faltos de eficiencia.
De hecho, una respuesta incorrecta a las solicitudes de conexión enviadas al servidor o fallos en operaciones de encriptación / desencriptación, así como la unidad de usuario del lado del servidor puede dar lugar al rechazo inesperado de unidades de usuario genuinas de la red.

Resumen de la invención

[0010] La presente invención pretende evitar el uso de dispositivos no autorizados o clonados para conectarse a los servidores de contenido, así como mejorar el rendimiento de la seguridad y la eficiencia en la transmisión de datos de gran volumen por banda ancha mediante la comprobación de la autenticidad de las unidades de usuario continuamente.
Incluso aunque ocurran interferencias o errores de transmisión; un usuario autenticado no es rechazado necesariamente gracias al uso de un procedimiento de rechazo dejando el servidor adaptarse por sí mismo a esta situación anormal.

[0011] Los objetivos se consiguen por un método para detectar la utilización de una unidad de usuario clonada que se comunica con un servidor, dicho método incluye una fase de inicialización y una fase nominal de envío de al menos una solicitud a dicho servidor y recibe al menos una respuesta del servidor, la fase de inicialización incluye las etapas de:

a) una unidad de usuario genera de manera aleatoria una clave de carga útil inicial;
b) recuperación de una clave de carga útil de una memoria de la unidad de usuario, y control del valor de dicha clave de carga útil
c) si el valor de la clave de carga útil tiene un valor predeterminado, se ajusta el valor de la clave de carga útil al valor de la clave de carga útil inicial, almacenando localmente la clave de carga útil en la memoria de la unidad de usuario, y se introduce en la fase nominal usando la clave de carga útil inicial como clave de carga útil,
d) si el valor de la clave de carga útil es diferente del valor predeterminado, se introduce en la fase nominal usando la clave de carga útil recuperada,
La fase nominal de envío de una solicitud al servidor y de recepción de al menos una respuesta del servidor incluye las etapas de:
e) preparación en la unidad de usuario de una solicitud para enviar al servidor, dicha solicitud contiene al menos un conjunto que comprende un identificador único de la unidad de usuario, datos de control y la clave de carga útil inicial, el conjunto es encriptado por una clave de transmisión primaria, y una instrucción de solicitud encriptada por la clave de carga útil,
f) desencriptación por el servidor del conjunto con la clave de transmisión primaria, obtención del identificador único de la unidad de usuario, los datos de control y la clave de carga útil inicial,
g) recuperación de la memoria del servidor de una clave de carga útil prevista y una clave de retorno que corresponde con el identificador único de la unidad de usuario, preparación de un parámetro de estado a estado correcto, y establecimiento de una clave temporal al valor de la clave de carga útil prevista,
h) desencriptación de las instrucciones de solicitud con la clave de carga útil temporal,
Si la desencriptación de las instrucciones de solicitud tiene éxito, se registrará el identificador único, los datos de control y el parámetro de estado a estado correcto en un registro del servidor,
Si la desencriptación de las instrucciones de solicitud falla, se preparará el parámetro de estado a un estado de advertencia, la clave temporal al valor de la clave de retorno y se desencriptarán las instrucciones de solicitud con la clave temporal,

Si la desencriptación de las instrucciones de solicitud con la clave temporal tiene éxito, se registrará el identificador único, los datos de control y el parámetro de estado a estado de emergencia en un registro del servidor,

Si la desencriptación de las instrucciones de solicitud con la clave temporal de la clave de retorno falla, se preparará del parámetro de estado a un estado inicial, se establecerá la clave temporal al valor de la clave de carga útil inicial y se desencriptará la instrucción de solicitud,

Si desencriptación de la instrucción de solicitud con la clave temporal tiene éxito, se registrará el identificador único, los datos de control y el parámetro de estado a estado inicial en un registro del servidor,

Si la desencriptación de las instrucciones de solicitud con la clave temporal falla, se preparará el parámetro de estado a un estado de error, se registrará el identificador único, los datos de control y el parámetro de estado a estado de error en un registro del servidor,

i) controlar el identificador único, los datos de control y el parámetro de estado en el registro del servidor,

Si el parámetro de estado está en estado de advertencia, inicial o de error, la verificación de la validez del identificador único de la unidad de usuario con los datos de control, y contramedidas de determinación o reglas predefinidas de aplicación según el resultado de la verificación,

j) de forma aleatoria se genera una nueva clave de carga útil, calculando una clave de derivación combinada con la clave temporal y la nueva clave de carga útil,

k) almacenando el identificador único, la nueva clave de carga útil como nueva clave de carga útil prevista y la clave temporal como nueva clave de retorno en la memoria del servidor,

l) enviando a la unidad de usuario una respuesta a las instrucciones de solicitud que comprende al menos datos de respuesta encriptados por la nueva clave de carga útil y la clave de derivación encriptada por una clave de transmisión secundaria,

m) en la unidad de usuario se recupera la clave de derivación mediante la desencriptación de la clave de transmisión secundaria,

n) calculando la nueva clave de carga útil por combinación de la clave de derivación y la clave de carga útil almacenada en la memoria de la unidad de usuario, desencriptando los datos de respuesta con la nueva clave de carga útil obtenida y almacenando la nueva clave de carga útil en la memoria.

[0012] Si la desencriptación de los datos de respuesta con la nueva clave de carga útil falla, calculando la nueva clave de carga útil mediante la combinación de la clave de derivación y la clave de carga útil inicial generada en la fase a), y almacenando la nueva clave de carga útil en la memoria.

[0013] A cada conexión al servidor, la unidad de usuario genera una clave inicial aleatoria y explora su memoria para encontrar una clave de carga útil almacenada tras una conexión previa al servidor.

Pueden ocurrir dos casos:

- la unidad de usuario es ya conocida por el servidor, bien por un registro precedente en una base de datos del servidor o por una conexión precedente al servidor causando el intercambio de datos con la unidad de usuario.

En este caso, el registro comprende un identificador único de la unidad de usuario, tal como un número de serie, una dirección MAC (control de acceso al medio o Media Access Control) o cualquier identificador definiendo la unidad de usuario de forma única y fiable en una red.

Por ejemplo, un teléfono móvil se identifica en la red con un identificador del dispositivo IMEI (Sistema Internacional para la Identidad de Equipos Móviles o International Mobile Equipment Identity) y un identificador IMSI (Identidad Internacional del Abonado al Móvil o International Mobile Subscriber Identity) de la tarjeta SIM para identificar al usuario.

El registro comprende además una clave de carga útil prevista y una clave de retorno.

- la unidad de usuario se desconoce o conecta desde el primer momento con el servidor.

En este caso, los registros pueden estar definidos bien por inscripción previa de un usuario interesado en beneficiarse de los servicios propuestos por el servidor o por la primera conexión al servidor mediante la recepción de una solicitud que incluye valores por defecto para el identificador y para la clave inicial.

[0014] Se establece una clave temporal en el valor de la clave de carga útil recuperada del registro del servidor o en valor de la clave inicial según los casos anteriormente mencionados que luego se usa para desencriptar las instrucciones de solicitud.

El servidor calcula luego una clave de derivación como clave de respuesta que será usada por la unidad de usuario para calcular una nueva clave de carga útil.

