(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 382 099**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08856161 .8**
(96) Fecha de presentación: **21.11.2008**
(97) Número de publicación de la solicitud: **2215580**
(97) Fecha de publicación de la solicitud: **11.08.2010**

(54) Título: **Procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, y dispositivo que comprende un módulo de control correspondiente**

(30) Prioridad:
26.11.2007 FR 0708242

(45) Fecha de publicación de la mención BOPI:
05.06.2012

(45) Fecha de la publicación del folleto de la patente:
05.06.2012

(73) Titular/es:
MORPHO
27, RUE LEBLANC
75015 PARIS, FR

(72) Inventor/es:
PELLETIER, Hervé y
DUMAS, Pascal

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, y dispositivo que comprende un módulo de control correspondiente.

La invención se refiere a un procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, que comprende un acceso o puerta de entrada-salida, un microprocesador, una memoria viva, una memoria muerta y una memoria no volátil y reprogramable que contiene una variable de estado de fin de vida del dispositivo electrónico, gobernada por un módulo de control.

Tales dispositivos electrónicos corresponden, de manera no exclusiva, a las tarjetas electrónicas o a cualquier dispositivo electrónico que comprenda al menos, o entre en relación con, una tarjeta de microprocesador, para la cual se requiera una buena resistencia de seguridad frente a cualquier intrusión externa.

A fin de garantizar una buena resistencia de seguridad de las tarjetas antes mencionadas, se activa un mecanismo de paso a fin de vida con la detección de un cierto número de errores críticos.

Los procedimientos de paso a fin de vida de este tipo de dispositivo, en particular por lo que concierne a las tarjetas de microprocesador, se presentan, sin embargo, problemáticos, ya que tal procedimiento se apoya, globalmente, en un procedimiento de escritura en memoria reprogramable y no volátil, generalmente una memoria EEPROM [memoria de solo lectura programable y susceptible de borrarse eléctricamente –“electrically erasable programmable read-only memory”], procedimiento de escritura que tiene como propósito el borrado de los datos y el bloqueo de las aplicaciones.

Tal procedimiento parece, no obstante, vulnerable, puesto que es detectable fuera de la tarjeta, en razón, sobre todo, de la fuerte demanda de corriente generada por el procedimiento de escritura en memoria reprogramable y la demanda, además, de un cierto tiempo por parte del ejecutor.

Un tercero malintencionado dispone, por tanto, de la perfecta oportunidad para impedir la ejecución de semejante procedimiento, cortando la alimentación eléctrica del dispositivo o de la tarjeta.

Los documentos FR-2.776.410-A y FR-2.784.763-A divulgan diferentes mecanismos de ocultación de las operaciones efectuadas en una tarjeta de microprocesador.

La presente invención tiene, en consecuencia, como propósito hacer que el procedimiento de paso a fin de vida de un tal dispositivo electrónico sea totalmente cierto o efectivo dentro de un retardo aleatorio tras el suceso, error crítico, en el origen del desencadenamiento del paso a fin de vida, al ocultar, en particular, a todos los terceros, la operación de escritura en memoria no volátil correspondiente al paso a fin de vida, lo que prohíbe, en la práctica, cualquier ataque por vía o canal oculto.

Según un aspecto remarcable, la invención tiene como propósito la ocultación de toda escritura de una variable de estado de paso a fin de vida en la memoria no volátil de un dispositivo electrónico, por medio de la dilución de esta operación de escritura en el desarrollo normal del programa de aplicación ejecutado por el dispositivo electrónico.

El procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, objeto de la invención, se aplica a cualquier dispositivo electrónico que comprenda un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil y reprogramable que contenga una variable de estado de fin de vida generada por un módulo de control, y un acceso o puerta de entrada / salida.

Cabe destacar que, en el momento del arranque o puesta en marcha del dispositivo electrónico, este consiste en cargar en la memoria viva, a partir de la memoria no volátil, el valor de la variable de estado de fin de vida, y, antes de la ejecución de cualquier orden en curso por parte del microprocesador, verificar si el valor de esta variable de estado de fin de vida memorizada en la memoria viva se encuentra en el valor no verdadero, y, con la respuesta negativa a esta verificación, llevar a cabo las operaciones de paso a fin de vida del dispositivo electrónico; en caso contrario, si la variable de estado de fin de vida memorizada en la memoria viva se encuentra en el valor no verdadero, proseguir con la inicialización o la ejecución de la orden en curso por parte del microprocesador del dispositivo electrónico, y, con la detección de un ataque intrusivo, instaurar por escritura, en la única memoria viva, la variable de estado de fin de vida del dispositivo electrónico en el valor verdadero y proseguir con la inicialización y/o la ejecución de la orden en curso, y diferir la escritura de la variable de estado de fin de vida en el valor verdadero en la memoria no volátil, para efectuarla en lugar de la próxima operación de escritura en memoria no volátil, lo que permite ocultar la inscripción de la variable de estado de fin de vida.

El procedimiento objeto de la invención es igualmente remarcable porque consiste, además, previamente a la ejecución de cada orden por parte del microprocesador, en cargar en la memoria viva, a partir de la memoria no volátil, el valor de la variable de estado de fin de vida.

