(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 675 749**

(51) Int. CI.:

H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.10.2007 PCT/EP2007/061470**

(87) Fecha y número de publicación internacional: **02.05.2008 WO08049882**

(96) Fecha de presentación y número de la solicitud europea: **25.10.2007 E 07821833 (6)**

(97) Fecha y número de publicación de la concesión europea: **16.05.2018 EP 2082574**

(54) Título: **Procedimiento de detección de una utilización anormal de un procesador de seguridad**

(30) Prioridad:

27.10.2006 FR 0654599

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.07.2018

(73) Titular/es:

VIACCESS (100.0%)
LES COLLINES DE L'ARCHE, TOUR OPERA C
92057 PARIS LA DEFENSE, FR

(72) Inventor/es:

CHIEZE, QUENTIN;
CUABOZ, ALAIN;
GIARD, ALEXANDRE;
GRANET, OLIVIER;
NEAU, LOUIS;
ROGER, MATTHIEU y
TRONEL, BRUNO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento de detección de una utilización anormal de un procesador de seguridad

Campo técnico

La invención se sitúa en el campo del control de acceso a unos servicios multimedia y se refiere más específicamente a un procedimiento de detección de una utilización anormal de un procesador de seguridad solicitado por al menos un terminal de recepción para controlar el acceso a un contenido digital aleatorizado proporcionado por al menos un operador a dicho terminal de recepción.

La invención se refiere, igualmente, a un procesador de seguridad destinado a controlar el acceso a un contenido digital aleatorizado proporcionado por al menos un operador a al menos un terminal de recepción.

La invención se aplica independientemente de la naturaleza de la red de soporte o del tipo de contenidos (TV en directo, programas de vídeo a solicitud VOD, Personal video recorder (PVR)).

Estado de la técnica anterior

Se conocen dos utilizaciones ilícitas de los sistemas de recepción que implementan un control de acceso. La primera tiene como finalidad analizar fraudulentamente el funcionamiento del procesador de control de acceso implementado en el receptor presentando a este último unos mensajes sintácticamente incorrectos, por ejemplo, con firma falsa, incompletos o que incluyen unas sucesiones ilícitas de mandos, la segunda tiene como propósito explotar los recursos de acceso condicional del sistema de recepción más allá de un uso normal autorizado. Esta segunda utilización puede estar realizada por la compartición del sistema de recepción considerado y, en particular, de su procesador de seguridad (tradicionalmente, card sharing) o por compartición o redistribución de las palabras de control (CW sharing).

De manera más particular, en el caso de una utilización compartida de los recursos del sistema de recepción, varios terminales solicitan el procesador de seguridad de este último mediante una red de comunicación bidireccional presentando a este último unos mensajes sintácticamente correctos, pero en número o diversidad excesivos.

La invención tiene como finalidad luchar contra las formas de pirateo descritas más arriba.

La invención se aplica de manera particular, pero no exclusivamente, cuando la interfaz entre el procesador de seguridad y el terminal no está protegida.

El documento europeo EP 1 447 976 A1 describe un método para impedir la compartición de un procesador de seguridad por varios terminales.

Este método consiste en medir los tiempos que separan la presentación de dos mensajes ECM (para Entitlement Control Message) sucesivos y en verificar que la cadencia de los tratamientos de los mensajes observada de este modo está conforme con unos esquemas de cadencia preestablecidos.

Este método no permite tomar en cuenta las perturbaciones en el encadenamiento de los tratamientos de los mensajes ECM ya que, en la realidad, la presentación de los mensajes ECM al procesador de seguridad depende, en concreto:

- de la organización de vinculación de estos mensajes ECM a los programas, según si el acceso a un programa depende de una condición de acceso global o de varias condiciones de acceso para cada componente de vídeo, audio u otros,
- de las capacidades ofrecidas por los decodificadores de tratar un solo programa o varios simultáneamente como en el caso de receptores multi-tuner que permiten registrar un programa durante la visualización de otro,
- de los hábitos de los usuarios cuyos "zapeos" repetidos provocan una rotura en el encadenamiento regular de los tratamientos de los mensajes ECM.

El documento EP15755293 describe un módulo de seguridad portátil que recibe una secuencia de mensajes de mando a unos intervalos distintos y los analiza. Una penalización se aplica asignando unos tiempos muertos al procesador hasta el bloqueo. Este procedimiento toma en cuenta los hábitos de zapeo y la presencia de varios en el aparato. Un nuevo arranque del módulo arrastra también una penalización. Otro objetivo de la invención es subsanar los inconvenientes de la técnica anterior descritos más arriba.

Descripción de la invención

La invención preconiza un procedimiento de detección de una utilización anormal de un procesador de seguridad solicitado por al menos un terminal de recepción para controlar el acceso a un contenido digital aleatorizado

proporcionado por al menos un operador a dicho terminal de recepción en el que, cada solicitación del procesador de seguridad consiste en presentar a este un mensaje de control de acceso ECM asociado al contenido aleatorizado y que transporta una palabra de control CW y la descripción de al menos una condición de acceso, con el fin de proporcionar al terminal la palabra de control para desaleatorizar el contenido,

Este procedimiento incluye las siguientes etapas:

- analizar la utilización del procesador de seguridad durante un periodo de observación T_{obs} predefinido que incluye un periodo de actividad T_{Act} de dicho procesador de seguridad constituido por acumulación de una pluralidad de duraciones de actividad sucesivas separadas por una duración mínima $T_{InaMín}$ de periodo de inactividad de dicho procesador de seguridad,
- contar a partir de dicho análisis el número N_{Ecm} de mensajes ECM tratados por el procesador de seguridad durante el periodo de actividad T_{act},
- determinar el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo de dicho procesador de seguridad durante dicho periodo de actividad T_{Act},
- comparar dicho valor medio M_{ECM} a un umbral $S_{máx}$ predefinido y,
- si el valor medio M_{ECM} es superior al umbral $S_{máx}$, aplicar a dicho terminal una sanción cuyo nivel de severidad crece gradualmente,

y, en una fecha corriente t_c, el conteo del número N_{ECM} de mensajes ECM contemporáneos tratados con éxito incluye las siguientes operaciones:

- comparar la fecha t a la fecha (t_C-T_{Diff}), representando T_{Diff} un retardo mínimo previamente definido que separa la fecha t y la fecha corriente t_C,
- incrementar el número N_{ECM} si la fecha (t_C-T_{Diff}) es inferior o igual a la fecha t de difusión de este mensaje ECM, si no, mantener el número N_{ECM} al valor corriente,
- si la fecha t está comprendida entre la fecha corriente t_C y la fecha t_C+$T_{InaMín}$, incrementar el periodo de actividad T_{Act} en el valor (t-t_C), si no, mantener el periodo de actividad T_{Act} al valor corriente.

