(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 391 676**

(51) Int. CI.:
G06F 21/00 (2006.01)
G06F 21/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08172025 .2**
(96) Fecha de presentación: **17.12.2008**
(97) Número de publicación de la solicitud: **2079034**
(97) Fecha de publicación de la solicitud: **15.07.2009**

(54) Título: **Procedimiento de aseguramiento de un microprocesador, programa de ordenador y dispositivo correspondientes**

(30) Prioridad:
26.12.2007 FR 0760359

(45) Fecha de publicación de la mención BOPI:
28.11.2012

(45) Fecha de la publicación del folleto de la patente:
28.11.2012

(73) Titular/es:
COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE INGENICO (100.0%)
192 AVENUE CHARLES DE GAULLE
92220 NEUILLY SUR SEINE, FR

(72) Inventor/es:
NACCACHE, DAVID y
DABBOUS, NORA

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de aseguramiento de un microprocesador, programa de ordenador y dispositivo correspondientes.

1. Dominio del Invento

El campo del invento es el del aseguramiento de objetos con microprocesador, también llamado chip, y/o de programas destinados a estar integrados en tales objetos con chip.

El invento se aplica principalmente a los microprocesadores y/o programas integrados en las tarjetas con chip. Se han descrito por tanto a continuación esencialmente tales tarjetas con chip, pero el invento puede fácilmente ser puesto en práctica para cualquier tipo de objeto, principalmente portátil, equipado con tal chip, cualquiera que sea la naturaleza de éste último.

2. Técnica anterior

Se utilizan desde hace mucho tiempo tarjetas con chip, principalmente para identificar o autentificar un producto, una cuenta y/o una persona. El chip, o microprocesador, presenta por tanto una estructura específica de transistores, que define una lógica de tratamiento y zonas de memoria, de las que al menos una parte es asegurada, que contiene datos secretos.

Los documentos XP002322251 (KOMMER-LING O y COL. “Principios de diseño para procesadores de tarjeta inteligente resistente a falsificaciones”) y XP002329915 (HAGAI BAREL y COL “La Guía del Aprendiz de Brujo para Ataques por Defecto”) recogen diferentes tipos de ataques clásicos, que pretenden adivinar estos datos secretos, y los medios para protegerse de ellos.

Estos datos secretos, todavía llamados datos asegurados o críticos, son el objeto de diferentes tipos de medidas de protección, por ejemplo para impedir el clonado de las tarjetas en las que están almacenadas, o la obtención de informaciones (un código secreto de identificación) que permiten una utilización fraudulenta de una tarjeta robada.

Por ejemplo, una técnica de aseguramiento consiste en almacenar estos datos en zonas de memoria no accesibles, no modificables.

Existen también medidas de protección llamadas contramedidas, que consisten en ocultar el consumo de corriente de una tarjeta a un “observador exterior”, durante el funcionamiento de la tarjeta, enmascarando este consumo o presentando un consumo caótico de corriente, no representativo del consumo real de corriente en la tarjeta.

En efecto, a falta de poder acceder a los datos críticos, una persona malintencionada puede obtener, observando el consumo de corriente de una tarjeta durante su funcionamiento, informaciones explotables sobre las operaciones lógicas realizadas.

La puesta en práctica de estas contramedidas permite por tanto ocultar el consumo de corriente de una tarjeta durante su funcionamiento.

Esta técnica corresponde por ejemplo a la activación de operaciones lógicas suplementarias, no necesarias para el funcionamiento de la tarjeta, y que entrañan un consumo suplementario de corriente, no representativo del funcionamiento real de la tarjeta.

Estas contramedidas pueden ser activadas sistemáticamente durante el funcionamiento de la tarjeta, de manera que aseguren la protección de los datos críticos que pueden ser manipulados durante el funcionamiento, como se ha divulgado por ejemplo por el documento FR 2860 933 A.

Un inconveniente en esta técnica anterior reside en el hecho de que la activación de estas contramedidas es costosa en términos de consumo de energía de la tarjeta.

Además, otro inconveniente corresponde al hecho de que la activación de operaciones suplementarias es costosa en términos de tamaño de código.

Finalmente, esta técnica de aseguramiento basada en la activación de contramedidas es igualmente costosa en tiempos de programación.

