

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 966 156**

51 Int. Cl.:

G06F 21/55 (2013.01)

G06F 21/86 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **09.04.2019** **PCT/EP2019/058903**

87 Fecha y número de publicación internacional: **17.10.2019** **WO19197377**

96 Fecha de presentación y número de la solicitud europea: **09.04.2019** **E 19715122 (8)**

97 Fecha y número de publicación de la concesión europea: **15.11.2023** **EP 3776302**

54 Título: **Método para activar sensores en un dispositivo de múltiples unidades**

30 Prioridad:

12.04.2018 EP 18305451

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

18.04.2024

73 Titular/es:

THALES DIS FRANCE SAS (100.0%)

6, rue de la Verrerie

92190 Meudon, FR

72 Inventor/es:

LOUBET MOUNDI, PHILIPPE y

CHARBONNIER, SYLVAIN

74 Agente/Representante:

DEL VALLE VALIENTE, Sonia

ES 2 966 156 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para activar sensores en un dispositivo de múltiples unidades

5 Campo de la invención

La presente invención se refiere al campo de la protección de chip contra ataques y, más particularmente, a un método y un dispositivo correspondiente que permite una activación de hardware de los sensores de seguridad de una unidad de cálculo solamente cuando ejecuta código de software.

10 Antecedentes de la invención

Los sistemas informáticos se usan comúnmente para realizar operaciones en datos confidenciales, tales como operaciones de cifrado o descifrado. Los ataques, tales como ataques de fallo, han sido diseñados por los cuales un atacante puede obtener acceso a dichos datos confidenciales, por ejemplo, perturbando la ejecución de un código de software por un chip de procesamiento para hacer que produzca errores de ejecución.

Para proteger los chips de procesamiento y los datos sensibles que procesan contra tales ataques, los sensores de seguridad están integrados en dispositivos de procesamiento. Dichos sensores monitorizan el comportamiento y el entorno de un dispositivo de procesamiento para detectar un comportamiento defectuoso que probablemente resultaría de un ataque. Cuando se detecta tal ataque, pueden tomar medidas que impiden que un atacante pueda acceder a datos confidenciales, por ejemplo, activando la activación de las medidas de contador.

Un inconveniente de usar tales sensores es que cuanto mayor es su sensibilidad, mayor es la probabilidad de detección de falso positivo que conduce a la activación de contramedidas mientras no está en curso ningún ataque. Esto puede ser un problema, ya que la contramedida puede pasar para matar un proceso o restablecer un dispositivo. En consecuencia, se han buscado soluciones para minimizar el riesgo de detección de falsos positivos. Una solución existente es controlar la activación y desactivación de los sensores por software y para insertarse en el código de software para ser ejecutado por un chip que activa y desactiva los sensores de seguridad de ese chip. Dicha solución tiene numerosos inconvenientes: aumenta el tamaño del código de software, disminuye su legibilidad, requiere ingenieros de software para insertar comandos manualmente en su código, puede dar como resultado cálculos realizados sin los sensores de seguridad requeridos activados o en los otros sensores de seguridad de mano activados mientras no es necesario cuando una o más comandos de activación/desactivación no se insertan correctamente en un código de software a ejecutar.

En consecuencia, existe la necesidad de un método que permita activar sensores de seguridad de un chip solo cuando sean necesarios, es decir, solo cuando el chip ejecuta código de software, sin impacto en el código de software que se ejecutará. El documento US 2017/357829 A1 describe un circuito integrado que incluye un circuito interno y un circuito de detección de ataque que incluye al menos un sensor configurado para detectar al menos una condición anormal del circuito interno. El documento US 2018/097825 A1 describe un aparato que comprende circuitos detectores para generar datos del sensor local basándose en una señal del sensor recibida desde un sensor incorporado en un dispositivo informático local cuya lógica de monitor está conectada al dispositivo informático local para identificar un evento en base a los datos del sensor local.

45 Resumen de la invención

La invención se define por las reivindicaciones independientes. Otras realizaciones de la invención están definidas por las reivindicaciones dependientes.