Por el hecho de que la etapa de comparación utiliza el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo, el método según la invención es de naturaleza estadística y permite que no esté falseado por unas perturbaciones localizadas en la estructura temporal de los programas tratados y unas variaciones de los comportamientos de los usuarios.

Según una característica de la invención, en el transcurso del periodo de observación T_{Obs}, el valor medio M_{ECM} está determinado durante un periodo de actividad T_{Act} de dicho procesador de seguridad constituido por acumulación de una pluralidad de duraciones de actividad sucesivas separadas por una duración mínima $T_{InaMín}$ de inactividad de dicho procesador de seguridad.

Un periodo de actividad representa un intervalo de tiempo acumulado durante el que un procesador de seguridad está solicitado por rangos temporales continuos. Debe tener una duración mínima $T_{ActMín}$ para garantizar el carácter significativo del análisis. El respecto de esta duración mínima permite reducir el riesgo de detectar como abusiva una utilización puntualmente importante, aunque normal y lícita del procesador de seguridad. En un ejemplo, cada solicitación del procesador de seguridad consiste en presentar a este un mensaje de control de acceso ECM asociado al contenido aleatorizado y que transporta una palabra de control CW y la descripción de al menos una condición de acceso.

El análisis de la utilización del procesador de seguridad incluye en este caso las siguientes etapas:

- determinar el número N_{Ecm} de mensajes ECM tratados por el procesador de seguridad durante el periodo de actividad T_{act},
- calcular la relación $M_{ECM} = N_{ECM}/T_{Act}$,
- comparar la relación M_{ECM} al valor umbral $S_{máx}$,
- aplicar la sanción si el valor medio M_{ECM} es superior al umbral $S_{máx}$.

En este ejemplo, el análisis de la utilización del procesador de seguridad incluye las siguientes operaciones: en una fecha corriente t_c,

- determinar, por una parte, los mensajes ECM que tienen una fecha de difusión contemporánea de dicha fecha corriente t_c y que están presentados al procesador de seguridad con vistas a una primera utilización de un contenido y, por otra parte, los mensajes ECM que tienen una fecha de difusión anterior a la fecha corriente t_c y que están presentados al procesador de seguridad con vistas a una reutilización de un contenido,
- medir el periodo de actividad T_{Act} del procesador de seguridad durante el que trata unos mensajes ECM contemporáneos sucesivos,
- contar el número N_{ECM} de mensajes ECM contemporáneos al menos en tanto en cuanto el periodo de actividad T_{Act} es inferior a una duración mínima $T_{ActMín}$ predefinida.

En un ejemplo, en la fecha t_c, la determinación de un mensaje ECM antiguo está realizada por comparación de la fecha t de tratamiento de este mensaje ECM a la fecha (t_C-T_{Diff}), representando T_{Diff} un retardo mínimo previamente definido que separa la fecha t y la fecha t_c. En un ejemplo, el conteo del número N_{ECM} de mensajes ECM contemporáneos tratados con éxito incluye las siguientes operaciones:

- comparar la fecha t a la fecha (t_C-T_{Diff}),
- incrementar el número N_{ECM} si la fecha (t_C-T_{Diff}) es inferior o igual a la fecha t, si no, mantener el número N_{ECM} al valor corriente,
- incrementar el periodo de actividad T_{Act} en el valor (t-t_C) si la fecha t está comprendida entre la fecha t_C y la fecha t_C+$T_{InaMín}$, si no, mantener el periodo de actividad T_{Act} al valor corriente.

Según otra característica ventajosa, la sanción se aplica gradualmente según las siguientes etapas:

- en primer lugar, la sanción se aplica con un nivel de severidad n_i un número de veces predeterminado R_i,
- a continuación, la sanción se aplica con un nivel de severidad siguiente n_{i+1} un número de veces predeterminado R_{i+1},
- finalmente, la sanción máxima se aplica cuando se alcanza el último nivel $n_{imáx}$.

En un ejemplo, la sanción incluye un primer nivel que consiste en un bloqueo temporal de la recepción del contenido, un segundo nivel que consiste en un bloqueo de la recepción del contenido con obligación de contactar al operador que proporciona dicho contenido y un tercer nivel que consiste en un bloqueo definitivo de la recepción de dicho contenido.

Preferentemente, el análisis de la utilización del procesador de seguridad está efectuado por un software según la reivindicación 10 integrado en dicho procesador de seguridad. En un ejemplo, este último incluye:

- un primer módulo para analizar su utilización durante un periodo de observación T_{obs} predefinido,
- un segundo módulo para determinar a partir de dicho análisis el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo de dicho procesador de seguridad durante dicho periodo de observación T_{obs} y para comparar dicho valor medio M_{ECM} a un umbral $S_{máx}$ predefinido y
- un tercer módulo para aplicar a dicho terminal una sanción cuyo nivel de severidad crece gradualmente si el valor medio M_{ECM} es superior al umbral $S_{máx}$.

Breve descripción de los dibujos

Otras características y ventajas de la invención surgirán de la descripción que va a seguir, tomada a título de ejemplo no limitativo, con referencia a las figuras adjuntas en las que:

- la figura 1 representa esquemáticamente un organigrama que ilustra el conteo del valor medio del número de solicitaciones por unidad de tiempo de dicho procesador de seguridad durante el periodo de observación T_{obs},
- la figura 2 ilustra esquemáticamente las etapas de análisis y de sanción según la invención.