El procedimiento objeto de la invención es igualmente remarcable porque, para un conjunto de órdenes ejecutadas por el microprocesador del dispositivo electrónico que incluye órdenes que comprenden una inscripción sistemática

en memoria no volátil y órdenes que no comprenden inscripción en memoria no volátil, consiste, además, independientemente de detección o de la no detección de un ataque intrusivo, en llevar a cabo la escritura en memoria no volátil de un octeto facticio, lo que permite ocultar toda escritura, eventualmente, de la variable de estado de fin de vida del dispositivo electrónico en la memoria no volátil.

Preferiblemente, la operación de escritura en memoria no volátil de este octeto facticio se lleva a cabo en la misma página de memoria que la de la variable de estado de fin de vida.

Por otra parte, de acuerdo con otro aspecto remarcable del procedimiento objeto de la invención, la operación de escritura en memoria no volátil de este octeto facticio se lleva a cabo previamente a cualquier ejecución de la operación de transmisión de datos por la conducción de la puerta de entrada / salida del dispositivo electrónico.

De acuerdo con otro aspecto remarcable, el procedimiento objeto de la invención incluye, además, consecutivamente a cualquier etapa de escritura en memoria volátil de la variable de estado de fin de vida, una etapa consistente en verificar en el valor verdadero el valor de la variable de estado de fin de vida, y, con la verificación de este valor verdadero, una etapa de ejecución de las operaciones de paso a fin de vida del dispositivo electrónico.

De acuerdo con otro aspecto, el procedimiento de la invención es, además, remarcable porque, con la verificación de que el valor de esta variable de estado de fin de vida se encuentra en el valor verdadero, se sustituye por la operación de escritura en memoria no volátil de este octeto facticio, la operación de escritura en memoria no volátil del valor de la variable de estado de fin de vida.

El dispositivo electrónico objeto de la invención comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil y reprogramable que contiene una variable de estado de fin de vida del dispositivo electrónico, gobernada por un módulo de control, y un acceso o puerta de entrada / salida (I/O). Es remarcable por cuanto que este módulo de control incluye un módulo de programa informático de ejecución de las etapas del procedimiento objeto de la invención previamente citadas.

El procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, y el dispositivo electrónico que incluye un módulo de control correspondiente, objetos de la invención, encuentran aplicación en todo tipo de dispositivos electrónicos pero, de manera preferida aunque no limitativa, en dispositivos electrónicos tales como las tarjetas de microprocesador que tratan y/o almacenan datos personales, privados o secretos.

Estos se comprenderán mejor por la lectura de la descripción y por la observación de las figuras que se acompañan, en las cuales:

- la Figura 1a representa, a título puramente ilustrativo, un organigrama o diagrama de flujo de las etapas esenciales de puesta en práctica del procedimiento objeto de la invención;
- la Figura 1b representa, a título puramente ilustrativo, un diagrama de flujo de las diferentes etapas llevadas a cabo en el curso de la puesta en práctica del procedimiento objeto de la invención, ilustrado en la Figura 1a;
- las Figuras 1c a 1f representan detalles de la puesta en práctica de las etapas del procedimiento ilustrado en la Figura 1a;
- la Figura 2 representa, a título puramente ilustrativo, en forma de diagrama funcional, la arquitectura o estructura de un dispositivo electrónico provisto de un módulo de control de paso a fin de vida, de conformidad con el objeto de la presente invención.

Se proporcionará, a continuación, en relación con las Figuras 1a a 1f, una descripción más detallada del procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, de acuerdo con el objeto de la presente invención.

De una manera general, se indica que el procedimiento de ocultación de paso a fin de vida de una tarjeta electrónica, objeto de la presente invención, se aplica a cualesquiera dispositivos electrónicos que comprendan un microprocesador, una memoria viva, una memoria muerta y una memoria no volátil y reprogramable que contiene una variable de estado de fin de vida del dispositivo electrónico, gobernada por un módulo de control. De manera más particular, el dispositivo electrónico puede comprender, igualmente, un acceso o puerta de entrada / salida que permite el intercambio de datos, ya sea con un aparato anfitrión, ya sea, incluso, en red, por ejemplo. La noción de memoria no volátil y reprogramable cubre, por ejemplo, las memorias reprogramables eléctricamente, las memorias EEPROM, o las memoras de tipo *flash* o de acceso por impulsos.

El aparato electrónico anteriormente mencionado, cuando está en funcionamiento, lleva a cabo una fase de arranque, denotada como ATR (Respuesta al reajuste o “Answer To Reset”, en inglés), y, después, las sucesivas órdenes en curso, denotadas por COM.

Se comprende, en particular, que el dispositivo electrónico correspondiente puede, ventajosamente, estar constituido, por ejemplo, por cualquier tarjeta de microprocesador.

Haciendo referencia a la Figura 1a, el procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, objeto de la invención, comprende una etapa A consistente en cargar en la memoria viva del dispositivo electrónico, a partir de la memoria no volátil de este último, el valor denotado por FdV_E de la variable de fin de vida memorizada en la memoria no volátil.

La operación correspondiente a la etapa A se indica como:

$FdV_E \rightarrow FdV_R$.

En la realización precedente, FdV_R designa el valor de la variable de estado de fin de vida del dispositivo electrónico cargado en la memoria viva.

A continuación de la etapa A de la Figura 1a, y previamente a la ejecución de cualquier orden en curso COM por parte del microprocesador, el procedimiento objeto de la invención consiste, seguidamente, en una etapa B, de verificar si el valor de la variable de estado de fin de vida memorizada en la memoria viva se encuentra en el valor no verdadero. En la etapa B de la Figura 1a, la verificación se ha representado por una etapa de comprobación:

FdV_R = NOK ?