50 Breve descripción de las figuras

La siguiente descripción y los dibujos adjuntos exponen en detalle ciertos aspectos ilustrativos y son indicativos de tan solo algunas de las diversas maneras en las que pueden emplearse los principios de las realizaciones. Otras ventajas y características novedosas resultarán evidentes a partir de la siguiente descripción detallada cuando se considere junto con los dibujos y se pretende que las realizaciones descritas incluyan todos tales aspectos y sus equivalentes, siempre que estén incluidas en el alcance de las reivindicaciones adjuntas.

- la Figura 1 es una ilustración esquemática de un dispositivo de múltiples unidades según la presente invención;

- la Figura 2 es una ilustración esquemática de un método para activar al menos un sensor entre una pluralidad de sensores integrados en un dispositivo de múltiples unidades según una realización de la presente invención.

Descripción detallada de las realizaciones de la invención

En la descripción detallada a continuación, se hace referencia a los dibujos adjuntos que muestran, a modo de ilustración, realizaciones específicas en las que puede ponerse en práctica la invención. Estas realizaciones se

describen con detalle suficiente para permitir que los expertos en la técnica pongan en práctica la invención. Debe entenderse que, aunque sean diferentes, las diversas realizaciones de la invención no son necesariamente mutuamente excluyentes. Por ejemplo, un rasgo, estructura o característica particular descrito en el presente documento en relación con una realización puede implementarse en otras realizaciones sin salirse del alcance de la invención. Además, debe entenderse que la ubicación o la disposición de elementos individuales en cada realización descrita puede modificarse sin salirse del alcance de la invención. La descripción detallada a continuación, por lo tanto, no debe tomarse en un sentido limitativo, y el alcance de la presente invención está definido únicamente por las reivindicaciones adjuntas, debidamente interpretadas, junto con el rango completo de equivalentes a los que tienen derecho las reivindicaciones.

La invención tiene como objetivo activar los sensores integrados en un dispositivo de múltiples unidades solamente cuando es útil, es decir, cuando los circuitos que protegen están siendo utilizados para realizar un cálculo.

La **Figura 1** muestra tal dispositivo 100 de múltiples unidades según la invención. Incluye al menos dos unidades 101a, 101b... de ejecución de código y una pluralidad de sensores 102a, 102b... Un dispositivo de múltiples unidades de este tipo puede, por ejemplo, mediante una CPU de múltiples núcleos o GPU, o un sistema en chip (SoC), o el chip de una tarjeta inteligente, también llamada elemento de seguridad. Las unidades de ejecución de código pueden ser, por ejemplo, núcleos de CPU o coprocesadores.

El dispositivo 100 de múltiples unidades también incluye una pluralidad de sensores 102a, 102b... Dichos sensores están configurados para detectar ataques que pueden producirse durante una ejecución por el dispositivo de múltiples unidades de un código de software que comprende instrucciones de código informático. Cada sensor puede asociarse a una unidad de ejecución de código. Dichos sensores pueden ser, por ejemplo, sensores de temperatura, sensores de fallo, sensores de tensión, sensores de luz, sensores de frecuencia, sensores de corriente, sensores de integridad digital...

El dispositivo 100 de múltiples unidades también incluye un circuito 103 de activación de sensor. Es un circuito de hardware que se encarga de la activación y desactivación de los sensores cuando la unidad de ejecución de código a la que se asocian se usa o no se usa. Puede ser un circuito dedicado, o puede ser un circuito que tenga otras funciones en el dispositivo de múltiples unidades, tal como gestión de acceso a la memoria o gestión de bus.

El dispositivo 100 de múltiples unidades también incluye al menos una memoria 104 que incluye una memoria 104a de acceso aleatorio (RAM), una memoria 104b de solo lectura (ROM) y/o una memoria 104c no volátil (NVM).

Más precisamente, la invención se refiere a un método para activar al menos un sensor entre la pluralidad de sensores integrados en el dispositivo de múltiples unidades. Las etapas de este método, representadas en la **Figura 2** y descritas aquí después, se ejecutan por el circuito de activación del sensor antes de la ejecución de una instrucción de código informático del código de software mediante una unidad de ejecución de código del dispositivo de múltiples unidades.

En una primera etapa S1, el circuito de activación del sensor determina la unidad de ejecución de código que se configura para ejecutar dicha instrucción.

En una segunda etapa S2, el circuito de activación del sensor activa solo los sensores asociados con la unidad de ejecución de código determinada.