Exposición detallada de modos de realización particulares

La invención se describirá en un contexto de difusión por un operador de programas audiovisuales protegidos por un sistema de acceso condicional (CAS). Estos programas están destinados a varios terminales de abonados provistos cada uno de un procesador de seguridad, tradicionalmente una tarjeta inteligente.

En este contexto, el control por el operador del acceso a un programa aleatorizado se efectúa condicionando el acceso al contenido a la posesión por el terminal de una palabra de control CW y a la disponibilidad de una autorización comercial. A este efecto, el operador adscribe al contenido una condición de acceso que debe ser cumplida por el abonado para poder acceder a este contenido. La transmisión a los terminales de abonados de las palabras de control CW y de la descripción de la condición de acceso está realizada mediante unos mensajes de control de acceso específicos ECM (para Entitlement Control Message). Al nivel de cada terminal, los mensajes ECM están presentados al procesador de seguridad para ser verificados en cuanto a su seguridad. Después de verificación por el procesador de seguridad de la validez de estos mensajes, la condición de acceso que transportan se compara a los títulos de acceso presentes en una memoria no volátil del procesador de seguridad. De forma conocida de por sí, estos títulos de acceso se reciben previamente por el terminal mediante unos mensajes de control de acceso EMM (para Entitlement Management Message). Si la condición de acceso se cumple por uno de estos títulos de acceso, el procesador de seguridad reproduce por descifrado la palabra de control CW y la proporciona al terminal, que permite, de este modo, la desaleatorización de los contenidos. De forma conocida de por sí, los mensajes ECM y EMM están protegidos por unas modalidades criptográficas, que implementan unos algoritmos y unas claves para garantizar la integridad de estos mensajes, su autenticidad y la confidencialidad de los datos sensibles que pueden transportar y la actualización de estas claves, en concreto, está asegurada por unos mensajes de gestión EMM específicos para la seguridad.

Es habitual modificar el valor arbitrario de la palabra de control más o menos frecuentemente, según unas estrategias variables elegidas según el contexto. Por ejemplo, una palabra de control puede modificarse cada 10 segundos, de forma convencional, en televisión difundida o, en extremo, en cada película únicamente en Video On Demand con particularización individual por abonado.

La implementación del procedimiento en este contexto tiene como finalidad permitir que el procesador de seguridad detecte cualquier utilización abusiva de la que es objeto y de reaccionar a ello. La utilización considerada en este documento es la que controla el acceso a los contenidos, representada, por lo tanto, por el tratamiento de los mensajes ECM por el procesador de seguridad.

Para detectar una utilización abusiva, se mide estadísticamente un parámetro representativo de la utilización del procesador de seguridad y se compara este parámetro con un valor de umbral predefinido representativo de una utilización normal de dicho procesador de seguridad.

La medición de la utilización del procesador de seguridad consiste en analizar las solicitaciones de este procesador de seguridad durante un periodo de observación T_{obs} predefinido, luego en determinar, a partir de dicho análisis, el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo durante dicho periodo de observación T_{obs}.

La comparación de dicho valor medio M_{ECM} a un umbral $S_{máx}$ predefinido permite detectar una utilización abusiva del procesador de seguridad sobre el periodo de observación T_{obs} considerado.

El establecimiento del umbral $S_{máx}$ está realizado por examen del comportamiento medio de usuarios durante una duración significativa de observación.

Con el fin de cubrir al menos un ciclo característico de utilización del terminal de recepción por el usuario final, se define un periodo de actividad del procesador de seguridad, durante el periodo de observación T_{obs}, que representa un intervalo de tiempo durante el que este último está solicitado por rangos temporales continuos, ya sea de manera lícita o ilícita. Se define, igualmente, una duración mínima de actividad $T_{ActMín}$ que representa la duración que tiene que alcanzar el periodo de actividad para garantizar el carácter significativo del análisis de la utilización del procesador de seguridad durante el periodo de actividad. El respecto de esta duración mínima permite minimizar el riesgo de detectar como abusiva una utilización puntualmente importante, aunque globalmente normal de la tarjeta. En efecto, una utilización normal puede presentar, tradicionalmente en caso de zapeo intenso, unos picos temporales de solicitación análoga a la solicitación de la tarjeta en un contexto de utilización abusiva.

Se define, igualmente, una duración mínima de inactividad $T_{InaMín}$ que representa la duración transcurrida desde el último mensaje ECM tratado con éxito a más allá de la que se considera que el periodo de actividad anterior está terminado.

Por otra parte, con el fin de determinar, en una fecha corriente t_c que corresponde al último tratamiento con éxito de un mensaje ECM, por una parte, los mensajes ECM contemporáneos de esta fecha corriente t_c presentados al procesador de seguridad con vistas a una primera utilización de un contenido, por otra parte, los mensajes ECM antiguos con respecto a la fecha t_c presentados al procesador de seguridad con vistas a una reutilización de un contenido, se designa por el parámetro T_{Diff} la duración mínima que separa la fecha de un mensaje ECM antiguo de la fecha corriente y se considera que un mensaje ECM está presentado al procesador de seguridad con vistas a una reutilización de un contenido si la fecha de este mensaje ECM es anterior a t_c en una duración superior o igual a T_{Diff}.

Señalemos que la fecha de difusión de un mensaje ECM puede estar determinada por diversas soluciones técnicas conocidas de por sí. Por ejemplo, está inscrita en este mensaje ECM, con la condición de acceso y la palabra de control, por el generador de mensajes ECM, ECM-G y se extrae por el procesador de seguridad durante el tratamiento de este mensaje ECM.

Las etapas del procedimiento según la invención se describirán a continuación con referencia a las figuras 1 y 2.

La figura 1 ilustra las etapas de conteo del número N_{Ecm} de mensajes ECM tratados por el procesador de seguridad durante un periodo de actividad T_{Act} y la medición casi simultánea de dicho periodo de actividad T_{Act}.

Con referencia a la figura 1, en una fecha corriente t_c durante un periodo de observación T_{obs} que se inicia en el instante t_o, el procesador de seguridad recibe un mensaje ECM_t que tiene como fecha de difusión t (etapa 10).

En la etapa 12, el procesador de seguridad analiza la sintaxis, la autenticidad y la integridad del mensaje ECM_t, luego determina la fecha t de ello y los criterios de acceso.