En esta relación, NOK representa el valor no verdadero de la variable de estado de fin de vida del dispositivo electrónico memorizado en la memoria viva.

Con la repuesta negativa a la comprobación de la etapa B, el procedimiento objeto de la invención consiste en llevar a cabo, C, las operaciones de paso a fin de vida del dispositivo electrónico.

Y al contrario, con la respuesta positiva a la comprobación realizada en la etapa B, de manera que la variable de estado de fin de vida memorizada en la memoria viva FdV_R se encuentra en el valor no verdadero NOK, el procedimiento objeto de la invención consiste en proseguir la inicialización o la ejecución de la orden en curso COM por parte del microprocesador del dispositivo electrónico. Se indica que la ejecución de la orden en curso corresponde a cualquier orden de una aplicación ejecutada por el dispositivo electrónico.

En el curso de esta ejecución, y al detectarse, en una etapa E, un ataque intrusivo, el procedimiento objeto de la invención consiste, en una etapa F, en instaurar, mediante escritura en la memoria viva única la variable de estado de fin de vida del dispositivo electrónico, la variable FdV_R en el valor verdadero, y en proseguir la inicialización y/o la ejecución de la orden en curso COM.

En la etapa F de la Figura 1a, la operación de instauración se indica por la relación:

FdV_R = OK.

En la relación anterior, se indica que el valor OK designa el valor verdadero de la variable de estado de fin de vida memorizada en la memoria viva.

Por último, la etapa de instauración F anteriormente mencionada es seguida por una etapa G consistente en diferir la escritura de la variable de estado de fin de vida FdV_E en el valor verdadero en la memoria no volátil, para efectuarla en lugar de la próxima operación de escritura en la memoria no volátil. Esto permite ocultar la inscripción de la variable de estado de fin de vida.

Se comprende, por supuesto, que la etapa G antes mencionada es seguida de un retorno a la ejecución de la siguiente orden en curso, con la intermediación de la etapa H. En la etapa antes mencionada, COM + 1 designa la orden siguiente.

Tal y como se ha representado en la Figura 1a, el retorno se efectúa en la Etapa B para la simple ejecución de la orden siguiente.

Sin embargo, según otra posibilidad de puesta en práctica del procedimiento objeto de la invención, el retorno puede ser efectuado, tal como se ha representado en línea discontinua en el dibujo de la Figura 1a, aguas arriba de la carga ejecutada en la etapa A, para la renovación del procedimiento de carga en memoria viva del valor de la variable de estado de fin de vida FdV_E, de manera sistemática. Semejante procedimiento no es, sin embargo, imprescindible, pero puede ser puesto en práctica como variante.

En la Figura 1b, se ha representado un diagrama cronológico o cronograma de las operaciones de ejecución de las etapas de la Figura 1a.

En particular, la etapa A puede ser ejecutada en el arranque ATR o previamente a la ejecución de cada orden COM, tal y como se ha mencionado anteriormente.

La comprobación de la etapa B se ejecuta previamente al arranque o a la ejecución de la orden en curso representada en sombreado a la izquierda de la Figura 1a. Se recuerda que la respuesta negativa a la comprobación de la etapa B lleva automáticamente al paso a fin de vida del dispositivo electrónico en la etapa C.

La prosecución del arranque o de la inicialización, o, incluso, de la ejecución de la orden en curso en la etapa D corresponde, de hecho, a la puesta en práctica de procedimientos algorítmicos de manejo de secretos para el dispositivo electrónico, cuando este último está constituido, por ejemplo, por una tarjeta de microprocesador.

La comprobación de la etapa E correspondiente a una comprobación de detección de ataque intrusivo, puede ponerse en práctica de un modo convencional, ya sea, por ejemplo, por la ejecución de mecanismos anti-DFA (Análisis de Fallo Diferencial, o “Differential Fault Analysis”, en inglés, procedimiento de ataque consistente en introducir un error en un tratamiento para deducir de ello informaciones sobre los datos tratados), ya sea por procedimientos de verificación de la integridad de los datos, por ejemplo.

La etapa de instauración de la variable de estado de fin de vida del dispositivo electrónico por escritura en la memoria viva única, etapa F, se lleva a cabo por el módulo de control del paso a fin de vida del dispositivo electrónico, y funciona por escritura de esta variable de estado con el valor verdadero, según la relación antes mencionada:

FdV_R = OK.

La etapa G, consistente en la puesta al día o actualización de la variable de estado de fin de vida FdV_E en la memoria no volátil, es decir, con la mayor frecuencia, en la memoria EEPROM, se lleva a cabo entonces de manera diferente, es decir, en lugar de la próxima escritura que se va a efectuar en la orden.

En la Figura 1b, esta operación se ha representado por un pico sombreado, a la derecha, que ilustra el aumento de la intensidad de corriente consumida por la memoria anteriormente citada, por causa de la operación de inscripción en la memoria antes mencionada.

La etapa E viene entonces seguida por una etapa de retorno, ya sea a la etapa B, ya sea a la etapa A, tal y como se ha descrito anteriormente en relación con la Figura 1a.