Al hacerlo, los sensores que protegen una unidad de ejecución de código se activan solo justo antes de ejecutar algún código de software. No se activan demasiado por adelantado para evitar la detección de un falso ataque mientras que la unidad de ejecución de código no realiza ningún cálculo. Además, dicha solución no tiene impacto en el propio código de software. Dado que la activación de los sensores es realizada por el circuito de activación del sensor por sí misma, no es necesario añadir ninguna instrucción adicional relacionada con la activación de los sensores en el código de software.

El método según la invención puede comprender una tercera etapa S3 también realizada por el circuito de activación del sensor, que se activa por la finalización de la ejecución de una instrucción de código informático, durante la cual el circuito de activación del sensor desactiva los sensores asociados con la unidad de ejecución de código determinada en la primera etapa S1. Tal finalización puede indicarse, por ejemplo, mediante una señal devuelta por la unidad de ejecución de código, mediante un cambio de estado de la unidad de ejecución de código a un estado inactivo o por un cambio en una señal de reloj proporcionada a la unidad de ejecución de código. Al hacerlo, los sensores de una unidad de ejecución de código se desactivan una vez que la unidad de ejecución de código ya no se usa para realizar cálculos.

Como resultado, los sensores de una unidad de ejecución de código permanecen activados solo cuando sea necesario, solo mientras que la unidad de ejecución de código ejecuta código de software.

Durante la primera etapa S1, la determinación de la unidad de ejecución de código configurada para ejecutar dicha instrucción puede realizarse por el circuito de activación del sensor mediante la detección de una activación de la unidad de ejecución de código.

5 Por ejemplo, tal activación puede detectarse detectando que se proporciona una señal de reloj a la unidad de ejecución de código por un circuito de reloj, detectando una señal de selección de chip dirigida a la unidad de ejecución de código o monitorizando un estado de la unidad de ejecución y detectando que la unidad de ejecución de código no está en un estado inactivo o en estado de ahorro de energía.

10 En otra realización, el circuito de activación del sensor determina la unidad de ejecución de código configurada para ejecutar una instrucción detectando un acceso de memoria a un rango específico de direcciones de memoria de la memoria 104 del dispositivo de múltiples unidades dedicado a una unidad de ejecución de código específico. Dicho acceso a memoria puede revelar de hecho una lectura en la memoria de datos usada como una entrada a un cálculo que va a realizarse por la unidad de ejecución de código.

15 Para evitar desactivar los sensores de una unidad de ejecución de código después de cada cálculo cuando la misma unidad de ejecución realiza varias ejecuciones de instrucciones uno después del otro, el circuito de activación del sensor puede esperar un retardo predeterminado después de la finalización de la ejecución de una instrucción de código informático antes de apagar cualquier sensor. Si las unidades de ejecución de código comienzan a realizar un nuevo cálculo antes de que haya transcurrido el retardo, los sensores de la unidad de ejecución de código ya no deben desactivarse y la unidad de activación de sensor puede restablecer la cuenta regresiva, esperar que la unidad de ejecución de código deje de ejecutar instrucciones, y luego esperar nuevamente el retardo predeterminado antes de desactivar los sensores.

25 Según un segundo aspecto, la invención se refiere a un producto programa informático directamente cargable en la memoria de al menos un ordenador, que comprende instrucciones de código de software para realizar, cuando dicho producto se ejecuta en el ordenador, las etapas del método descrito aquí anteriormente.

30 Según un tercer aspecto, la invención se refiere al dispositivo de múltiples unidades descrito aquí antes, que comprende:

- una pluralidad de sensores 102a, 102b...,
- al menos dos unidades 101a, 101b... de ejecución de código,
- y un circuito 103 de activación de sensor,

40 dichos sensores están configurados para detectar ataques durante una ejecución por dicho dispositivo de múltiples unidades de un código de software que comprende instrucciones de código informático, y,

estando asociado cada sensor a una unidad de ejecución de código y,

45 estando configurado dicho 103 circuito de activación del sensor para realizar, antes de la ejecución de una instrucción de código informático de dicho código de software mediante una de dichas unidades de ejecución de código, las etapas del método descrito aquí anteriormente.

50 Además de estas características, el programa informático según el segundo aspecto de la invención y el dispositivo de múltiples unidades según el tercer aspecto de la invención puede configurarse para realizar o puede comprender cualquier otra característica descrita anteriormente.