En la etapa 14, el procesador de seguridad verifica la validez de los criterios de acceso, así como la autenticidad y la integridad del mensaje.

Si estos últimos no se satisfacen o si el mensaje no es auténtico o íntegro, el procesador de seguridad analiza el

mensaje ECM siguiente (flecha 16).

Si los criterios de acceso se satisfacen (flecha 18), el procesador de seguridad trata el mensaje ECM_t y compara, en la etapa 20, la fecha t de este mensaje ECM_t a la fecha t_c-T_{diff} para determinar si el mensaje ECM_t está presentado para una primera utilización del contenido o para una reutilización después de registro de este.

Si t_c-T_{diff} es inferior a t, dicho de otra manera, si el mensaje ECM_t se refiere a una primera explotación del programa aleatorizado, el procesador de seguridad incrementa el número de mensajes ECM tratados en una unidad en la etapa 22.

Si la fecha t del mensaje ECM_t está comprendida entre las fechas t_c y t_c+$T_{InaMín}$ (etapa 24), el procesador de seguridad concluye que el periodo de actividad anterior todavía no está terminado y, en la etapa 26, la duración del periodo de actividad corriente T_{Act} se incrementa en la duración t-t_c.

La determinación del periodo de actividad T_{Act} y el conteo del número N_{Ecm} de mensajes ECM tratados por el procesador de seguridad se efectúan, de este modo, hasta el final del periodo de observación T_{obs}.

La figura 2 ilustra esquemáticamente las etapas de análisis de la utilización del procesador de seguridad y de sanción según la invención.

En la etapa 30, el procesador de seguridad calcula la relación M_{ECM}=N_{ECM}/T_{act}, en la que N_{Ecm} representa el número de mensajes ECM contados y T_{Act} representa la duración total el periodo de actividad durante el periodo de observación T_{obs}.

En la etapa 32, el procesador de seguridad verifica si T_{Act} es superior o igual a una duración $T_{ActMín}$ predefinida. Esta etapa tiene como finalidad verificar que el periodo de actividad T_{Act} es suficiente para garantizar el carácter significativo del análisis.

Si T_{Act} es inferior a $T_{ActMín}$, el procesador de seguridad descifra en la etapa 54 la palabra de control contenida en el mensaje ECM_t, luego verifica en la etapa 34 si la duración de observación T_{obs} está acabada.

En caso afirmativo, el procesador de seguridad reinicializa (etapa 36) los valores N_{Ecm}, T_{act}, y T_0.

En caso negativo, estos valores no se reinicializan.

En los dos casos, el proceso se continúa por la etapa 38 que consiste en verificar si la fecha t del mensaje ECM_t es posterior a la fecha corriente t_c.

Si sí, la fecha t se asigna a la fecha corriente t_c.

El proceso se continúa a partir de la etapa 10 del conteo (figura 1).

Si T_{Act} es superior o igual a $T_{ActMín}$, el procesador de seguridad verifica (etapa 50) si el valor medio calculado M_{ECM} es superior al umbral $S_{máx}$.

Si sí, se aplica una sanción y el número n de sanciones y/o el nivel de la sanción aplicada se incrementa (etapa 52) y los valores N_{ECM}, T_{Act} y t_O se reinicializan (etapa 53).

Si no, la palabra de control CW se descifra y transmite al terminal para permitir la desaleatorización del contenido (etapa 54).

El procedimiento se continúa, a continuación, por la etapa 34 que consiste en verificar si la duración (t-t_O) es superior a la duración T_{Obs} del periodo de observación.

En caso afirmativo, el procesador de seguridad reinicializa (etapa 36) los valores N_{Ecm}, T_{act}, y T_0.

En caso negativo, estos valores no se reinicializan.

En los dos casos, el proceso se continúa por la etapa 38 que consiste en verificar si la fecha t del mensaje ECM_t es posterior a la fecha corriente t_c.

Si la fecha t de difusión del mensaje ECM_t es posterior a la fecha t_c, la etapa 40 la fecha t se asigna a la fecha corriente t_c, y el procedimiento se continúa a partir de la etapa 10 del conteo (figura 1).

La gestión de la sanción en la etapa 52 comprende el incremento del número n de sanciones y/o del nivel de la sanción. Esta gestión de sanción es característica de la invención. Por el hecho de que el procedimiento es un

análisis estadístico de las solicitaciones del procesador de seguridad basado en una modelización previa como se describirá esto más adelante, definir una sola sanción y aplicarla desde el momento en que la detección de uso anormal es excesivo y puede hacer el procedimiento finalmente no operativo. Con el fin de beneficiarse de la progresividad aportada por el análisis estadístico en la detección de la utilización abusiva del procesador, la gestión de las sanciones mejor adaptada y, por lo tanto, inherente al procedimiento es una gestión progresiva. Esta gestión define varios niveles de sanciones de severidad creciente y aplicadas progresivamente por pasos.

A título de ejemplo, una primera detección de uso abusivo del procesador de seguridad hace interrumpir el acceso al contenido impidiendo la desaleatorización de este. Cuando esta sanción de severidad escasa se ha repetido un cierto número de veces a causa de confirmación del uso abusivo, se aplica otra sanción de severidad media que consiste en bloquear temporalmente el terminal con obligación para el usuario de contactar a su operador para desbloquear el terminal. Cuando esta segunda sanción se ha aplicado un cierto número de veces debido a la persistencia del uso abusivo, se aplica una sanción final de severidad fuerte que consiste en invalidar de forma definitiva el procesador de seguridad.

El proceso descrito más arriba implementa unos parámetros frecuentemente actualizados en una memoria del procesador de seguridad de tipo EEPROM (para Electrically Erasable Programmable Read-Only Memory), con el fin de asegurar la continuidad del análisis en caso de interrupción de la alimentación del procesador de seguridad.

Ahora bien, este tipo de memoria soporta un número limitado de escrituras. También, con el fin de compensar esta restricción tecnológica, los parámetros N_{ECM}, t_C y T_{Act} que son los más solicitados por los cálculos se almacenan en memoria no permanente (RAM) y se salvaguardan regularmente en la memoria EEPROM.