De una manera más específica, se indica que el valor no verdadero, denotado por NOK, de la variable de estado de fin de vida del dispositivo electrónico tiene un valor numérico arbitrario. El valor verdadero OK de la variable de estado de fin de vida es, por el contrario, todo valor numérico distinto del valor numérico arbitrario antes mencionado.

Tal y como se ha representado, además, en la Figura 1c, se considera todo conjunto de órdenes ejecutadas por el microprocesador del dispositivo electrónico, incluyendo órdenes (COM_W) que comprenden una inscripción sistemática en la memoria no volátil, y órdenes ($COM_{\overline{W}}$) que no comprenden inscripción en memoria no volátil. En esta hipótesis, el procedimiento objeto de la invención consiste, independientemente de la detección o de la no detección de un ataque intrusivo, en ejecutar la escritura D_2, en la memoria no volátil, de un octeto facticio, el cual se denota por OF. Esto permite ocultar cualquier escritura eventual de la variable de estado de fin de vida del dispositivo en la memoria no volátil.

De preferencia, la escritura del octeto facticio OF se lleva a cabo en la misma página de memoria que la de la variable de estado de fin de vida.

En la etapa D_2 representada en la Figura 1c, la operación de escritura en la misma página de memoria se ha representado por la relación:

WAP(OF) = WAP(FdVE).

En la relación anterior, WAP designa la dirección de la página de memoria de escritura.

La etapa D2 es seguida de la llamada a la etapa E de la Figura 1a.

Además, tal y como se ha representado en la misma Figura 1c, la operación de escritura en memoria no volátil del octeto facticio se lleva a cabo previamente a cualquier operación de transmisión de datos por la línea o conducción de la puerta de entrada / salida del dispositivo electrónico. En la Figura 1c, la operación correspondiente se ha representado de manera simbólica por la detección de cualquier operación de entrada / salida, por la relación:

COM = I/O?

La detección de semejante operación provoca entonces la escritura sistemática e inmediata del octeto facticio, tal y como se ha descrito previamente en la descripción.

Por último, como se ha representado en la Figura 1d, el procedimiento objeto de la invención incluye, de forma

ventajosa, consecutivamente a cualquier etapa de escritura en la memoria no volátil de la variable de estado de fin de vida tal y como se ha representado en la Figura G1, una etapa denotada por G2, consistente en verificar si se encuentra en el valor verdadero el valor de la variable de estado de fin de vida FdV_R, memorizado en la memoria viva. La operación correspondiente a la etapa antes citada se indica por la relación:

FdV_R = OK.

Con la verificación de que la variable de estado de fin de vida se encuentra en el valor verdadero, se lleva a cabo una etapa de realización de las operaciones de paso a fin de vida del dispositivo electrónico, mediante la apelación o llamada a la etapa C representada en la Figura 1a.

Y al contrario, en ausencia de verificación de que la variable de estado de fin de vida se encuentra en el valor verdadero, se efectúa un retorno a la etapa H.

Además, tal y como se ha representado igualmente en la Figura 1e, con la verificación, en la etapa D_{21}, de que el valor de la variable de estado de fin de vida FdV_R se encuentra en el valor verdadero, o sea, con una repuesta positiva a la comprobación D_{21} antes mencionada, la operación de escritura en la memoria no volátil del octeto facticio OF, representada en la etapa D_{22} de la Figura 1e, se sustituye por la escritura en la memoria EEPROM del valor de la variable de estado de fin de vida, mediante la llamada a la etapa G de la Figura 1a.

El procedimiento objeto de la invención permite, además, poner en práctica un contador de errores.

De una manera general, la actualización de un contador de errores se ve sometida a la misma restricción que la escritura de una variable de fin de vida.

Debido al hecho de que se trata de una escritura en memoria no volátil del tipo de EEPROM, dicha escritura es, normalmente, detectable como consecuencia de la intensidad excesiva, o sobreintensidad, consumida por esta última en el curso de la operación de escritura.

El procedimiento objeto de la invención puede, por tanto, permitir, de manera ventajosa, en el caso de la detección de errores que no justifiquen un paso directo a fin de vida, la implementación de un contador antes de efectuar la escritura normal. El valor de este contador es, seguidamente, verificado regularmente, y el sobrepaso de un valor de umbral permite desencadenar entonces un paso a fin de vida.

Semejante modo operativo se ha representado en la Figura 1f de la manera siguiente:

-- con la detección I_1 de un error de ejecución temporal de una instrucción distinto de un ataque intrusivo y que no justifica un paso a fin de vida del dispositivo electrónico, de manera que la detección del error temporal se designa por $\exists$ TE ?, donde TE designa el error de ejecución temporal antes citado, la respuesta positiva a la comprobación I_1 apela a una etapa I_2 de actualización por medio de la implementación de un contador de errores en la memoria viva. El valor actualizado en la etapa I_2, representado por la relación:

TE = TE + 1,

es entonces seguido por una etapa de comparación I_3 del valor de conteo de los valores actualizados con un valor de umbral, denotado por STE.

En la etapa de comprobación I_3, la operación de comparación se indica como:

TE > STE ?

Al sobrepasarse el valor de umbral por el valor de conteo de errores actualizado, es decir, con una respuesta positiva a la comprobación I_3, la escritura del valor de la variable de estado de fin de vida del dispositivo electrónico en el valor verdadero y el paso a fin de vida son efectuados por apelación a la etapa F y, seguidamente, a la G, tal y como se ha representado en la Figura 1f.