Existe otra técnica de aseguramiento por contramedidas, que limita los inconvenientes citados más arriba y que consiste en activar las contramedidas solamente en ciertos momentos del funcionamiento de la tarjeta, como se ha divulgado por ejemplo por los documentos US 2001/016910 A1 o DE 198 28 936 A1.

Por ejemplo, el programa principal que asegura el funcionamiento de la tarjeta puede ser modificado de manera que prevea activar contramedidas en momentos definidos como críticos. Por ejemplo, estos momentos pueden corresponder a partes de código del programa, o a acciones programadas, que manipulan datos identificados como críticos. Estos momentos críticos son identificados por el autor del programa.

Un inconveniente de esta técnica reside en el hecho de que no garantiza que todos los datos críticos están bien asegurados, porque en el programador puede haber olvidado identificar una parte del código como crítica, o haber juzgado mal el nivel de seguridad de una acción o de una parte de código.

3. Exposición del Invento

El invento propone una solución nueva que no presenta el conjunto de estos inconvenientes de la técnica anterior, en forma de un procedimiento de aseguramiento de un microprocesador que contiene al menos un programa principal, que coopera menos con una memoria, comprendiendo dicho procedimiento una etapa de puesta en práctica de contramedidas, durante la cual operaciones suplementarias, no necesarias para dicho programa principal, son puestas en práctica de manera que modifiquen el consumo de corriente y/o el tiempo de tratamiento de dicho microprocesador.

Según el invento, tal procedimiento comprende las etapas siguientes:

- identificación de al menos una dirección o una zona de memoria de la o de dichas memorias, llamadas direcciones críticas, y que contiene, o es susceptible de contener, datos críticos para dicho programa principal;

- vigilancia de los puertos de direccionamiento de la o de dichas memorias, de manera que detecte un acceso a la o a dichas direcciones críticas;

- activación de dicha etapa de puesta en práctica de contramedidas, cuando un acceso a la o a dichas direcciones criticas es detectado.

Así, el invento descansa sobre una aproximación nueva e inventiva del aseguramiento de un microprocesador, basada en la identificación de zonas o de direcciones de memoria de almacenamiento para datos críticos que sirven para el funcionamiento del microprocesador, y sobre la activación de contramedidas en cada acceso a una o varias de las zonas o direcciones previamente identificadas.

Por ejemplo, estos datos sirven para un programa principal que asegura el funcionamiento del microprocesador. Los datos críticos para tal microprocesador pueden corresponder por ejemplo a códigos de identificación para una tarjeta que sirve para el pago electrónico, o a informaciones biométricas, por ejemplo para una tarjeta que permite un acceso seguro que necesita la autenticación de su usuario. Estos datos pueden igualmente ser utilizados para uno o varios periféricos que dialogan con la tarjeta.

Contrariamente a las disposiciones de la técnica anterior que identificaban los datos críticos ellas mismas para intentar protegerlas, el procedimiento según el invento identifica las zonas de memoria donde están almacenados estos datos y asegura todos los accesos a estas zonas de memorias, asegurando así los propios datos.

El aseguramiento de la tarjeta es asegurado por la activación de contramedidas, que permiten confundir o enmascarar la corriente durante los momentos en los que el funcionamiento de la tarjeta necesita un acceso a uno o varios datos críticos.

El procedimiento según el invento permite una optimización de la utilización de las contramedidas, únicamente durante los momentos “cruciales” del funcionamiento de la tarjeta, y no ya sistemáticamente durante el funcionamiento.

El procedimiento comprende en particular una etapa de vigilancia de los puertos de direccionamiento de la o de dichas memorias.

Así, cada acceso con una dirección crítica, por el programa principal de la tarjeta, o por uno de los periféricos, es vigilado y detectado de manera que active contramedidas. Así, la vigilancia de todos los accesos a las direcciones de memoria identificadas como críticas (almacenando pues datos críticos), permite optimizar el aseguramiento de estos datos críticos, de forma independiente a la elección del autor de un programa, contrariamente a una disposición de la técnica anterior. En efecto, al estar todos los datos críticos almacenados en zonas de memoria identificadas a su vez como críticas, la vigilancia sistemática del acceso, en lectura, escritura, ejecución de código, etc., a estas zonas de memoria permite activar contramedidas cada vez que uno de estos datos críticos es manipulado.