A este efecto, se definen los siguientes nuevos parámetros:

- el número N_{Buf} de mensajes ECM tratados con éxito desde la última transferencia de los parámetros N_{ECM}, t_C y T_{Act} en la memoria EEPROM.
- el número $N_{máx}$ que representa un umbral máximo del número N_{Buf} que dispara la actualización en memoria EEPROM de los parámetros N_{ECM}, t_C y T_{Act}.

Los parámetros N_{ECM}, t_c y T_{Act} se gestionan, entonces, de la siguiente forma:
Durante la puesta en tensión del procesador de seguridad o la activación del análisis de la utilización del procesador de seguridad, los parámetros N_{ECM}, t_C y T_{Act} se crean e inscriben con su valor de inicialización en memoria EEPROM si todavía lo han sido nunca anteriormente.

Después de puesta en tensión del procesador de seguridad o a la activación del análisis de la utilización de este procesador de seguridad:

- los parámetros N_{ECM}, t_C y T_{Act} se cargan en memoria RAM
- cualquier incremento de estos parámetros se hace en memoria RAM
- si $N_{Buf} > N_{máx}$, sus valores se actualizan, además, en memoria EEPROM.

De este modo, cada vez que el número de mensajes ECM tratados con éxito durante la duración T_{obs} aumenta en el valor de umbral $N_{máx}$ predefinido, los parámetros N_{ECM}, t_C y T_{Act} se transfieren a una memoria EEPROM.

Señalemos que si los valores N_{ECM}, t_C y T_{Act} se conocen, una persona malintencionada que intervenga puede hacer no efectivo el procedimiento poniendo regularmente fuera de tensión el procesador de seguridad. De este modo, los valores memorizados se pierden, impidiendo analizar la utilización del procesador de seguridad y permitiendo, de este modo, que el pirata lo comparta con total impunidad.

Para evitar este sorteo ilícito del procedimiento, una solución es descargar en el procesador de seguridad un nuevo valor más escaso del umbral $N_{máx}$. Otra solución consiste en incrementar, después de cada puesta en tensión, los valores de T_{Act} y N_{ECM} respectivamente en $T_{Act,ini}$ (Corrección del tiempo de actividad) y $N_{ECM,ini}$ (Corrección del número de mensajes ECM tratados con éxito).

Esto equivale a bajar el valor del umbral $N_{máx}$.

En un modo preferente de realización, la parametrización y la activación del análisis son programables por el operador por envío de mensaje EMM.

Esta parametrización puede realizarse, igualmente, en fase de personalización de la tarjeta.

Consiste en:

- elegir, de entre una lista dada, la sanción de cada uno de los niveles de severidad media y fuerte;
- fijar los números de repeticiones de las sanciones de severidades escasa y media.

Además, dicho mensaje EMM transporta al menos uno de los siguientes parámetros:

- la duración T_{obs} del periodo de observación,
- la duración mínima de actividad $T_{ActMín}$,
- el retardo T_{Diff},
- la duración mínima de inactividad $T_{InaMín}$,
- el valor del umbral $S_{máx}$,
- el valor del umbral N_{Buf}.

Estos parámetros se completan por los siguientes parámetros relativos a la implementación del procedimiento:

$N_{máx}$: Umbral de memorización expresado en número de mensajes ECM,

$T_{Act,ini}$: Corrección del tiempo de actividad expresada en segundos,

$N_{ECM,ini}$: corrección del número de mensajes ECM tratados con éxito,

T_{SFA}: Duración, expresada en segundos, del no tratamiento de los ECM a título de la sanción de nivel de severidad escasa,

R_{SFA}: Número de repeticiones de la sanción de nivel de severidad escasa,

R_{SMO}: Número de repeticiones de la sanción de nivel de severidad media.

A continuación, describimos un ejemplo de una parametrización de este tipo que es el resultado de una modelización del uso normal del procesador de seguridad.

Se considera que el comportamiento de un usuario varía según el día de la semana, pero se repite de una semana a la otra.

El análisis se basa, por otra parte, en las siguientes hipótesis:

- Hipótesis de zapeo: 1 mensaje ECM suplementario en cada zapeo,
- Zapeo Escaso: 20 mensajes ECM más/hora, o sea, 1 cada 3 minutos,
- Zapeo Medio: 60 mensajes ECM más/hora, o sea, 1 por minuto,
- Zapeo Normal: 120 mensajes ECM más/hora, o sea, cada 30 segundos,
- Zapeo Superabundante: 1.000 mensajes ECM más/hora, o sea, cada 3 segundos.

En el ejemplo de realización que se describirá, el análisis se ha experimentado sobre un periodo de observación de 7 días, luego sobre un periodo de observación de 15 días. En el caso de programas que incluyen varios componentes aleatorizados, solo se realiza el conteo de la vía ECM principal, relativa al Vídeo, por ejemplo.

Finalmente, están fijados los siguientes valores:

- Tiempo mínimo de inactividad: 15 segundos
- Retardo de diferido: 5 minutos,
- Criptoperiodo: 10 segundos,
- El número de tuners del sistema de recepción está limitado a 2, permitiendo el acceso simultáneo a dos contenidos, el uno en visualización directa, el otro en registro sobre la memoria masiva del terminal.
- Periodo de observación: 7 a 14 días,

Basándose en las hipótesis de más arriba y los usos conocidos, se han elaborado varios perfiles de utilización lícita y de utilización ilícita de un sistema de recepción. Para poder discriminar estas dos categorías de perfiles de utilización, la modelización conduce a determinar los siguientes valores de los parámetros T_{Obs}, $T_{ActMín}$ y $S_{Máx}$:

- El tiempo de observación T_{Obs} es de 14 días, o sea, 1209600 segundos.
- Una solicitación de 0,22 ECM por segundo permite la discriminación buscada con un margen de seguridad que

habilita una latitud amplia de comportamiento para el usuario lícito de un sistema de recepción con uno o dos tuners. El máximo de solicitación lícita $S_{Máx}$ está fijado a este valor.

- El tiempo mínimo de actividad $T_{ActMín}$ está fijado a 30 horas, o sea, 108000 segundos.

