(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 309 770**

(51) Int. Cl.:
G06F 1/00 (2006.01)
G06F 9/445 (2006.01)
H04N 7/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05754114 .6**
(96) Fecha de presentación : **16.06.2005**
(97) Número de publicación de la solicitud: **1756696**
(97) Fecha de publicación de la solicitud: **28.02.2007**

(54) Título: **Método de actualización protegida de software instalado en un módulo de seguridad.**

(30) Prioridad: **17.06.2004 EP 04102768**

(45) Fecha de publicación de la mención BOPI:
16.12.2008

(45) Fecha de la publicación del folleto de la patente:
16.12.2008

(73) Titular/es: **NagraCard S.A.**
22, route de Genève
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es: **Osen, Karl**

(74) Agente: **Tomás Gil, Tesifonte Enrique**

DESCRIPCIÓN

Método de actualización protegida de software instalado en un módulo de seguridad.

Campo de la invención

La presente solicitud se refiere al campo de los módulos de seguridad, en particular los módulos de seguridad que disponen de softwares que pueden ser actualizados.

Estado de la técnica

Estos módulos de seguridad tienen a cargo numerosas funciones tales como la autentificación, la verificación de los derechos o la gestión de un crédito. Estas funciones necesitan capacidades de tratamiento importantes y disponen de microprocesadores rápidos cuya mayoría del software es memorizada en una memoria reinscribible.

De esta manera, una vez que un error de programación o un fallo en la seguridad es detectado, un bloque de corrección es preparado y almacenado en una región libre de la memoria. Una modificación es efectuada también en la parte programa para beneficiarse de las funcionalidades de este nuevo bloque de programa.

Cuando un tal módulo es utilizado en un sistema descentralizado, la actualización de los módulos de seguridad se hace por los medios de telecomunicación disponibles tales como la difusión (un gran número de módulos reciben el mismo mensaje) o una conexión punto por punto.

En ambos casos, pero particularmente en el primer caso, el mensaje de actualización es vulnerable a los ataques de las personas malintencionadas. El análisis del mensaje recibido por un módulo podría dar índices reveladores sobre el funcionamiento de dicho módulo y revelar secretos ligados a la seguridad.

Es cierto que estos mensajes son encriptados, pero medios importantes son aplicados por estas personas malintencionadas para descifrar estos mensajes y extraer el contenido.

Los módulos considerados por la presente invención son utilizados en la televisión de pago, en los teléfonos móviles, incluso en las aplicaciones bancarias.

Para el resto de la exposición, tomaremos el ámbito de la televisión de pago como ejemplo.

Según un procedimiento conocido, el centro de vigilancia es informado de un fallo de la seguridad y va a preparar un bloque de programa, llamado “patch” que está destinado a actualizar el software del módulo de seguridad.

El bloque así preparado, es encriptado por una o varias claves propias de los módulos de seguridad. Es posible encriptar este bloque o por una clave global, común a todos los módulos de seguridad, o por una clave personal, propia de cada módulo. En este último caso, habrá que preparar tantos mensajes como módulos de seguridad diferentes hayan.

El mensaje es después enviado al centro de gestión que dispone los medios de transmisión hacia los módulos. En un sistema unidireccional, el mensaje es repetido durante un período dado a fin de asegurarse de que cada módulo lo ha recibido.

El experto en la materia se pone en una posición difícil cuando un fallo de seguridad es detectado porque debe sopesar los riesgos de que un tal mensaje sea analizado por un tercero y los riesgos de dejar este fallo abierto. Este dilema ha conducido a veces a prohibir corregir un defecto del programa porque el riesgo de comprensión del programa de reemplazo era demasiado importante.

La actualización de programas en un descodificador de televisión de pago es bien conocida y se describe por ejemplo en el documento US2004/107349. Los módulos programas son enviados al descodificador encriptados por una clave que es utilizada una vez. Es el principio de la lista a tachar que se aplica aquí. El módulo programa una vez recibido es almacenado en la memoria del descodificador y activado según un protocolo usual (derivación de una dirección hacia el patch).

Breve descripción de la invención

El objetivo de la presente invención es permitir al experto en la materia transmitir un mensaje conteniendo un bloque de programa en un mensaje sin tener que inquietarse por el resultado de una desencriptación malintencionada de este mensaje.