Según aspecto particular del invento, el procedimiento comprende una etapa de interrupción de dicha etapa de puesta en práctica de contramedidas, una vez que dicha o dichas llamadas direcciones críticas no son utilizadas.

Así, las contramedidas son desactivadas una vez que las direcciones identificadas como críticas no son ya utilizadas, de manera que se limiten los efectos costosos, en términos de tiempos, de consumo de corriente, etc., de la activación de las contramedidas.

En efecto, estas últimas no son activadas más que en el momento en el que uno o varios datos críticos son manipulados, siendo detectado este momento por una vigilancia del acceso a las direcciones críticas previamente identificadas.

Por ejemplo, dicha etapa de puesta en práctica de contramedidas comprende al menos una de las operaciones que pertenecen al grupo siguiente:

- realización de operaciones matemáticas o lógicas aleatorias;
- duplicación de operaciones efectuadas por dicho programa principal;
- lanzamiento de un programa secundario de camuflaje.

Así, las contramedidas pueden por ejemplo corresponder a operaciones matemáticas o lógicas que no sirven para el funcionamiento propiamente dicho de la tarjeta, sino que entrañan un sobreconsumo de corriente, impidiendo a un observador distinguir las operaciones útiles, y los datos críticos manipulados, de las operaciones unidas a las contramedidas.

Las contramedidas pueden corresponder a operaciones del programa principal, por ejemplo operaciones duplicadas, u operaciones de un programa secundario, llamado programa de camuflaje, que comprende únicamente operaciones de contramedidas, y eventualmente el código de vigilancia de los puertos de direccionamiento.

Según un modo de realización, dicha etapa de identificación designa al menos una dirección a una zona de memoria que comprende al menos uno de los elementos que pertenecen al grupo de comprende:

- una parte de código de dicho programa principal;
- datos asegurados.

Así, las direcciones críticas pueden ser identificadas como direcciones en las que se han almacenado directamente datos críticos, o bien direcciones en las que se han almacenado partes de código juzgadas igualmente críticas en sí mismas. Los datos críticos pueden ser por ejemplo informaciones biométricas, códigos de identificación, etc.

En particular, dichas memorias pertenecen al que comprende:

- las memorias RAM;
- las memorias ROM;
- las memorias EPROM;
- las memorias EEPROM;
- las memorias flash.

Otro aspecto del invento se refiere a un producto de programa de ordenador descargable desde una red de comunicación y/o registrado en un soporte legible por ordenador y/o ejecutable por un procesador, que comprende instrucciones de código de programa para la puesta en práctica del procedimiento de aseguramiento tal como se ha descrito previamente.

El invento se refiere igualmente a un dispositivo de microprocesador asegurado que contiene al menos un programa principal, que coopera con al menos una memoria, comprendiendo dicho dispositivo medios de puesta en práctica de contramedidas, durante la cual operaciones suplementarias, no necesarias para dicho programa principal, son empleadas de tal forma que modifiquen el consumo de corriente y/o el tiempo de tratamiento de dicho microprocesador.

Según el invento, tal dispositivo comprende:

- medios de identificación de al menos una dirección o una zona de memoria de dicha o de dichas memorias, llamadas direcciones críticas, y que contiene, o es susceptible de contener, datos críticos para dicho programa principal;
- medios de vigilancia de los puertos de direccionamiento de dicha o de dichas memorias, de manera que detecten un acceso a dicha o a dichas direcciones críticas;
- medios de activación de dicha etapa de puesta en práctica de contramedidas, cuando una acceso a dicha o a dichas direcciones críticas es detectado.

Tal dispositivo es particularmente apto para poner en práctica el procedimiento de aseguramiento descrito precedentemente.

Por ejemplo, tal dispositivo se presenta en forma de una tarjeta con microprocesador.

4. Lista de las figuras

Otras características y ventajas del invento aparecerán más claramente con la lectura de la descripción siguiente de un modo de realización particular, dada a título de simple ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, entre los que:

La fig. 1 presenta las principales etapas del procedimiento según el invento;

La fig. 2 ilustra un ejemplo de un dispositivo de aseguramiento que pone en práctica una técnica de aseguramiento según un modo de realización del invento.