El procedimiento según la invención se implementa por un procesador de seguridad que incluye:

- un primer módulo para analizar su utilización durante un periodo de observación T_{obs} predefinido,
- un segundo módulo para determinar a partir de dicho análisis el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo de dicho procesador de seguridad durante dicho periodo de observación T_{Obs} y para comparar dicho valor medio M_{ECM} a un umbral $S_{máx}$ predefinido y
- un tercer módulo para aplicar a dicho terminal una sanción cuyo nivel de severidad crece gradualmente si el valor medio M_{ECM} es superior al umbral $S_{máx}$.

Este procesador de seguridad implementa un software que incluye:

- unas instrucciones para analizar la utilización de dicha tarjeta inteligente por dicho terminal durante un periodo de observación T_{obs} predefinido,
- unas instrucciones para determinar a partir de dicho análisis el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo de dicha tarjeta inteligente por dicho terminal durante dicho periodo de observación T_{obs} y para comparar dicho valor medio M_{ECM} a un umbral $S_{máx}$ predefinido y
- unas instrucciones para aplicar a dicho terminal una sanción cuyo nivel de severidad crece gradualmente si el valor medio M_{ECM} es superior al umbral $S_{máx}$.

El procedimiento se ha descrito en el caso en que los ECM tomados en cuenta en el conteo y el análisis son unos ECM tratados con éxito, es decir, reconocidos como sintácticamente correctos, auténticos, íntegros y satisfechos por los derechos *ad hoc* para permitir el acceso a los contenidos. Como variante, el procedimiento puede implementarse, igualmente, tomando en cuenta los ECM reconocidos como erróneos por el procesador de seguridad, en concreto, a título de la sintaxis, de la autenticidad y/o de la integridad. Esto permite integrar significativamente, en el análisis de un uso abusivo del procesador, los ataques por fuerza bruta por presentaciones reiteradas de ECM voluntariamente incorrectos. En este caso, la etapa 14 de la figura no se ejecuta y el procedimiento de la figura 1 se continúa en la etapa 20.

REIVINDICACIONES

1. Procedimiento de detección de una utilización anormal de un procesador de seguridad solicitado por al menos un terminal de recepción para controlar el acceso a un contenido digital aleatorizado proporcionado por al menos un operador a dicho terminal de recepción en el que, cada solicitación del procesador de seguridad consiste en presentar a este un mensaje de control de acceso ECM asociado al contenido aleatorizado y que transporta una palabra de control CW y la descripción de al menos una condición de acceso, con el fin de proporcionar al terminal la palabra de control para desaleatorizar el contenido,
procedimiento que incluye las siguientes etapas:

- analizar la utilización del procesador de seguridad durante un periodo de observación T_{obs} predefinido que incluye un periodo de actividad T_{Act} de dicho procesador de seguridad constituido por acumulación de una pluralidad de duraciones de actividad sucesivas separadas por una duración mínima $T_{InaMín}$ de periodo de inactividad de dicho procesador de seguridad,
- contar a partir de dicho análisis el número N_{Ecm} de mensajes ECM tratados por el procesador de seguridad durante el periodo de actividad T_{act},
- determinar el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo de dicho procesador de seguridad durante dicho periodo de actividad T_{Act},
- comparar dicho valor medio M_{ECM} con un umbral $S_{máx}$ predefinido y,
- si el valor medio M_{ECM} es superior al umbral $S_{máx}$, aplicar a dicho terminal una sanción cuyo nivel de severidad crece gradualmente,

Procedimiento en el que, en una fecha corriente t_c, el conteo del número N_{ECM} de mensajes ECM contemporáneos tratados con éxito incluye las siguientes operaciones:

- comparar la fecha t con la fecha (t_C-T_{Diff}), representando T_{Diff} un retardo mínimo previamente definido que separa la fecha t y la fecha corriente t_c,
- incrementar el número N_{ECM} si la fecha (t_c-T_{Diff}) es inferior o igual a la fecha t de difusión de este mensaje ECM, si no, mantener el número N_{ECM} al valor corriente,
- si la fecha t está comprendida entre la fecha corriente t_c y la fecha t_C+$T_{InaMín}$, incrementar el periodo de actividad T_{Act} en el valor (t-t_C), si no, mantener el periodo de actividad T_{Act} al valor corriente.

2. Procedimiento según la reivindicación 1, en el que el análisis de la utilización del procesador de seguridad lo realiza un software integrado en dicho procesador de seguridad.

3. Procedimiento según la reivindicación 2, en el que dicha sanción incluye un primer nivel que consiste en un bloqueo temporal de la recepción del contenido, un segundo nivel que consiste en un bloqueo de la recepción del contenido con obligación de entrar en contacto con el operador que proporciona dicho contenido y un tercer nivel que consiste en un bloqueo definitivo de la recepción de dicho contenido.

4. Procedimiento según la reivindicación 1, en el que el análisis de la utilización del procesador de seguridad incluye las siguientes operaciones:
en la fecha corriente t_c,

- determinar, por una parte, los mensajes ECM que tienen una fecha de difusión contemporánea de la fecha corriente t_c y que están presentados al procesador de seguridad con vistas a una primera utilización de un contenido, por otra parte, los mensajes ECM que tienen una fecha de difusión anterior a la fecha corriente t_c y que están presentados al procesador de seguridad con vistas a una reutilización de un contenido,
- contar el número N_{ECM} de mensajes ECM contemporáneos al menos en tanto en cuanto el periodo de actividad T_{Act} es inferior a una duración mínima $T_{ActMín}$ predefinida.

5. Procedimiento según la reivindicación 4, en el que, en la fecha t_c, la determinación de un mensaje ECM antiguo está realizada por comparación de la fecha t de difusión de este mensaje ECM con la fecha (t_C-T_{Diff}), representando T_{Diff} un retardo mínimo previamente definido que separa la fecha t y la fecha t_c.