Un dispositivo electrónico que comprende un microprocesador denotado por 1_1, una memoria viva denotada como 1_2, una memoria no volátil del tipo de EEPROM, denotada por 1_3, y una memoria muerta denotada por 1_4, se describe, a continuación, con referencia a la Figura 2. Además, tal y como se ha representado en la mencionada Figura, el dispositivo comprende una puerta de entrada / salida denotada por I/O.

Tal como se ha representado en la Figura 2, el dispositivo electrónico en funcionamiento comprende una variable de estado de fin de vida de este dispositivo electrónico, denotada por FdV_E, gobernada por un módulo de control CM que puede, por ejemplo, ser un módulo de programación o software implantado en la memoria muerta 1_4.

El módulo de control CM incluye un módulo SCM de programas informáticos que permite, por supuesto, la ejecución de las etapas del procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, según se han descrito anteriormente en relación con las Figuras 1a a 1f.

Por supuesto, el módulo SCM de programa informático puede ser implantado en la memoria no volátil de tipo de EEPROM, la cual constituye un soporte de memorización. Este módulo de programa informático incluye una serie de instrucciones ejecutables por el microprocesador del dispositivo electrónico y, en el momento de la ejecución de las instrucciones precitadas, lleva a cabo las etapas de puesta en práctica del procedimiento, tal y como se ha descrito anteriormente en relación con las Figuras 1a a 1f.

El procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico, objeto de la invención, se ha puesto en práctica en tarjetas electrónicas. Ensayos muy exigentes llevados a cabo en tarjetas electrónicas por entidades de confianza independientes no han permitido impedir el paso a fin de vida de estas tarjetas electrónicas, contrariamente a las tarjetas electrónicas provistas de procedimientos de paso a fin de vida convencionales, para las cuales es posible repetir ataques intrusivos hasta que se pone en evidencia un fallo explotable. En consecuencia, parece que el procedimiento objeto de la invención no permite ya diferenciar a tiempo el caso en que se ha detectado un ataque y este va, por tanto, a conllevar un paso a fin de vida del dispositivo electrónico, del caso en que no se ha detectado el ataque o este no ha producido ningún efecto.

REIVINDICACIONES

1.- Procedimiento de ocultación de paso a fin de vida de un dispositivo electrónico que comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil y reprogramable que contiene una variable de estado de fin de vida del dispositivo electrónico, gobernada por un módulo de control, y un acceso o puerta de entrada / salida, caracterizado por que dicho procedimiento consiste, al menos, en el momento del arranque o puesta en marcha (ATR) del dispositivo electrónico, en:

- cargar (A) en la memoria viva, a partir de dicha memoria no volátil, el valor (FdV_E) de dicha variable de estado de fin de vida; y, previamente a la ejecución de toda orden en curso por parte de dicho microprocesador;

- verificar (B) si el valor de dicha variable de estado de fin de vida memorizada en la memoria viva, (FdV_R), se encuentra en el valor no verdadero; y, con la respuesta negativa a esta verificación;

- llevar a cabo (C) las operaciones de paso a fin de vida del dispositivo electrónico; si no, si dicha variable de estado de fin de vida memorizada en la memoria viva, (FdV_R), se encuentra en el valor no verdadero,

- proseguir (D) con la inicialización o la ejecución de la orden en curso (COM) por parte del microprocesador del dispositivo electrónico; y, al detectarse (E) un ataque intrusivo,

- instaurar (F) por escritura, en la única memoria viva, dicha variable de estado de fin de vida del dispositivo electrónico, (FdV_R), en el valor verdadero y proseguir con la inicialización y/o la ejecución de la orden en curso; y

- diferir (G) la escritura de la variable de estado de fin de vida (FdV_E) en el valor verdadero, en dicha memoria no volátil, a fin de efectuarla en lugar de la siguiente operación de escritura en memoria no volátil, contenida en la orden, lo que permite ocultar la inscripción de dicha variable de estado de fin de vida.

2.- Procedimiento de acuerdo con la reivindicación 1, caracterizado por que el valor no verdadero (FdV_R = NOK) de dicha variable de estado de fin de vida del dispositivo electrónico es un valor numérico arbitrario, y por que el valor verdadero (FdV_R = OK) de dicha variable de estado de fin de vida del dispositivo electrónico es todo valor numérico distinto de dicho valor numérico arbitrario.

3.- Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado por que, para un conjunto de órdenes ejecutadas por el microprocesador del dispositivo electrónico ($COM \in \{COM_W, COM_{\overline{W}}\}$), incluyendo órdenes ($COM_W$) que comprenden una inscripción sistemática en memoria no volátil, y órdenes ($COM_{\overline{W}}$) que no comprenden una inscripción en memoria no volátil, dicho procedimiento consiste, además, independientemente de la detección o la no detección de un ataque intrusivo, en llevar a cabo la escritura en la memoria no volátil de un octeto facticio, lo que permite ocultar toda escritura eventual de la variable de estado de fin de vida del dispositivo electrónico en la memoria no volátil.

4.- Procedimiento de acuerdo con la reivindicación 3, caracterizado por que este consiste en llevar a cabo la escritura de dicho octeto facticio en la misma página de memoria que la de dicha variable de estado de fin de vida.