[0015] La clave de derivación se devuelve de forma segura, es decir, encriptada con la clave de transmisión secundaria, a la unidad de usuario, de modo que solo la unidad de usuario que conoce la clave de carga útil usada para encriptar las instrucciones de solicitud previamente enviadas es capaz de calcular la nueva clave de carga útil. Este último se almacena en el servidor y en la unidad de usuario y será usado para siguientes intercambios.

[0016] Si se hace así, la clave de carga útil se modifica preferiblemente durante cada intercambio de datos entre la unidad de usuario y el servidor, permitiendo así que el servidor compruebe en la siguiente solicitud entrante de la misma unidad de usuario si la clave de carga útil es capaz de desencriptar exitosamente las instrucciones de solicitud.

El servidor también almacena una clave de carga útil de retorno, que es la última en ser usada por la unidad de usuario.
Mediante la comprobación del parámetro de estado en desencriptación con la clave de carga útil prevista o con la clave de retorno, el servidor puede distinguir, mediante la aplicación de reglas de empresa predefinidas, comportamientos correctos o unidades de usuario autorizadas de los fallos de sistema inesperados (red, almacenamiento, interferencias, bloqueo de un conjunto de programas de aplicación, etc.) y de ataques reales de clones.

[0017] Se pueden aplicar diferentes tipos de contramedidas cuando una unidad de usuario clonada es detectada, tal como el bloqueo de acceso al servidor o deshabilitar la solicitud, servicios o recursos usados en la unidad de usuario para ver contenido proporcionado por el servidor.

[0018] Una ventaja del método es que solo es necesaria una solicitud de la unidad de usuario al servidor seguida de una respuesta de dicho servidor a la unidad de usuario para detectar una unidad de usuario clonada.

Breve descripción de las figuras

[0019] La invención se entenderá mejor con la siguiente descripción detallada, que se refiere a la figura adjunta dada como ejemplo no limitativo.
La figura 1 muestra un diagrama de bloques incluyendo los pasos de la fase de inicialización y el principio de la fase nominal donde el servidor recupera una clave de carga útil prevista y una clave de retorno de la memoria.
La figura 2 muestra un diagrama de bloques incluyendo los pasos de la fase nominal realizados para evitar el acceso de una unidad de usuario clonada al contenido en un servidor remoto que hacen diferentes pruebas para determinar si la unidad de usuario está autorizada o no.
La figura 3: muestra una forma de realización donde la respuesta del servidor incluye el parámetro de estado manejado por la unidad de usuario.

Descripción detallada de la invención

[0020] Las unidades de usuario PC tales como ordenadores de escritorio u ordenadores portátiles personales, decodificadores de televisión digital, conjuntos de televisores, terminales inalámbricos como teléfonos móviles, etc, se conectan a un servidor S mediante una red de comunicación bidireccional por cable o inalámbrica.
Cada una de las unidades de usuario PC y el servidor S tienen una memoria (MPC; MS) para almacenar claves, identificadores y otros parámetros a procesar.
Los diagramas de bloque de las figuras 1 y 2 ilustran los distintos pasos a) a n) del método según la invención con datos almacenados por la unidad de usuario y el servidor en sus respectivas memorias y el intercambio de datos entre ellos en forma de solicitud y respuesta correspondientes.

[0021] La fase de inicialización se completa por definición de una clave de transmisión Ks1 que puede ser global para todos o un grupo de acceso PC de unidades de usuario al servidor S o individuo para cada unidad de usuario.
Una clave de transmisión global se define por el servidor que la manda a una unidad de usuario cuando la inscripción de un usuario ha terminado o se puede precargar en la unidad de usuario y en el servidor de modo que el servidor no tiene a distribuirla.
Una clave de transmisión individual se define bien por el servidor o la unidad de usuario y envía a la unidad de usuario respectivamente al servidor en la inscripción de usuario y se almacena en el registro con la identificación única de la unidad de usuario UA.
Como clave de transmisión global, las claves de transmisión individual se pueden precargar en las unidades de usuario y en el servidor.

[0022] En una forma de realización preferida el valor de la clave de transmisión usado para enviar la solicitud de la unidad de usuario al servidor no es la mismo que la clave de transmisión enviada en respuesta del servidor a la unidad de usuario.
La clave de transmisión se define por lo tanto por una clave de transmisión primaria y secundaria (Ks1, Ks2).
La clave de transmisión primaria Ks1 puede ser una clave pública de un par de claves de transmisión asimétrica y la clave de transmisión secundaria Ks2 una clave privada correspondiente o viceversa.
Opcionalmente las llaves de transmisión primaria y secundaria (Ks1; Ks2) pueden tener el mismo valor cuando se trata de una clave de transmisión simétrica.

[0023] La unidad de usuario PC se inicializa en los pasos a a d generando y almacenando en la memoria MPC una clave de carga útil inicial Kip.
Esta clave Kip se puede obtener bien por generación aleatoria o por cálculo usando funciones matemáticas en valores predefinidos o tomados de una lista preprogramada.

[0024] La unidad de usuario PC recupera una clave de carga útil Kp de su memoria MPC y verifica su valor.
Pueden ocurrir dos casos:

1) el valor de la clave de carga útil Kp en la memoria MPC tiene un valor predeterminado o nulo.

Esto ocurre cuando la unidad de usuario conecta por primera vez con el servidor o cuando su memoria ha sido reiniciada de modo que todos los parámetros, llaves y datos tienen un valor predeterminado.
En este caso, el valor de la clave de carga útil Kp se fija al valor de la clave de carga útil inicial Kip previamente generada.
Esta clave de carga útil Kp se almacena luego en la memoria MPC.
2) el valor de la clave de carga útil es diferente del valor predeterminado, es decir la unidad de usuario ya ha sido conectada al servidor o ha recibido una clave de carga útil Kp de una fuente externa.

[0025] Cuando la clave de carga útil se define bien como la clave de carga útil inicial Kip o como una clave de carga útil Kp recuperada de la memoria de la unidad de usuario, la unidad de usuario entra en la fase nominal de su autentificación.

[0026] Para ser autentificado por un servidor S o reconocido como un una unidad de usuario PC genuina única en la red, la unidad de usuario PC manda una solicitud REQ al servidor S que devolverá una respuesta RES y autoriza el acceso cuando todas las operaciones de verificación han tenido éxito.

[0027] La solicitud REQ comprende una primera parte consistente en un conjunto que incluye el identificador único UA, los datos de control CD y la clave de carga útil inicial Kip, este conjunto es encriptado por una clave de transmisión primaria Ks1 conocida por el servidor S y la unidad de usuario PC y una segunda parte compuesta por unas instrucciones de solicitud Rq encriptadas por la clave de carga útil Kp.
Los datos de control CD son una cadena de bits, una asimilación o una huella digital obtenida aplicando resumen criptográfico u otra función matemática en atributos como el identificador único UA, fuente, configuración de hardware y software, versión de software, etc. de la unidad de usuario permitiendo al servidor S reconocer la unidad de usuario mediante la realización de una verificación basada en esos atributos.