6. Procedimiento según la reivindicación 1, en el que, en el transcurso de un periodo de observación que se inicia en un instante t_0, el análisis de la utilización del procesador de seguridad incluye las siguientes operaciones:

- calcular la relación $M_{ECM} = N_{ECM}/T_{Act}$,
- verificar si T_{Act} es superior o igual a una duración $T_{ActMín}$ predefinida y si M_{ECM} es superior a $S_{máx}$,

en caso afirmativo,

-- aplicar la sanción,
-- incrementar el número n de sanciones y/o el nivel de la sanción aplicada,
-- reinicializar los valores N_{ECM}, T_{Act} y t_O. si no,

-- descifrar la palabra de control CW,

- si la duración ($t-t_O$) es superior a la duración T_{Obs} del periodo de observación,

-- reinicializar los valores de N_{ECM}, T_{Act} y t_O

- si la fecha t es superior a la fecha t_C

-- sustituir la fecha t_C por la fecha t.

7. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que la parametrización y la activación del análisis son programables por el operador por envío de mensaje EMM.

8. Procedimiento según la reivindicación 7, en el que dicho mensaje EMM transporta al menos uno de los siguientes parámetros:

- la duración T_{Obs} del periodo de observación,
- la duración mínima de actividad $T_{ActMín}$,
- el retardo T_{Diff},
- la duración mínima de inactividad $T_{InaMín}$,
- el valor del umbral $S_{máx}$,
- el valor del umbral N_{Buf}.

9. Procesador de seguridad destinado a controlar el acceso a un contenido digital aleatorizado proporcionado por al menos un operador a al menos un terminal de recepción que incluye:

- un primer módulo para analizar su utilización durante un periodo de observación T_{obs} predefinido que incluye un periodo de actividad T_{Act} de dicho procesador de seguridad constituido por acumulación de una pluralidad de duraciones de actividad sucesivas separadas por una duración mínima $T_{InaMín}$ de periodo de inactividad de dicho procesador de seguridad,
- un segundo módulo para -contar a partir de dicho análisis el número M_{ECM} de mensajes ECM tratados por el procesador de seguridad durante el periodo de actividad T_{act} y el valor medio M_{ECM} del número de solicitaciones por unidad de tiempo de dicho procesador de seguridad durante dicho periodo de observación T_{Obs} y para comparar dicho valor medio M_{ECM} con un umbral $S_{máx}$ predefinido, consistiendo cada solicitación del procesador de seguridad en presentar a este un mensaje de control de acceso ECM asociado al contenido aleatorizado y que transporta una palabra de control CW y la descripción de al menos una condición de acceso, con el fin de proporcionar al terminal la palabra de control para desaleatorizar el contenido y
- un tercer módulo para aplicar a dicho terminal una sanción cuyo nivel de severidad crece gradualmente si el valor medio M_{ECM} es superior al umbral $S_{máx}$, en el que, el primer módulo está configurado de modo que en una fecha corriente t_C, el conteo del número N_{ECM} de mensajes ECM contemporáneos tratados con éxito incluye las siguientes operaciones:

  - comparar la fecha t con la fecha (t_C-T_{Diff}), representando T_{Diff} un retardo mínimo previamente definido que separa la fecha t y la fecha corriente t_c,
  - incrementar el número N_{ECM} si la fecha (t_C-T_{Diff}) es inferior o igual a la fecha t de difusión de este mensaje ECM, si no, mantener el número N_{ECM} al valor corriente,
  - si la fecha t está comprendida entre la fecha corriente t_c y la fecha $t_C+T_{InaMín}$, incrementar el periodo de actividad T_{Act} en el valor ($t-t_C$), si no, mantener el periodo de actividad T_{Act} al valor corriente.

10. Programa de ordenador que comprende unas instrucciones para la ejecución de las etapas del procedimiento según una de las reivindicaciones 1 a 9 cuando dicho programa se ejecuta sobre una tarjeta inteligente asociada a un terminal de recepción de contenidos digitales proporcionados por un operador.

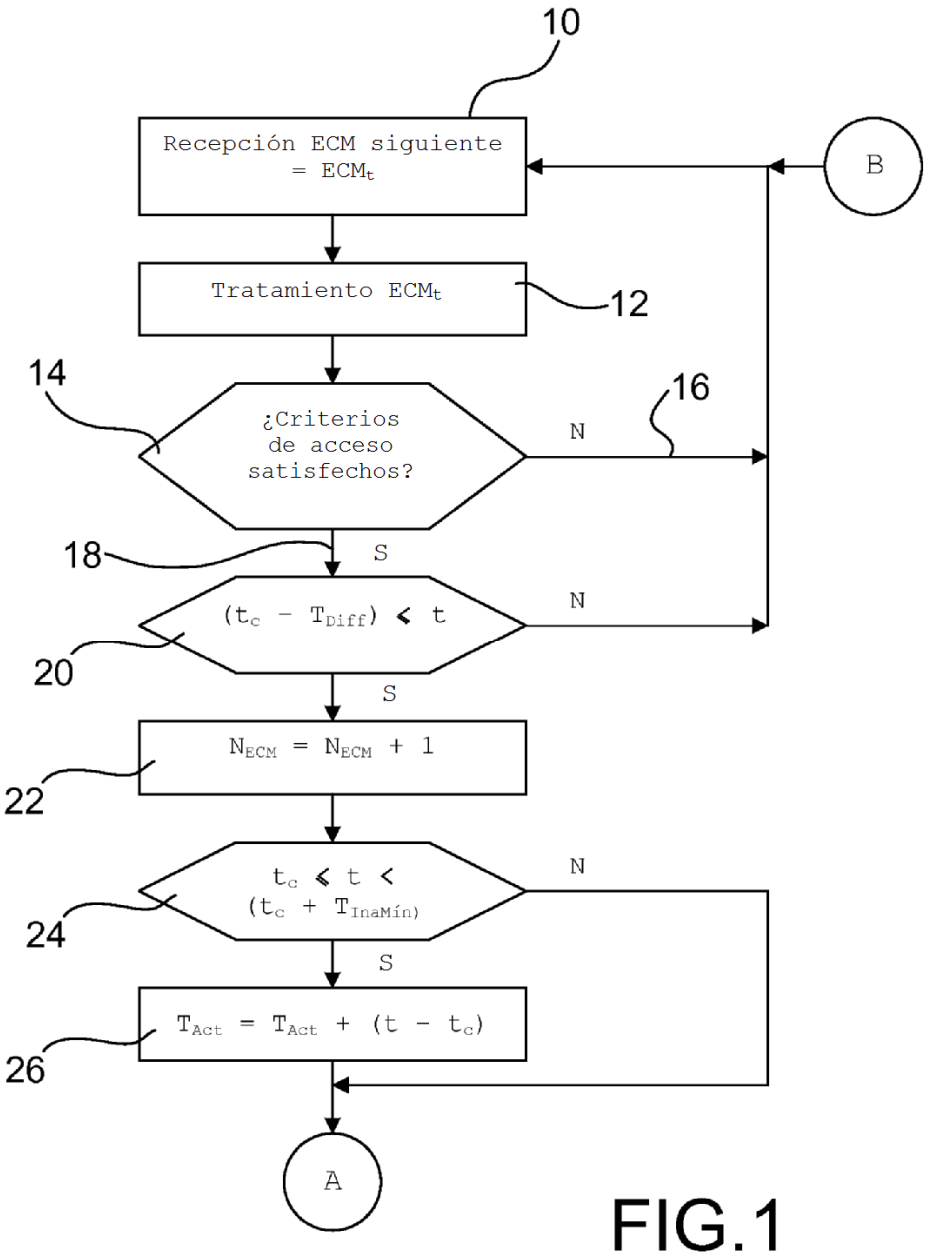
10
Recepción ECM siguiente = ECM_t
B
Tratamiento ECM_t
12
14
¿Criterios de acceso satisfechos?
N
16
S
18
$(t_c - T_{Diff}) < t$
N
20
S
$N_{ECM} = N_{ECM} + 1$
22
$t_c < t < (t_c + T_{InaMín})$
N
24
S
$T_{Act} = T_{Act} + (t - t_c)$
26
A