5.- Procedimiento de acuerdo con una de las reivindicaciones 3 y 4, caracterizado por que dicha operación de escritura en la memoria no volátil de dicho octeto facticio se lleva a cabo previamente a cualquier ejecución de operación de trasmisión de datos por la línea o conducción de la puerta de entrada / salida del dispositivo electrónico de microprocesador.

6.- Procedimiento de acuerdo con la reivindicación 5, caracterizado por que, con la verificación de que el valor de dicha variable de estado de fin de vida (FdV_R) se encuentra en el valor verdadero, se sustituye, en lugar de dicha operación de escritura en la memoria no volátil de dicho octeto facticio, la operación de escritura en la memoria no volátil del valor de la variable de estado de fin de vida (FdV_E).

7.- Procedimiento de acuerdo con una de las reivindicaciones 3 a 6, caracterizado por que este incluye, además, consecutivamente a cualquier etapa de escritura en la memoria no volátil de la variable de estado de fin de vida (FdV_E), una etapa consistente en verificar si se encuentra en el valor verdadero el valor de dicha variable de estado de fin de vida, memorizado en la memoria viva (FdVr), y, al verificarse que se encuentra en el valor verdadero, una etapa de ejecución de las operaciones de paso a fin de vida del dispositivo electrónico.

8.- Procedimiento de acuerdo con una de las reivindicaciones precedentes, caracterizado por que, con la detección de un error de ejecución temporal de una instrucción distinto de un ataque intrusivo, que no justifica un paso a fin de vida del dispositivo electrónico, dicho procedimiento incluye, además,

- la puesta al día o actualización mediante el incremento de un contador de errores en la memoria viva;

- la comparación del valor de conteo de errores con un valor de umbral; y, al sobrepasarse dicho valor de umbral por dicho valor de conteo de errores,

- la escritura del valor de dicha variable de estado de fin de vida del dispositivo electrónico con el valor verdadero, y el paso a fin de vida del dispositivo electrónico.

9.- Dispositivo electrónico que comprende un microprocesador, una memoria viva, una memoria muerta, una memoria no volátil y reprogramable, que contiene una variable de estado de fin de vida del dispositivo electrónico (FdV_E), gobernada por un módulo de control, y un acceso o puerta de entrada / salida, caracterizado por que dicho módulo de control incluye un módulo de programa informático (SCM) de ejecución de etapas del procedimiento de acuerdo con una de las reivindicaciones 1 a 8.

10.- Un producto de programa informático, memorizado en un soporte de memorización y que incluye una serie de instrucciones ejecutables por una computadora o por el microprocesador de un dispositivo electrónico, caracterizado por que, en el momento de la ejecución de dichas operaciones, dicho programa lleva a cabo las etapas del procedimiento de acuerdo con una de las reivindicaciones 1 a 8.

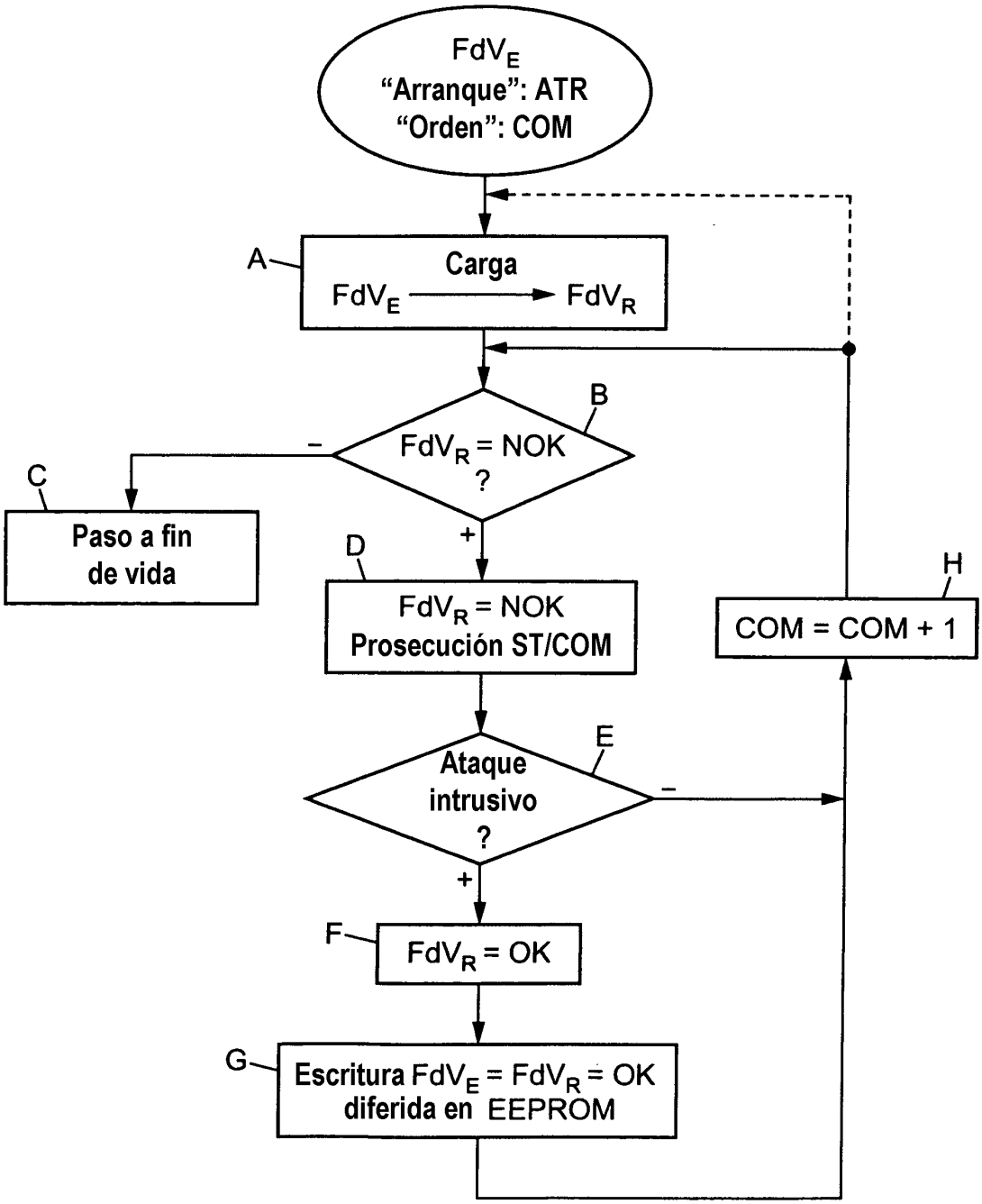
FdV_E
"Arranque": ATR
"Orden": COM
A
Carga
FdV_E → FdV_R
B
FdV_R = NOK
?
–
+
C
Paso a fin
de vida
D
FdV_R = NOK
Prosecución ST/COM
H
COM = COM + 1
E
Ataque
intrusivo
?
–
+
F
FdV_R = OK
G
Escritura FdV_E = FdV_R = OK
diferida en EEPROM