Este objetivo se alcanza por un método de actualización protegida con software instalado en un módulo de seguridad, este método incluyendo las etapas siguientes:

- formación de un primer bloque de programa de actualización,

- determinación de una zona de memoria objetivo de dicho módulo de seguridad,

- determinación para dicho módulo de seguridad, de un contenido preregistrado en dicha zona de memoria objetivo,

- formación de un segundo bloque de programa obtenido por la mezcla del contenido preregistrado y del primer bloque de programa,

- transmisión del segundo bloque de programa al módulo de seguridad,

- recepción del segundo bloque por el módulo de seguridad,

- lectura de la zona de memoria objetivo,

- obtención y escritura en la zona de memoria objetivo del primer bloque por la mezcla inversa del segundo bloque y del contenido de la zona de memoria objetivo.

De este modo, gracias a la invención, el código transmitido (segundo bloque) no tiene ninguna relación con el primer bloque para quien no conoce el contenido de la memoria objetivo.

Un tercero que lleve a cabo la descodificación del mensaje no aprenderá nada más sobre el funcionamiento del módulo de seguridad.

Este método puede aplicarse a un envío del mismo mensaje a todos los módulos de seguridad y en tal caso, se considera que el contenido de la zona de memoria objetivo es el mismo para todos los módulos. Si se realiza un direccionamiento individual, es posible que el contenido de cada memoria sea diferente. Una vez que el primer bloque de programa es generado, se mezcla con los datos de cada módulo de seguridad para crear tantos segundos bloques de programa.

Breve descripción de las figuras

La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere a los dibujos anexos que son dados a título de ejemplo en ningún caso limitativo, a saber:

- la figura 1 ilustra el procedimiento de generación del segundo bloque,

- la figura 2 ilustra el procedimiento de escritura en la memoria del módulo de seguridad.

Descripción detallada

Según una primera variante de realización, el contenido de la memoria objetivo es prerregistrado con valores pseudo-aleatorios. A la hora de la personalización de un tal módulo, se memorizan datos generados aleatoriamente MM_Ref por una parte en el módulo de seguridad MEM y por otra parte al centro de gestión.

Según una segunda variante de realización los datos prerregistrados están constituidos de un código programa que podría ser ejecutado por el procesador del módulo de seguridad. De hecho, este código no es ejecutado jamás y sirve de valor de inicialización de la región de actualización. Como en el ejemplo anterior, todos los módulos pueden tener el mismo programa artificial donde cada módulo recibe un programa diferente.

La figura 1 ilustra el procedimiento de formación de un segundo bloque de programa destinado a la difusión.

Cuando un bloque de programa PBI está listo para ser difundido, el método de la invención consiste en determinar la localización futura de este bloque en el módulo de seguridad. Una vez conocida esta localización, se puede recobrar el contenido que había sido programado durante la personalización gracias a los datos memorizados en el centro de gestión. Una vez conocidos estos datos, la operación consiste en mezclar estos datos con el bloque de programa PBI con el fin de obtener un nuevo bloque de datos SBI.

Esta operación de mezcla puede ser de tipo diferente. Lo más sencillo es utilizar una función XOR entre el bloque de programa PBI y los datos prerregistrados MM_Ref.

Un segundo ejemplo de mezcla consiste en cifrar cada reserva de memoria del bloque de programa PBI con el contenido de los datos prerregistrados MM_Ref.

El resultado de esta mezcla forma el segundo bloque de programa SBI. Este bloque así compuesto puede ser transmitido al módulo de seguridad concernido, según el modo de comunicación disponible entre el centro de gestión y el módulo de seguridad. Es cifrado por claves de cifrado del sistema según los métodos conocidos.

La figura 2 muestra los procesos de escritura en la memoria del módulo de seguridad.

La operación de escritura del nuevo bloque de programa en la memoria del módulo de seguridad, una vez recibido el segundo bloque, pasa por una operación de lectura del contenido de la reserva de memoria objetivo. Según nuestro ejemplo, cada reserva de memoria i de la zona objetivo MEM es leída y tratada (o mezclada) según el algoritmo elegido. En este ejemplo, cada reserva de memoria es mezclada con la reserva correspondiente i del segundo bloque SBI de programa. El resultado es inscrito en la memoria del módulo de seguridad.

Se debe señalar que el bloque de programa para actualizar es acompañado de datos de verificación según los modos conocidos (hash, CRC etcétera). Una vez almacenado el programa en la memoria del módulo, y debidamente verificado, puede ser activado habitualmente por la modificación de una parte del programa en la zona principal.

Este proceso puede ser recurrente es decir que si se desea modificar una parte en la zona de programa que ya ha acogido un programa, el antiguo programa hace el papel de valor prerregistrado. Según un ejemplo en el cual el nuevo programa ocuparía más espacio, el centro de gestión tomaría como valores prerregistrados, el contenido del programa precedente y para el espacio de memoria todavía no utilizado, utilizaría los valores prerregistrados generados durante la personalización.