5. Descripción de un modo de realización del invento

5.1 Principio General

El principio general del invento descansa sobre la identificación y la vigilancia de direcciones de memoria, o de zonas de memoria, críticas, es decir en las que están almacenados, o pueden ser almacenados, datos críticos, en un microprocesador. A cada acceso de una de estas direcciones críticas son activadas contramedidas, que permiten el aseguramiento de datos manipulados durante estos accesos de memoria.

El procedimiento según el invento permite la optimización de la activación de las contramedidas en momentos cruciales del funcionamiento del microprocesador, y por tanto la optimización del aseguramiento de datos críticos en el microprocesador.

5.2 Descripción de un modo de realización

Se presentan, en relación con las figs. 1 y 2, las principales etapas del procedimiento de aseguramiento según un modo de realización del invento.

Se considera un microprocesador, o una tarjeta, que contiene al menos un programa principal 20. Por ejemplo, esta tarjeta es una tarjeta de pago electrónico. Un usuario puede servirse de ella para un pago electrónico, o para una retirada de especies de un distribuidor, y debe identificarse con un código personal. Este código personal forma principalmente parte de los datos críticos a asegurar, y por tanto a salvaguardar en una o varias zonas de memoria específicas que cooperan con el microprocesador. La parte de código que permite la autenticación del usuario de la tarjeta puede igualmente formar parte de los datos a asegurar. Ciertas informaciones que se refieren por ejemplo a las coordenadas bancarias del usuario pueden igualmente estar almacenadas en una zona de memoria a asegurar

Durante una primera etapa 10, el procedimiento de aseguramiento según el invento identifica una o varias zonas de memoria 22, 23, que contienen o susceptibles de contener datos críticos. Estas zonas de memoria, 22, 23 pueden ser utilizadas por el programa principal, o por uno o varios periféricos 24 que interactúan con el microprocesador.

Estas zonas de memoria están referenciadas, por puertos de direccionamiento, y contienen en particular los datos críticos descritos más arriba, tales como el código de identificación del usuario, sus coordenadas bancarias, y la parte del programa principal que permite la autenticación del usuario. Una vez que se han identificado estas zonas de memoria, el autor del programa principal deber tener en cuenta para almacenar todos los datos críticos utilizados en el programa principal en estas zonas de memoria específicas.

Así, contrariamente a la técnica anterior en que las acciones para asegurar deben ser identificadas antes, o en el momento de la programación del programa principal, para activar en consecuencia las contramedidas, las zonas de memoria son aquí identificadas antes de la programación, y el autor del programa debe simplemente tenerlas en cuenta para almacenar en ellas los datos críticos.

Según este modo de realización del invento, un programa de vigilancia 21, distinto del problema principal, es el encargado de vigilar, durante una etapa 11, los puertos de direccionamiento de estas zonas de memoria 22, 23, previamente identificadas.

Así, una vez que el problema principal 20, o un periférico 24, accede a una de las zonas de memoria, 22, 23, el programa de vigilancia emite una alerta, que activa las contramedidas 25 previstas para asegurar los datos manipulados por el acceso de memoria en cuestión. Esta activación de las contramedidas (etapa 12), corresponde por ejemplo a la activación de una banderola o indicador, que indica que un acceso a una dirección de memoria crítica está en curso.

Por ejemplo, el programa de vigilancia puede comprender una sucesión de ensayos, que consisten en detectar todos los accesos a los puertos de direccionamiento de las zonas de memoria 22, 23, y en activar contramedidas en cada detección positiva.

Las contramedidas 25 pueden estar descritas en el programa de vigilancia y pueden corresponder por ejemplo a una sucesión de operaciones matemáticas aleatorias, puestas en práctica durante toda la duración del acceso a la dirección de memoria detectada.

Así, todas las acciones relativas al acceso a la dirección de memoria, es decir todas las acciones que manipulan uno

o varios datos críticos, son enmascaradas por contramedidas activadas durante toda la duración del acceso de memoria, y así aseguradas.

Al final de cada acceso a una zona de memoria crítica 22, 23, las contramedidas son desactivadas, para evitar un sobreconsumo de corriente inútil.