FIG. 1a

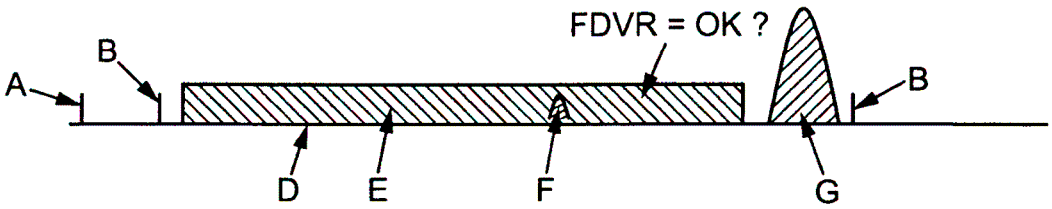
FDVR = OK ?
A
B
B
D
E
F
G

FIG. 1b

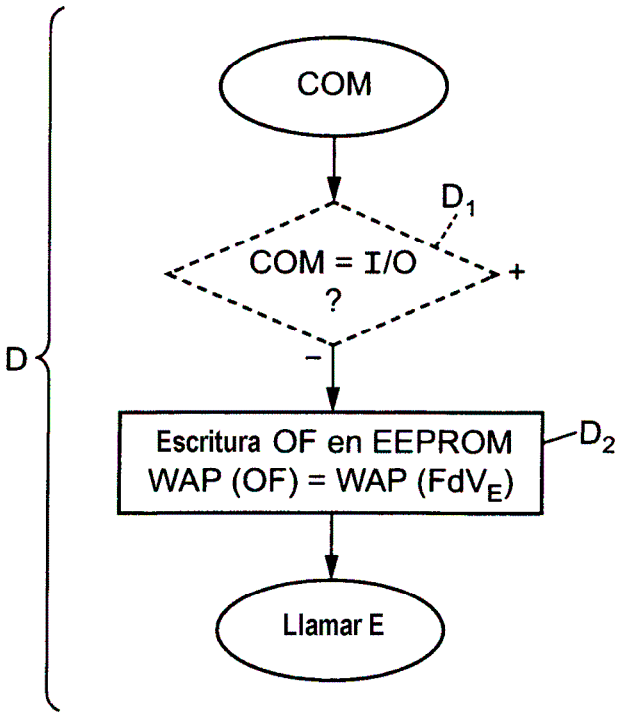
D
COM
D1
COM = I/O
?
+
–
Escritura OF en EEPROM
WAP (OF) = WAP (FdVE)
D2
Llamar E

FIG. 1c

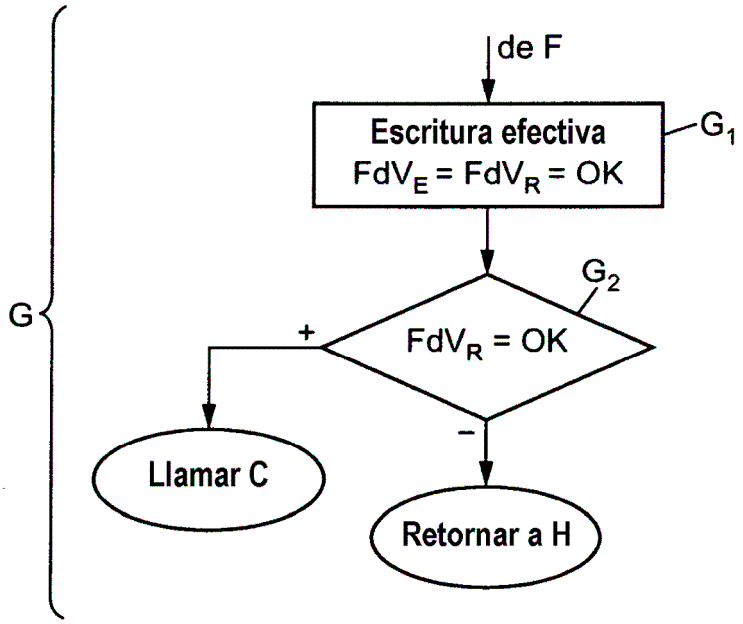
de F
Escritura efectiva
FdV$_E$ = FdV$_R$ = OK
G$_1$
G$_2$
FdV$_R$ = OK
+
–
Llamar C
Retornar a H
G