[0028] La clave de transmisión Ks puede ser cualquiera de tipo simétrico o asimétrico en cuyo caso cada unidad de usuario PC almacena su clave privada y clave pública del servidor S mientras el servidor almacena su clave privada y las claves públicas que se corresponden con cada unidad de usuario enumerada en los registros por el identificador único UA.
Las claves simétricas pueden ser únicas para una unidad de usuario dada o globales para todos o un grupo de unidades de usuario.

[0029] La solicitud REQ = [UA, CD, Kip]Ks, [Rq]Kp así obtenida se envía al servidor S, (paso e) que desencripta el conjunto [UA, CD, Kip] con la clave de transmisión Ks1 para obtener el identificador único UA, los datos de control CD y la clave de carga útil inicial Kip (paso e).

[0030] El identificador único UA es usado por el servidor S para recuperar de su memoria MS una clave de carga útil prevista correspondiente Kep y una clave de retorno Kfp.
El servidor S establece un valor St de parámetro de estado a un estado (OK) y una clave temporal Kt al valor de la clave de carga útil prevista Kep, (paso f).

[0031] Luego el servidor trata de desencriptar las instrucciones de solicitud [Rq]Kp con la clave temporal Kt que tiene el valor de la clave de carga útil prevista Kep (paso h).

[0032] Si la desencriptación tiene éxito, el servidor apunta en un registro el registro compuesto por el identificador único UA, los datos de control CD y el valor de parámetro de estado (OK).

[0033] Si la desencriptación de las instrucciones de solicitud Rq falla con la clave de carga útil prevista Kep, el parámetro de estado St se fija en un estado de advertencia y el servidor establece la clave temporal Kt a la clave de retorno Kfp para tratar de desencriptar las instrucciones de solicitud Rq.
Si la desencriptación tiene éxito el servidor apunta en el registro el registro compuesto por el identificador único UA, los datos de control CD y el valor de parámetro de estado (advertencia).

[0034] Si la desencriptación de las instrucciones Rq falla con la clave de retorno Kfp, el parámetro de estado St se fija a un estado inicial y la clave temporal Kt se fija al valor de la clave de carga útil inicial Kip.

[0035] El servidor trata a desencriptar las instrucciones de solicitud Rq con la clave de carga útil inicial Kip.
Si tiene éxito, el identificador único UA, los datos de control CD y el valor de parámetro de estado St (init) se anotan en el registro.

[0036] Si la desencriptación con la clave de carga útil inicial Kip falla, el parámetro de estado St se fija en un estado de error, el identificador único UA, los datos de control CD y el valor de parámetro de estado (error) St se anotan en el registro.

[0037] Antes de enviar una respuesta a la unidad de usuario, los registros son revisados para determinar si las contramedidas tienen que ser tomadas en la unidad de usuario, especialmente cuando el valor de estado registrado es diferente a OK, (etapa i).
Dependiendo del resultado de la verificación, se pueden aplicar otras reglas tales como acceso limitado a servicios específicos, tiempo de acceso limitado u otras restricciones.

[0038] El servidor verifica validez del identificador único UA basándose en los datos de control CD cuando el valor de parámetro de estado St es o bien un estado de advertencia, un estado init o un estado de error.
Si el identificador único registrado UA no da los datos de control CD correctos aplicando la función apropiada, luego la unidad de usuario PC se puede considerar como no autorizada.
Se pueden aplicar otras reglas como la reinicialización, el acceso limitado a servicios propuestos por el servidor, el registro de la unidad en una lista negra, etc.

[0039] Cuando la verificación del identificador único UA es exitoso el usuario PC unitario se puede considerar como un autorizado un o, dependiendo de las reglas predefinidas, como un unitario a observar y además pasos se realizan para suministrar una respuesta RES a la solicitud REQ y una clave de carga útil nueva Kp'.
El valor de parámetro de estado St puede ser OK, advertencia, init o error.
Una nueva clave de carga útil Kp' se genera aleatoriamente y se almacena como una nueva clave de carga útil prevista y la clave temporal Kt usada para la desencriptación de las instrucciones de solicitud Rq se almacena como clave de retorno Kfp.
Estas claves almacenadas con el identificador único UA serán luego usadas en la siguiente conexión de la unidad de usuario PC con el servidor S, paso k.

[0040] En el paso j, una clave de derivación Kd se calcula al combinar la nueva clave de carga útil Kp' y la clave temporal Kt aplicando una función matemática reversible de operación exclusiva o (XOR), por ejemplo.
El resultado así obtenido Kd = Kt ? Kp' se encripta con una clave de transmisión secundaria Ks2 que se corresponde con la transmisión primaria Ks1 usada para el encriptado de la solicitud REQ.
La respuesta a la solicitud RES = [Kd]Ks2, [Rs]Kp' que comprende al menos la clave de derivación encriptada [Kd]Ks2 y datos de respuesta [Rs]Kp' encriptados por la nueva clave de carga útil Kp' se envía a la unidad de usuario, (paso l).
Los datos de respuesta Rs pueden comprender reglas, parámetros, o instrucciones para la unidad de usuario dependiendo de la solicitud.
La unidad de usuario finalmente desencripta la clave de derivación Kd con la clave de transmisión Ks2, (paso m), la clave de derivación Kd así obtenido se combina con la clave de carga útil Kp almacenada en la memoria del usuario unitario para obtener la nueva clave de carga útil Kp' gracias al inverso de la función o la operación XOR.

[0041] Cuando los datos de respuesta Rs se desencriptan con éxito gracias a la nueva clave de carga útil Kp', el último se almacena en la memoria MPC del usuario PC.
La nueva clave de carga útil Kp' o bien reemplaza la clave de carga útil previamente usada Kp (paso n), o bien se puede almacenar en una dirección diferente de la clave de carga útil previamente usada Kp que es luego conservada.

[0042] Si la desencriptación de los datos de respuesta (Rs) con la nueva clave de carga útil (Kp') falla, la unidad de usuario (PC) calcula una nueva clave de carga útil (Kp') para combinar la clave de derivación (Kd) con la clave de carga útil inicial (Kip).

[0043] La clave de carga útil inicial Kip que siempre se envía al servidor S en la solicitud REQ tiene una función doble: 1) clave de inicialización para inicialización de la unidad de usuario al principio de la conexión de la unidad de usuario y 2) clave de copia de seguridad o de reinicio para restaurar la conexión si falla la desencriptación de la solicitud o datos de respuesta (Rq; Rs) con una clave de carga útil Kp o Kp'.
En otras palabras, tal fallo ocurre cuando las claves de carga útil del lado de la unidad de usuario y del lado del servidor no corresponden o están desincronizadas.

1) primera inicialización de la unidad de usuario:

[0044] La unidad de usuario genera una clave inicial Kip que también se usa como clave de carga útil Kp en la solicitud REQ = [UA, CD, Kip]Ks, [Rq]Kp.
La desencriptación con la clave temporal Kt establecida en la clave de carga útil prevista Kep y en la clave de carga útil de plan Kfp recuperada de la memoria del servidor falla con el identificador único UA de la unidad de usuario PC.
No obstante, la desencriptación con la clave temporal Kt establecida en la clave de carga útil inicial Kip tiene éxito y el parámetro de estado tiene un valor init.
En este caso, después del análisis de las registros anotados y si las reglas lo permiten, el proceso continúa de los pasos j a n. Una nueva clave de carga útil Kp' se genera aleatoriamente por el servidor en el paso j y se usa para calcular la clave de derivación Kd que se envía a la unidad de usuario PC en la respuesta RES.
El usuario unitario combina la clave de carga útil Kp con esta clave de derivación Kd para determinar la nueva clave de carga útil Kp'.