55 Por lo tanto, el método y los sistemas propuestos permiten activar los sensores de las unidades de ejecución de código del dispositivo de múltiples unidades solo cuando se necesitan, activar los sensores de una unidad de ejecución solo durante la ejecución por esta unidad de código de software que manipula datos a proteger, y sin requerir ninguna modificación del propio código de software.

REIVINDICACIONES

1. Un método para activar al menos un sensor entre una pluralidad de sensores (102a, 102b...) incrustado en un dispositivo (100) de múltiples unidades, estando configurado dicho al menos un sensor para detectar ataques durante una ejecución por dicho dispositivo de múltiples unidades de un código de software que comprende instrucciones de código informático, en donde:
5
10 dicho dispositivo de múltiples unidades comprende al menos dos unidades (101a, 101b...) de ejecución de código operables para ejecutar al menos una instrucción de código informático del código de software y un circuito (103) de activación de sensor, y cada sensor está asociado a una unidad de ejecución de código, y comprendiendo dicho método, realizado por dicho circuito (103) de activación de sensor antes de la ejecución de una instrucción de código informático de dicho código de software mediante una de dichas unidades de ejecución de código:
15
-determinar (S1) la unidad de ejecución de código configurada para ejecutar dicha instrucción,
-activar (S2) solo los sensores asociados con la unidad de ejecución de código determinada;
20 activada al finalizar la ejecución de dicha instrucción de código informático, desactivar (S3) dichos sensores asociados con la unidad de ejecución de código determinada.
2. El método de la reivindicación 1, en donde la etapa de determinar (S1) la unidad de ejecución de código configurada para ejecutar dicha instrucción comprende detectar la activación de la unidad de ejecución de código.
25
3. El método de la reivindicación 1, en donde dicho dispositivo de múltiples unidades comprende una memoria y la etapa de determinar (S1) la unidad de ejecución de código configurada para ejecutar dicha instrucción comprende detectar un acceso de memoria a un intervalo específico de direcciones de memoria de dicha memoria dedicada a dicha unidad de ejecución de código.
30
4. El método de la reivindicación 1, en donde la etapa de determinar (S1) la unidad de ejecución de código configurada para ejecutar dicha instrucción comprende detectar que proporciona una señal de reloj a la unidad de ejecución de código.
35
5. El método de la reivindicación 1, que comprende esperar un retardo predeterminado después de completar la ejecución de dicha instrucción de código informático antes de apagar un sensor.
40
6. Un producto de programa informático directamente cargable en la memoria de al menos un ordenador, que comprende instrucciones de código de software para realizar las etapas de la reivindicación 1 cuando dicho producto se ejecuta en el ordenador.
45
7. Dispositivo (100) de múltiples unidades que comprende:
45
-una pluralidad de sensores (102a, 102b...),
-al menos dos unidades (101a, 101b...) de ejecución de código operables para ejecutar al menos una instrucción de código informático del código de software
50 -y un circuito (103) de activación del sensor,
dichos sensores están configurados para detectar ataques durante una ejecución por dicho dispositivo de múltiples unidades de un código de software que comprende instrucciones de código informático, y,
55 estando asociado cada sensor a una unidad de ejecución de código y, estando configurado dicho circuito (103) de activación del sensor para realizar, antes de la ejecución de una instrucción de código informático de dicho código de software por una de dichas unidades de ejecución de código, las etapas de las reivindicaciones 1 a 5.
8. El dispositivo de múltiples unidades de la reivindicación 7, en donde cada unidad (101a, 101b...) de ejecución de código está entre un núcleo de CPU o un coprocesador.
60
9. El dispositivo de múltiples unidades de la reivindicación 7, siendo dicho dispositivo (100) de múltiples unidades entre una CPU de múltiples núcleos o GPU, un sistema en chip o el chip de una tarjeta inteligente.

10. El dispositivo de múltiples unidades de la reivindicación 7, en donde los sensores (102a, 102 b...) están entre sensores de temperatura, sensores de fallo, sensores de tensión, sensores de luz, sensores de frecuencia, sensores de corriente, sensores de integridad digital.