FIG. 1d

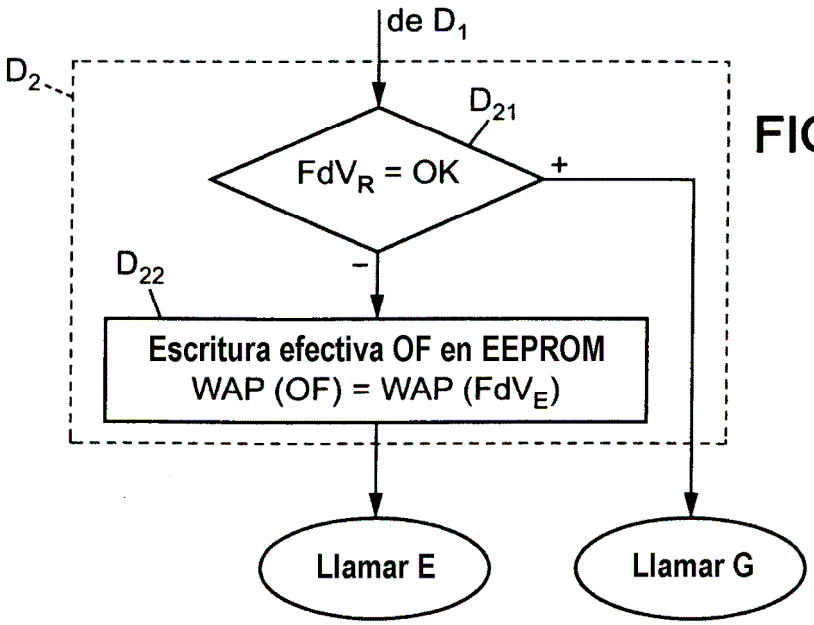
de D$_1$
D$_2$
D$_{21}$
FdV$_R$ = OK
+
–
D$_{22}$
Escritura efectiva OF en EEPROM
WAP (OF) = WAP (FdV$_E$)
Llamar E
Llamar G

FIG. 1e

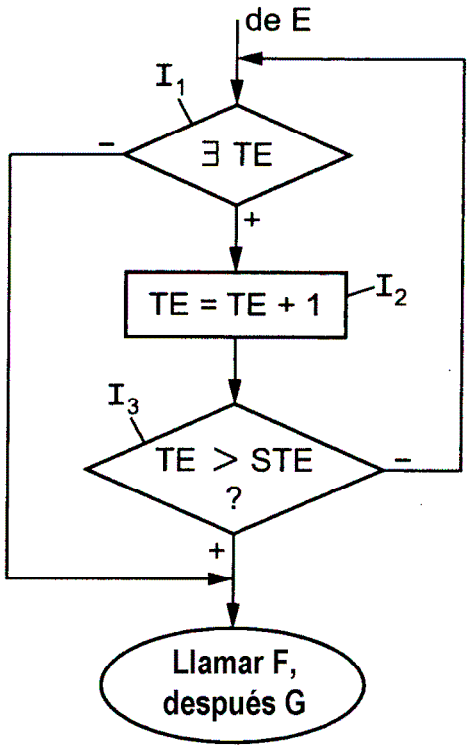
de E
I1
∃ TE
–
+
TE = TE + 1
I2
I3
TE > STE
?
–
+
Llamar F,
después G

FIG. 1f

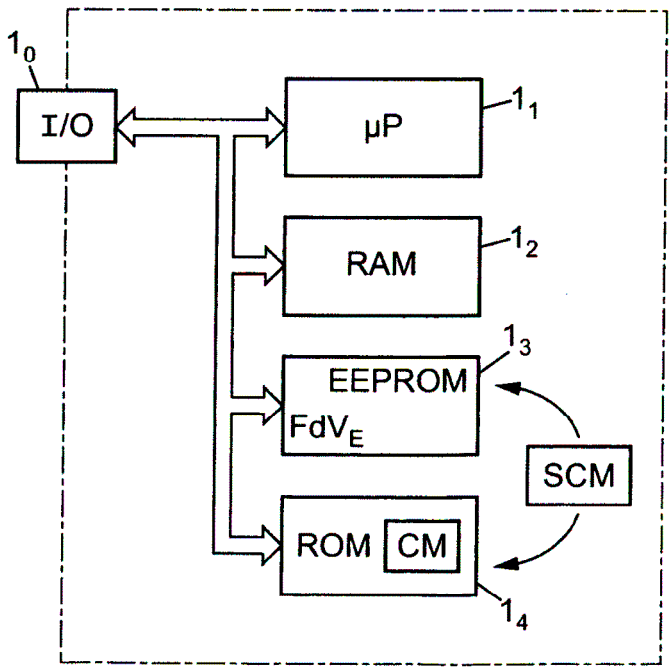
10
I/O
µP
11
RAM
12
EEPROM
FdVE
13
SCM
ROM
CM
14

FIG. 2