Así, la unidad de usuario PC y el servidor tienen la misma clave de carga útil Kp' en su memoria y se sincronizan de modo que en la siguiente conexión con el servidor el valor de parámetro de estado sea OK si no ocurren otros errores.
En la siguiente solicitud para acceder al servidor se usará la nueva clave de carga útil Kp' y la unidad de usuario PC se autentificará según los pasos a) a n).
El identificador único UA de la unidad de usuario permite al servidor recuperar las llaves de carga útil almacenadas que son Kp' para la clave de carga útil prevista Kep y si es necesario la clave Kip para la clave de retorno Kfp.

2) reinicialización de la unidad de usuario

[0045] La unidad de usuario genera una clave de carga útil inicial Kip y usa la clave de carga útil Kp recuperada de la memoria de la unidad de usuario para proteger parte de la solicitud REQ = [UA, CD, Kip]Ks, [Rq]Kp.
La desencriptación con la clave temporal Kt establecida en la clave de carga útil prevista Kep y en la clave de carga útil de retorno Kfp recuperada de la memoria del servidor con el identificador único UA de la unidad de usuario PC falla.
La desencriptación con la clave temporal Kt establecida en la clave de carga útil inicial Kip también falla y el parámetro de estado tiene valor de error.
En este caso, después análisis de los registros anotados y si las reglas lo permiten, el proceso continúa de los pasos j a n. Una nueva clave de carga útil Kp' se genera aleatoriamente por el servidor en el paso j y se usa para calcular la clave de derivación Kd que se envía a la unidad de usuario PC en la respuesta RES.
La unidad de usuario combina la clave de carga útil inicial Kip con esta clave de derivación Kd para determinar la nueva clave de carga útil Kp'.
Así, la unidad de usuario PC y el servidor tienen la misma clave de carga útil Kp' en su memoria y se resincronizan de modo que para una siguiente conexión con el servidor el valor de parámetro de estado será OK si no ocurren otros errores.
En siguientes solicitudes para acceder al servidor se usará la nueva clave de carga útil Kp' y la unidad de usuario PC será autentificada según los pasos a) a n).
El identificador único UA de la unidad de usuario permite al servidor que recupere las claves de carga útil almacenada que son Kp' para la clave de carga útil prevista Kep y si es necesario la clave Kip para la clave de retorno Kfp.

[0046] En una forma de realización ilustrada por la figura 3, la respuesta RES incluye el parámetro de estado St que se puede aprovechar por la unidad de usuario según su valor.
En este caso, el parámetro de estado St es preferiblemente enviado con la clave de derivación Kd en un conjunto que se encripta con la clave de transmisión Ks2.
La respuesta RES será RES = [Kd, St]Ks2, [Rs]Kp', el parámetro de estado St es luego recuperado al mismo tiempo que la clave de derivación Kd por desencriptación con la clave de transmisión Ks2.

[0047] El servidor considera auténtica una unidad de usuario cuando todas verificaciones han tenido éxito y particularmente cuando el valor de parámetro de estado St es OK.

[0048] En el caso de una unidad de usuario clonada, ya se han hecho previamente una o más peticiones por la misma unidad de usuario y las claves de carga útil que corresponden con el identificador UA de la unidad de usuario han sido almacenadas en el registro del servidor S como claves previstas y de retorno (Kep, Kfp).
La clave de carga útil prevista almacenada Kep y clave de retorno Kfp tienen así un valor diferente del conjunto de valor predeterminado en la fase de inicialización, paso a.

[0049] Las desencriptaciones de los datos de solicitud Rq con la clave de carga útil prevista Kep y con la clave de carga útil de retorno Kfp llevan al valor de parámetro de estado St a error, de modo que el la unidad de usuario PC es considerada por el servidor como una unidad clonada y por lo tanto es rechazada, o más bien procesada, según las reglas predefinidas.

[0050] Una unidad de usuario también se puede considerar como un clon cuando el valor de parámetro de estado es init.
De hecho, una mismo unidad de usuario puede producir constantemente un valor de parámetro de estado init usando permanentemente la clave de carga útil inicial a cada conexión del servidor.
Las contramedidas CM también serán definidas según las reglas predefinidas y un análisis de las anotaciones de registro.

[0051] Cuando una unidad de usuario produce constantemente un valor de estado de advertencia también se puede considerar como un clon.
De hecho, dos unidades de usuario con el mismo identificador único UA pueden conectar alternativamente al servidor de modo que, en el paso h, en cada unitario la clave temporal Kt es siempre establecida en la clave de retorno Kfp para desencriptar exitosamente los datos de solicitud Rq mientras la desencriptación con la clave temporal Kt se establece que falla en la clave de carga útil prevista Kep.
En este caso, se pueden definir contramedidas CM por una regla apropiada.

[0052] Las contramedidas CM aplicadas en el servidor y / o en el acceso de bloque de la unidad de usuario al servidor o deshabilitando la solicitud, servicios o recursos en la unidad de usuario impidiendo por ejemplo el visionado de contenido proporcionado por el servidor.
Según una forma de realización, la transmisión de una respuesta RES del servidor S a la unidad de usuario PC está desactivada y el proceso termina en el paso i.

[0053] Otro control del identificador único UA con los datos de control CD permite también eliminar unidades de usuario no autorizadas y el proceso podría terminar en el paso i.

[0054] Según una forma de realización, cada vez que se usa la clave de retorno Kfp y el valor de parámetro de estado está en nivel de advertencia, se puede visualizar un mensaje específico en la unidad de usuario.
El servidor S también puede contar y almacenar el número de valores de estado en nivel de advertencia de cada identificador único para el funcionamiento del sistema de estadísticas y el historial.
Si el número de advertencias excede un límite predefinido durante un periodo predefinido, el servidor puede aplicar contramedidas de una manera similar a cuando una unidad de usuario clonada es detectada.

[0055] Cuando la respuesta RES incluye un valor de parámetro de estado St en error, la unidad de usuario calcula la nueva clave de carga útil Kp' para combinar la clave de derivación Kd con la clave de carga útil inicial Kip en lugar de la clave de carga útil Kp actual.
El objetivo es de obtener una clave de carga útil Kp' capaz de desencriptar los datos de respuesta Rs.
Si este nueva clave de carga útil Kp' permite la desencriptación, la unidad de usuario se puede reinicializar de modo que ésta reenciende el proceso completo usando la nueva clave de carga útil Kp' en lugar de la clave de carga útil Kp previamente usada.

[0056] Otra posibilidad es negar acceso al servidor y mostrar un mensaje de error en la unidad de usuario cuando se descubre un mensaje de error en el valor de parámetro de estado St cuando se encuentra en error tras la desencriptación con la clave de transmisión Ks2.
La desencriptación de los datos de respuesta Rs con la nueva clave de carga útil Kp' expedida de la clave de derivación Kd se vuelve en este caso facultativa.