En la práctica, el centro de gestión va a conservar un módulo de seguridad virtual cuyo contenido representa el contenido del módulo de seguridad en el entorno. Todos los programas destinados a los módulos de seguridad son introducidos igualmente en el módulo virtual.

Según una variante de realización, una parte solamente de la zona objetivo es prerregistrada por valores específicos, por ejemplo una reserva sobre tres. El resto se deja intacto. De este modo la mezcla será efectuada solamente sobre una reserva sobre tres, las otras reservas dejándose sin modificación.

Referencias citadas en la descripción

Esta lista de referencias citada por el solicitante ha sido recopilada exclusivamente para la información del lector. No forma parte del documento de patente europea. La misma ha sido confeccionada con la mayor diligencia; la OEP sin embargo no asume responsabilidad alguna por eventuales errores u omisiones.

Documentos patentes citados en la descripción

- US 2004107349 A [0013]

REIVINDICACIONES

1. Método de actualización protegida de software instalado en un módulo de seguridad, este método incluyendo las etapas siguientes:

- formación de un primer bloque de programa (PBI) de actualización,
- determinación de una zona de memoria objetivo de dicho módulo de seguridad,
- determinación para dicho módulo de seguridad, de un contenido prerregistrado (MM_Ref) en dicha zona de memoria objetivo,
- formación de un segundo bloque de programa (SBI) obtenido por la mezcla de todo o parte del contenido prerregistrado y del primer bloque de programa (PBI),
- transmisión del segundo bloque de programa (SBI) al módulo de seguridad,
- recepción del segundo bloque por el módulo de seguridad,
- lectura de la zona de memoria objetivo (MEM),
- obtención y escritura en la zona de memoria objetivo del primer bloque por la mezcla inversa de todo o parte del segundo bloque y del contenido de la zona de memoria objetivo.

2. Método según la reivindicación 1, **caracterizado** por el hecho de que la zona de memoria objetivo es prerregistrada por valores generados aleatoriamente.

3. Método según la reivindicación 1 poniendo en marcha un módulo que comprende un microprocesador, **caracterizado** por el hecho de que la zona de memoria objetivo es prerregistrada por un programa artificial no ejecutado por el microprocesador del módulo de seguridad.

4. Método según las reivindicaciones 1 a 3, **caracterizado** por el hecho de que la operación de mezcla es una función O exclusiva.

5. Método según las reivindicaciones 1 a 3, **caracterizado** por el hecho de que la operación de mezcla es una función de encriptación con el contenido de la memoria prerregistrada como clave de encriptación.

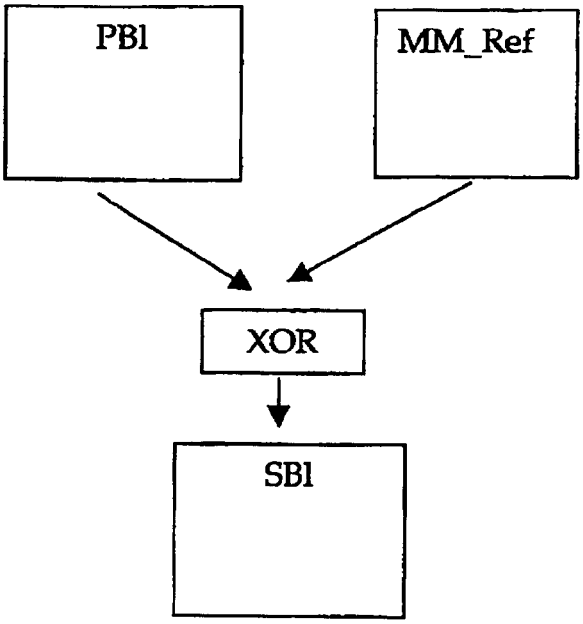

Fig. 1

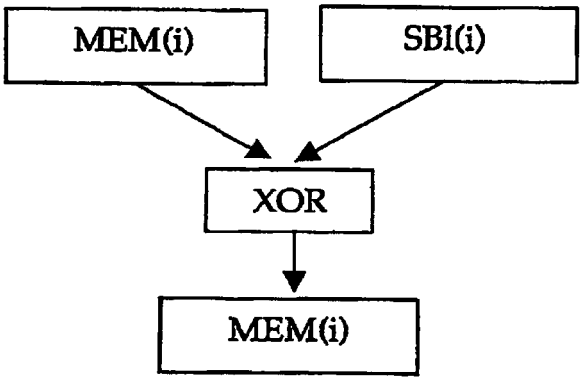

Fig. 2