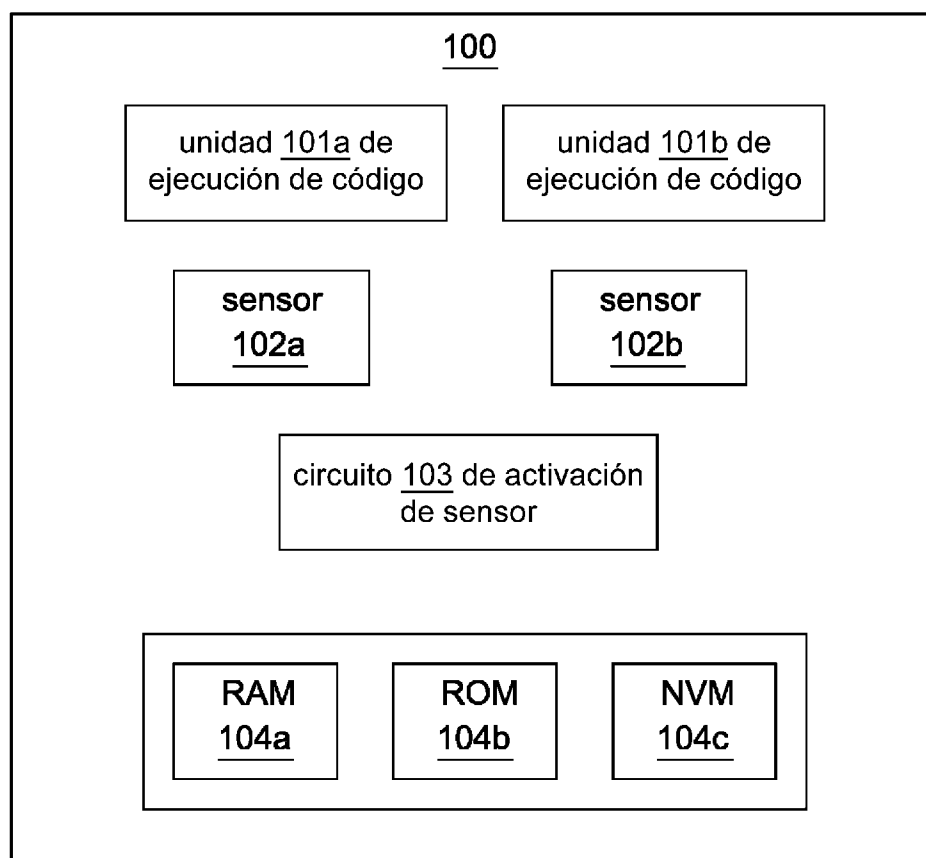


Fig. 1

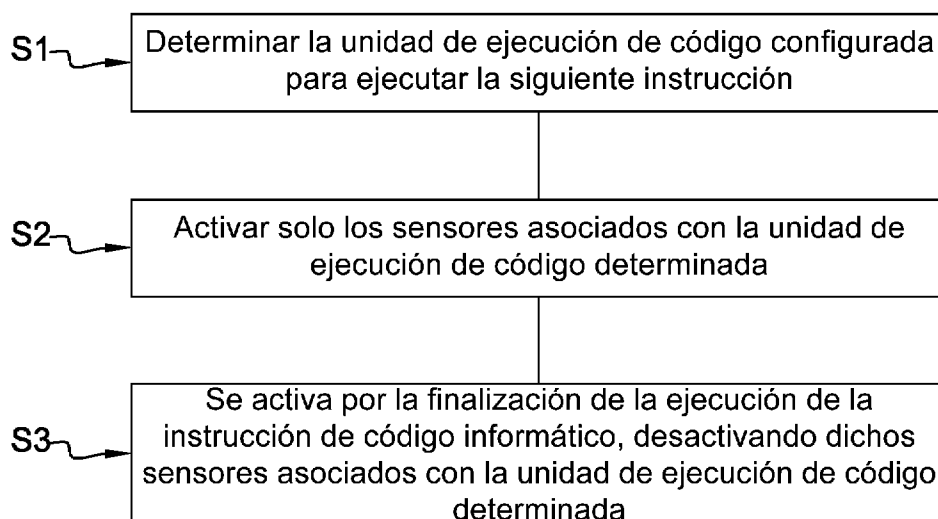


Fig. 2