[0057] A cada solicitud REQ le sigue una respuesta RES autorizando el acceso al servidor S, la clave de carga útil Kp se cambia y la clave de carga útil precedente se mantiene en la memoria MS del servidor S como clave de reserva (retorno) Kfp a ser recuperada en caso de corrupción de la clave de carga útil Kp actualmente usada.
Si una clave de carga útil nueva Kp' no puede ser obtenida en caso de interferencias en la respuesta de servidor, la clave de carga útil precedente Kp puede todavía usarse como clave de retorno Kfp y la clave de carga útil generada a continuación se usará para un acceso estándar al servidor.
Opcionalmente la clave de carga útil precedente Kp también se puede almacenar en la memoria de la unidad de usuario.

[0058] Según una forma de realización, el servidor S almacena todas claves de carga útil usadas por la unidad de usuario para acceder al servidor S como llaves de retorno (Kfp1,...,Kfpn). Si los datos de solicitud Rq no se pueden descifrar con la última, es decir, la clave de carga útil más reciente almacenada como clave de retorno Kfp1, el servidor ajustará la clave temporal Kt al valor de cada clave de carga útil precedente hasta que se pueda realizar una desencriptación exitosa de los datos de solicitud Rq.
En tal caso, el estado se fija al estado de advertencia como cuando se usa con éxito la clave de retorno Kfp1 más reciente.
Si ninguna de las claves almacenadas como clave de retorno es capaz de desencriptar los datos de solicitud Rq, el valor de parámetro de estado (St) se fija al estado inicial y la clave temporal (Kt) se fija al valor de la clave de carga útil inicial ().
La figura 2 muestra esta forma de realización mediante la flecha discontinua en la prueba de la clave de retorno kfp en el paso h. Los otros pasos (j a n) del método se realizan después como se ha descrito anteriormente en la forma de realización principal.

[0059] En una forma de realización, la clave de derivación Kd puede corresponder a la nueva clave de carga útil Kp' de modo que la unidad de usuario PC no realiza más cálculos para determinar la nueva clave de carga útil Kp'.
Como en la primera forma de realización, la nueva clave de carga útil Kp' y la respuesta RES son encriptadas preferiblemente por la clave de transmisión Ks2.
[0060] En otra forma de realización se puede enviar de un mensaje de reconocimiento desde la unidad de usuario PC al servidor S cuando la unidad de usuario PC recibe una respuesta del servidor S.

[0061] Según otra forma de realización al menos una de las solicitudes (REQ) enviadas desde unidad de usuario (PC) al servidor (S), la respuesta (Res) enviada desde el servidor (S) a la unidad de usuario (PC), son firmadas por la clave de carga útil (Kp) de la clave de derivación Kd.

La firma, preferiblemente encriptada por la clave de transmisión Ks1, se compone de una asimilación obtenida por ejemplo por una función libre de colisión de resumen criptográfico sobre los datos a verificar: solicitud, respuesta, clave de carga útil, clave de respuesta o clave de derivación.
Después de la desencriptación, la asimilación recibida se compara con una asimilación localmente generada y cuando la comparación tiene éxito el proceso continúa.
Por el contrario, el proceso puede o bien ser repetido desde el principio o ser detenido por el servidor que manda mensajes de error adecuados a la unidad de usuario.

[0062] El método de la invención se puede implementar en numerosas aplicaciones que requieren una autentificación de una unidad de usuario con un servidor remoto antes de acceder a servicios proporcionados por el servidor.

[0063] Por ejemplo, en la aplicación de televisión de ancho de banda vía red bidireccional cablegrafiada o inalámbrica, la solicitud enviada por la unidad de usuario (decodificador de señales digitales, ordenador personal, teléfono móvil, etc.) al servidor (extremo principal, centro de administrando, proveedor de servicios de televisión e internet, etc.) comprende en parte la clave de carga útil e instrucciones, diferentes parámetros relacionados con la solicitud televisiva.
Estos parámetros comprenden particulares de usuario, derechos de acceso a programas televisivos, canales o servicios enlazados con una suscripción adquirida por el usuario, derechos y actualización de conjunto de los programas de aplicación, etc. La respuesta devuelta por el servidor incluye datos de respuesta Rs comprendiendo la solicitud específica de parámetros solicitados tales como reconocimientos de derechos o actualizaciones, conjunto de programas de aplicación actualizados, etc.

[0064] En una forma de realización de la implementación, la autentificación y el procedimiento de detección del clon se puede establecer como preámbulo en un procedimiento de acceso de usuario más complejo que requiere un intercambio de datos adicional entre unidad de usuario y servidor.
El procedimiento de acceso se lanzará por lo tanto solo después de que la unidad de usuario haya sido reconocida por el servidor como auténtica.

REIVINDICACIONES

1. Método para detectar el uso de una unidad de usuario (PC) clonada que se comunica con un servidor (S), dicho método incluye una fase de inicialización, una fase nominal de envío de al menos una solicitud (REQ) a dicho servidor (S) y la recepción al menos una respuesta (Res) del servidor (S), la fase de inicialización incluye las etapas de:

A) generación aleatoria de una clave de carga útil inicial (Kip) por una unidad de usuario (PC);

B) recuperación de una clave de carga útil (Kp) desde una memoria (MPC) de la unidad de usuario (PC), y control del valor de dicha clave de carga útil (Kp)

C) si el valor de la clave de carga útil (Kp) es un valor predeterminado, se ajusta el valor de la clave de carga útil (Kp) al valor de la clave de carga útil inicial (Kip), almacenando localmente la clave de carga útil (Kp) en la memoria (MPC) de la unidad de usuario (PC), e introduciéndose en la fase nominal usando la clave de carga útil inicial (Kip) como clave de carga útil,

D) si el valor de la clave de carga útil (Kp) es diferente del valor predeterminado, se introduce en la fase nominal usando la clave de carga útil recuperada (Kp),

La fase nominal de envío de una solicitud (REQ) al servidor y de recepción de al menos una respuesta (Res) del servidor (S) incluye las etapas de:

E) preparación en la unidad de usuario (PC) una solicitud (REQ) para enviar al servidor (S), dicha solicitud (REQ) contiene al menos un conjunto que comprende un identificador único (UA) de la unidad de usuario (PC), datos de control (CD), y la clave de carga útil inicial (Kip), el conjunto es encriptado por una clave de transmisión primaria (Ks1), y unas instrucciones (Rq) encriptadas por la clave de carga útil (Kp),

F) desencriptación por el servidor (S) del conjunto con la clave de transmisión primaria (Ks1), obtención del identificador único (UA) de la unidad de usuario (PC), los datos de control (CD) y la clave de carga útil inicial (Kip),

G) recuperación desde la memoria (MS) del servidor (S) de una clave de carga útil prevista (Kep) y una clave de retorno (kfp) que corresponde con el identificador único (UA) de la unidad de usuario (PC), preparando un parámetro de estado (St) en estado OK, y estableciendo una clave temporal (Kt) al valor de la clave de carga útil prevista (Kep),