FIG.1

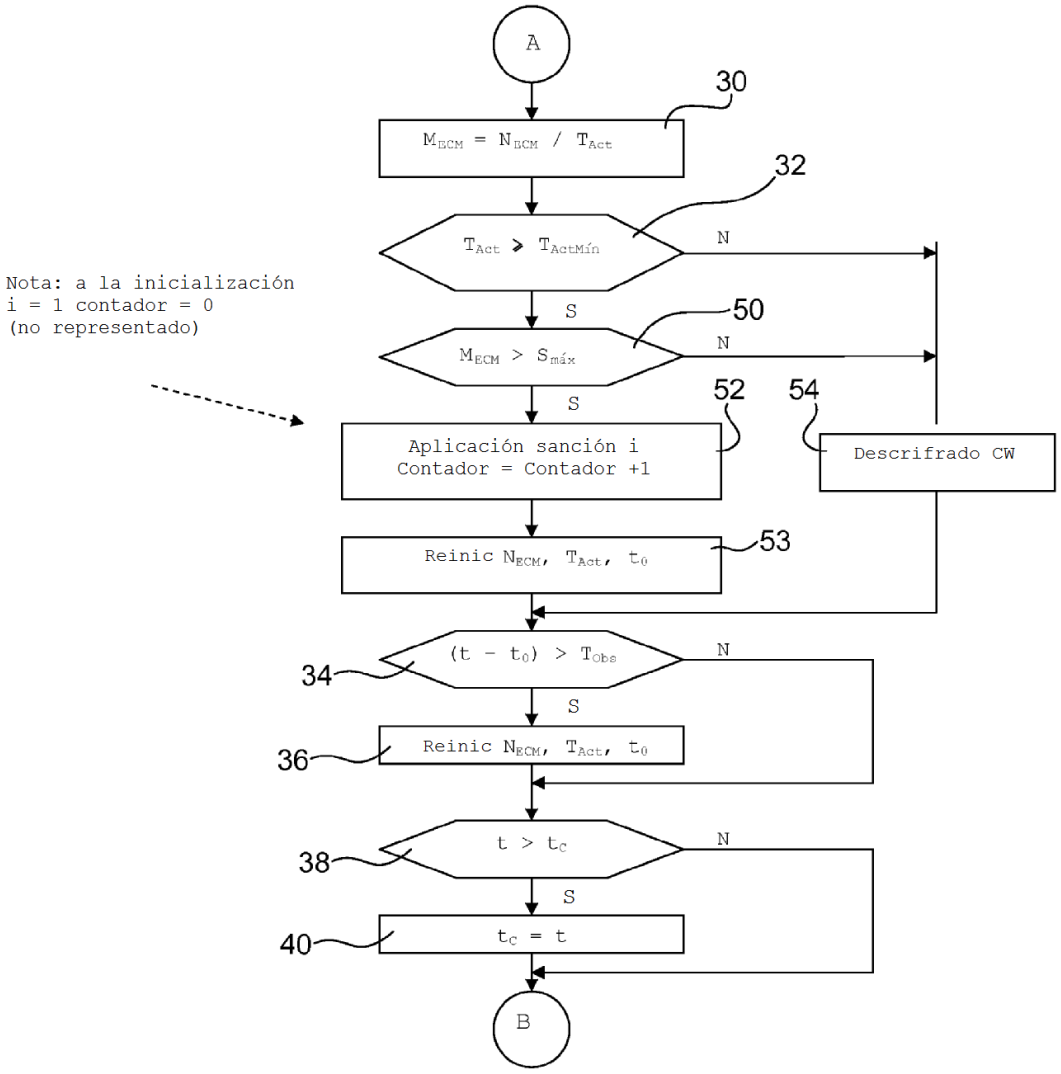
A
30
$M_{ECM} = N_{ECM} / T_{Act}$
32
$T_{Act} > T_{ActMín}$
N
S
50
$M_{ECM} > S_{máx}$
N
S
52
54
Aplicación sanción i
Contador = Contador +1
Descrifrado CW
Reinic N_{ECM}, T_{Act}, t_0
53
$(t - t_0) > T_{Obs}$
34
N
S
36
Reinic N_{ECM}, T_{Act}, t_0
$t > t_C$
38
N
S
40
$t_C = t$
B
Nota: a la inicialización
i = 1 contador = 0
(no representado)

FIG.2