Según una variante de este modo de realización, contramedidas suplementarias pueden igualmente ser puestas en práctica, en el programa principal. Por ejemplo, el autor del programa principal puede desear asegurar una parte del código del programa principal, que no hacen intervenir datos críticos, pero que necesitan según él un cierto grado de seguridad. Puede entonces activar contramedidas, activando una banderola en el código, según el mismo principio que la activación de las contramedidas descrita precedentemente.

REIVINDICACIONES

1. Un procedimiento de aseguramiento de un microprocesador que contiene al menos un programa principal, que coopera con al menos una memoria, comprendiendo dicho procedimiento una etapa de puesta en práctica de contramedidas, durante la cual operaciones suplementarias, no necesarias para dicho programa principal, son puestas en práctica de manera que modifiquen el consumo de corriente y/o el tiempo de tratamiento de dicho microprocesador durante la utilización de una parte de código crítico para dicho programa principal, caracterizado porque comprende las etapas siguientes:

- identificación de al menos una zona de memoria de dicha o de dichos memorias, llamadas zonas críticas, y que contiene, o es susceptible de contener, dicha parte de código;

- vigilancia de los puertos de direccionamiento de dicha o de dichas memorias, de manera que detecte un acceso a dicha o a dichas zonas criticas;

- activación de dicha etapa de puesta en práctica de contramedidas, cuando se ha detectado un acceso a dicha o a dichas zonas críticas.

2. Un procedimiento según la reivindicación 1, caracterizado porque comprende una etapa de interrupción de dicha etapa de puesta en práctica de contramedidas, una vez que dicha o dichas llamadas zonas críticas no son ya utilizadas.

3. Un procedimiento según una cualquiera de las reivindicaciones 1 y 2, caracterizado porque dicha etapa de puesta en práctica de contramedidas comprende al menos una de las operaciones que pertenecen al grupo siguiente:

- realización de operaciones matemáticas o lógicas aleatorias;

- duplicación de operaciones efectuadas por dicho programa principal;

- lanzamiento de un programa secundario de camuflaje.

4. Un procedimiento según una cualquiera de las reivindicaciones 1 a 3, caracterizado porque dichas memorias pertenecen al grupo que comprende:

- las memorias RAM;

- las memorias ROM;

- las memorias EPROM;

- las memorias EEPROM;

- las memorias flash.

5. Un producto de programa de ordenador descargable desde una red de comunicación y/o grabado o registrado sobre un soporte legible por ordenador y/o ejecutable por un procesador, caracterizado porque comprende instrucciones de código de programa para la puesta en práctica del procedimiento de aseguramiento según una al menos de las reivindicaciones 1 a 4.

6. Un dispositivo con microprocesador asegurado que contiene al menos un programa principal, que coopera con al menos una memoria, comprendiendo dicho dispositivo medios de puesta en práctica de contramedidas, durante la cual operaciones suplementarias, no necesarias para dicho programa principal, son puestas en práctica de manera que modifiquen el consumo de corriente y/o el tiempo de tratamiento de dicho microprocesador, durante la utilización de una parte de código crítico para dicho programa principal, caracterizado porque comprende:

- medios de identificación de al menos una zona de memoria de dicha o de dichas memorias, llamadas zonas críticas, y que contiene, o es susceptible contener, dicha parte código;

- medios de vigilancia de los puertos de direccionamiento de dicha o de dichas memorias, de manera que detecte un acceso a dicha o a dichas zonas críticas;

- medios de activación de dicha etapa de puesta en práctica de contramedidas, cuando un acceso a dicha o a dichas zonas críticas es detectado.

7. Un dispositivo según la reivindicación 6, caracterizado porque se presenta en forma de una tarjeta con microprocesador.

Figura 1

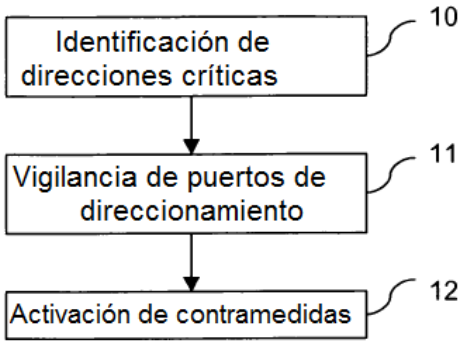

Figura 2