H) desencriptación las instrucciones de solicitud (Rq) con la clave de carga útil temporal (Kt),

Si desencriptación de las instrucciones de solicitud (Rq) tiene éxito, se accede al identificador único (UA), los datos de control (CD) y el parámetro de estado (St) a estado OK en un registro del servidor (S),

Si la desencriptación de las instrucciones de solicitud (Rq) falla, se establece el parámetro de estado (St) en estado de advertencia, fijando la clave temporal (Kt) al valor de la clave de retorno (Kfp) y desencriptando las instrucciones de solicitud (Rq) con la clave de carga útil temporal (Kt),

Si la desencriptación de las instrucciones de solicitud (Rq) con la clave de carga útil temporal (Kt) tiene éxito, se accede al identificador único (UA), los datos de control (CD) y el parámetro de estado (St) a estado de advertencia en un registro del servidor (S),

Si desencriptación de las instrucciones de solicitud (Rq) con la clave de carga útil temporal (Kt) falla, se establece el parámetro de estado (St) en estado de advertencia, fijando la clave temporal (Kt) al valor de la clave carga útil inicial (Kip) y desencriptando las instrucciones de solicitud (Rq),

Si la desencriptación de las instrucciones de solicitud (Rq) con la clave de carga útil temporal (Kt) tiene éxito, se accede al identificador único (UA), los datos de control (CD) y el parámetro de estado (St) a estado inicial en un registro del servidor (S),

Si la desencriptación de la instrucción de solicitud (Rq) con la clave de carga útil temporal (Kt) falla, se establece el parámetro de estado (St) a un estado de error, accediendo al identificador único (UA), los datos de control (CD) y el parámetro de estado (St) en estado de error en un registro del servidor (S),

I) control del identificador único (UA), los datos de control (CD) y el parámetro de estado (St) en el registro del servidor (S)

Si parámetro de estado (St) está en estado de advertencia o inicial o de error, se verifica la validez del identificador único (UA) de la unidad de usuario (PC) con los datos de control (CD), y se establecen contramedidas (CM) o reglas predefinidas de aplicación según el resultado de la verificación,

J) generación de forma aleatoria de una nueva clave de carga útil (Kp'), calculando una clave de derivación (Kd) (Kd = Kt ? Kp') mediante la combinación de la clave temporal (Kt) y la nueva clave de carga útil (Kp') aplicando una función matemática reversible ?,

K) almacenaje del identificador único (UA), la nueva clave de carga útil (Kp') como nueva clave de carga útil prevista (Kep') y la clave temporal (Kt) como nueva clave de retorno (Kfp') en la memoria (MS) del servidor (S),

L) envío a la unidad de usuario (PC) de una respuesta (Res) a la solicitud (REQ) que comprende al menos datos de respuesta (Rs) encriptados por la nueva clave de carga útil (Kp') y un conjunto (Kd; St) con la clave de derivación (Kd) y el parámetro de estado (St) asociados a la clave de derivación (Kd), el conjunto (Kd; St) es encriptado por una clave de transmisión secundaria (Ks2),

M) recuperación en la unidad de usuario (PC) de la clave de derivación (Kd) mediante la desencriptación con la clave de transmisión secundaria (Ks2),

N) cálculo de la nueva clave de carga útil (Kp') (Kp' = Kd ? Kp) mediante la combinación de la clave de derivación (Kd) y la clave de carga útil (Kp) aplicando el inverso de la función matemática ?, dicha clave de carga útil (Kp) se almacena en la memoria (MPC) de la unidad de usuario (PC), desencriptando los datos de

respuesta (Rs) con la nueva clave de carga útil (Kp') así obtenida y almacenando la nueva clave de carga útil (Kp') en la memoria (MPC).
Si la desencriptación de los datos de respuesta (Rs) con la nueva clave de carga útil (Kp') previamente obtenida falla, se calcula la nueva clave de carga útil (Kp'), (Kp' = Kd ?? Kip) mediante la combinación de la clave de derivación (Kd) y la clave de carga útil inicial (Kip) generada en el paso a) aplicando el inverso de la función matemática?, y almacenando la nueva clave de carga útil (Kp') en la memoria (MPC).

2. Método según la reivindicación 1, **caracterizado por** el hecho de que la clave de derivación (Kd) corresponde a la nueva clave de carga útil (Kp').

3. Método según las reivindicaciones 1 o 2, **caracterizado por** el hecho de que al menos una de las solicitudes (REQ) enviadas desde la unidad de usuario (PC) al servidor (S), la respuesta (Res) enviada desde el servidor (S) a la unidad de usuario (PC), la clave de carga útil (Kp), la clave de derivación (Kd) están firmadas.

4. Método según cualquiera de las reivindicaciones 1 a 3, **caracterizado por** el hecho de que cada vez que se usa la clave de retorno (Kfp) y el valor del parámetro de estado (St) está en advertencia, se visualiza un mensaje específico en la unidad de usuario (PC).

5. Método según cualquiera de las reivindicaciones 1 a 3, **caracterizado por** el hecho de que el servidor S cuenta y almacena el número de valores de estado de advertencia de cada identificador único (UA) para el funcionamiento de sistema de estadística y el historial.

6. Método según la reivindicación 5, **caracterizado por** el hecho de que el servidor aplica contramedidas de una manera similar a cuando un se detecta una unidad de usuario clonada si el número de advertencias excede un límite predefinido durante un periodo predefinido.

7. Método según la reivindicación 1, **caracterizado por** el hecho de que se envía un mensaje de reconocimiento desde la unidad de usuario (PC) al servidor (S) cuando la unidad de usuario (PC) recibe una respuesta del servidor (S).

8. Método según la reivindicación 1, **caracterizado por** el hecho de que la contramedida (CM) comprende un paso de deshabilitación de la transmisión de una respuesta (Res) desde el servidor (S) a la unidad de usuario (PC).

9. Método según la reivindicación 1, **caracterizado por** el hecho de que la unidad de usuario (PC) calcula una nueva clave de carga útil (Kp') mediante la combinación de la clave de derivación (Kd) con la clave de carga útil inicial (Kip) cuando la respuesta (Res) incluye un valor del parámetro de estado (St) de error, la unidad de usuario (PC) se reinicializa y reinicia el proceso completo usando la nueva clave de carga útil (Kp') como clave de carga útil (Kp), dicha clave de carga útil (Kp) se almacena en la memoria (MPC) de la unidad de usuario (PC).

10. Método según la reivindicación 1, **caracterizado por** el hecho de que el servidor (S) almacena todas claves de carga útil usadas por la unidad de usuario para acceder del servidor (S) como claves de retorno (Kfp1,... Kfpn).

11. Método según la reivindicación 10, **caracterizado por** el hecho de que el servidor establece la clave temporal (Kt) en el valor de cada clave de carga útil precedente hasta que una desencriptación exitosa de dichos datos de solicitud (Rq) si la desencriptación de los datos de solicitud (Rq) falla con la clave de carga útil más reciente almacenada como clave de retorno (Kfp1), el parámetro de estado (St) se establece en estado de advertencia.

12. Método según la reivindicación 11, **caracterizado por** el hecho de que el valor de parámetro de estado (St) se fija en el estado inicial y la clave temporal (Kt) se fija en el valor de la clave inicial de carga útil (Kip) si la desencriptación de los datos de solicitud (Rq) falla con cada clave de retorno almacenada.

13. Método según la reivindicación 1, **caracterizado por** el hecho de que la clave de transmisión primaria (Ks1) es una clave pública de un par de claves de transmisión asimétrica y la clave de transmisión secundaria (Ks2) es la clave privada correspondiente o viceversa.

14. Método según la reivindicación 1, **caracterizado por** el hecho de que la clave de transmisión primaria (Ks1) y la clave de transmisión secundaria (Ks2) son simétricas teniendo el mismo valor.

15. Método según las reivindicaciones 13 o 14, **caracterizado por** el hecho de que las claves de transmisión (Ks1; Ks2) son o bien globales para todas las unidades de usuario o un grupo de unidades de usuario o bien individuales para cada unidad de usuario, dichas claves de transmisión (Ks1; Ks2) son precargadas en las unidades de usuario (PC) y en el servidor (S) o definidas en una inscripción de un usuario en el servidor (S).

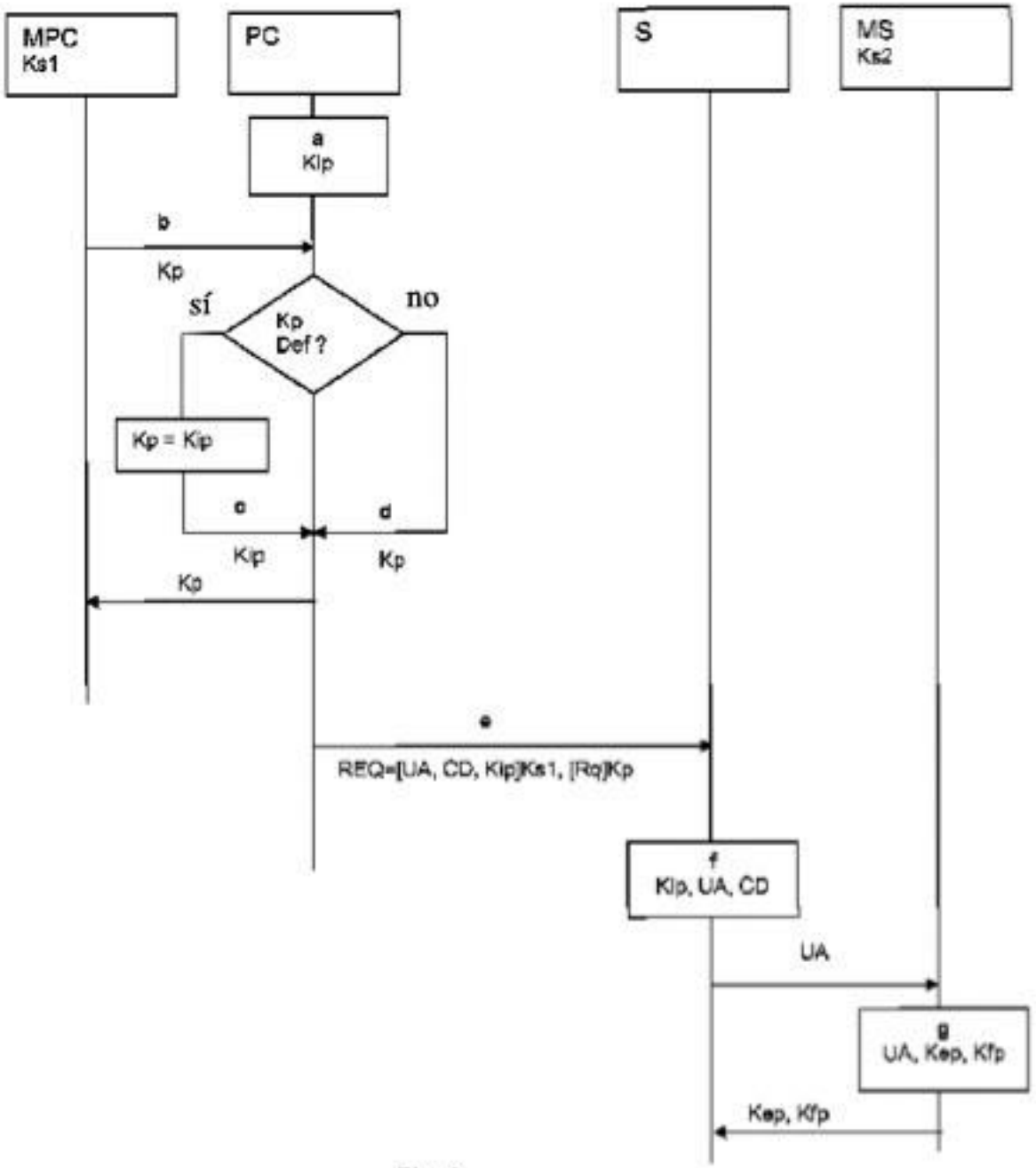
MPC
Ks1
PC
S
MS
Ks2
a
Klp
b
Kp
sí
Kp
Def ?
no
Kp = Klp
c
d
Klp
Kp
Kp
e
REQ=[UA, CD, Klp]Ks1, [Rq]Kp
f
Klp, UA, CD
UA
g
UA, Kep, Kfp
Kep, Kfp

Fig. 1

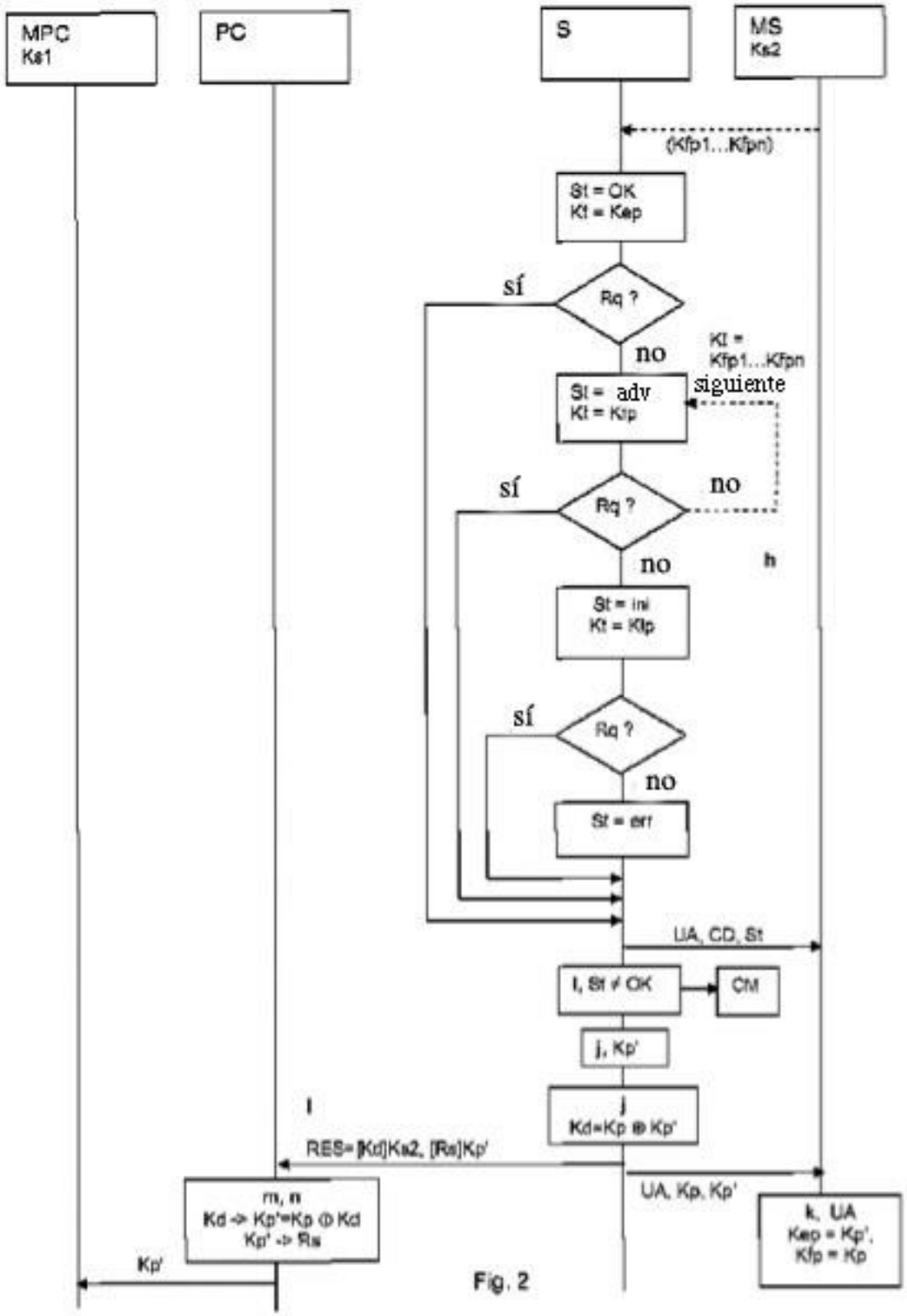
MPC
Ks1
PC
S
MS
Ks2
(Kfp1...Kfpn)
St = OK
Kt = Kep
sí
Rq ?
no
Kt = Kfp1...Kfpn
St = adv
Kt = Ktp
siguiente
sí
Rq ?
no
no
h
St = ini
Kt = Ktp
sí
Rq ?
no
St = err
UA, CD, St
I, St ≠ OK
CM
j, Kp'
j
Kd=Kp ⊕ Kp'
I
RES=[Kd]Ks2, [Rs]Kp'
UA, Kp, Kp'
m, n
Kd -> Kp'=Kp ⊕ Kd
Kp' -> Rs
k, UA
Kep = Kp',
Kfp = Kp
Kp'

Fig. 2

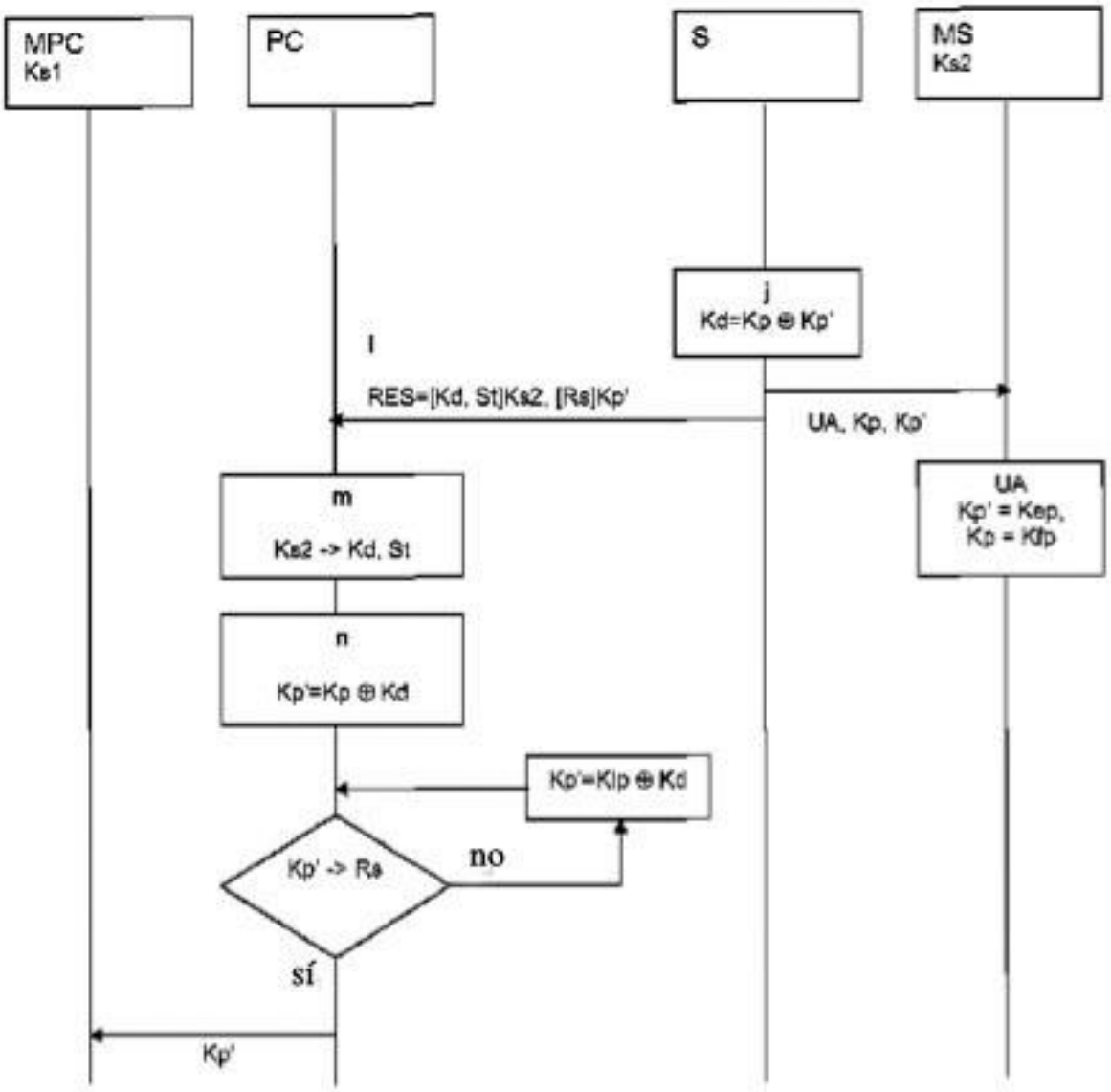
MPC
Ks1
PC
S
MS
Ks2
j
Kd=Kp ⊕ Kp'
l
RES=[Kd, St]Ks2, [Rs]Kp'
UA, Kp, Kp'
UA
Kp' = Kep,
Kp = Kdp
m
Ks2 -> Kd, St
n
Kp'=Kp ⊕ Kd
Kp'=Klp ⊕ Kd
Kp' -> Rs
no
sí
Kp'

Fig. 3