(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 429 766**

(51) Int. CI.:

G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.01.2009 E 09713901 (8)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2013 EP 2229648**

(54) Título: **Método de transferencia segura de datos**

(30) Prioridad:

11.01.2008 FR 0800156

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.11.2013

(73) Titular/es:

MORPHO (100.0%)
11 Boulevard Galliéni
92130 Issy Les Moulineaux, FR

(72) Inventor/es:

DECROIX, DAVID;
ROUDIERE, GUILLAUME y
PEPIN, CYRILLE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método de transferencia segura de datos

La invención concierne al aseguramiento de la transferencia de datos entre varios componentes de una tarjeta inteligente.

Antecedentes de la invención

El chip de una tarjeta inteligente contiene típicamente un procesador o microcontrolador así como una memoria volátil tal como una memoria RAM, y una memoria no volátil tal como una memoria Flash, EEPROM o también ROM.

La ejecución de una operación por un software de la tarjeta inteligente necesita numerosos intercambios de datos desde la memoria no volátil hacia la memoria volátil del chip. Así, cualquier explotación de datos registrados en la memoria no volátil requiere una transferencia hacia la memoria volátil.

Éste es el caso durante la lectura de un archivo que puede contener especialmente datos ligados a un código secreto a fin de compararle con un valor facilitado en entrada, y durante la lectura de una clave para efectuar un cálculo criptográfico.

Éste es igualmente el caso durante la lectura de una tabla estática de constantes registrada en una memoria ROM, que contenga por ejemplo datos representativos de los derechos de acceso a los archivos registrados en la tarjeta.

Esta fase de transferencia, que está asegurada por un bus de datos del chip, es sensible a perturbaciones de orden electromagnético. Existe así un procedimiento de fraude consistente en someter a la tarjeta a una fuente de radiación electromagnética durante la transferencia de datos, lo que permite al defraudador acceder a datos que normalmente le deben permanecer ocultos.

Estas perturbaciones provocan por ejemplo una modificación de los datos durante la transferencia, en cuyo caso, los datos cargados en la memoria volátil difieren de los datos fuente de la memoria no volátil.

Esta sensibilidad permite potencialmente recuperar fraudulentamente una clave o un código secreto de la tarjeta, eludir los derechos de acceso a los archivos contenidos en la tarjeta, y/o modificar parámetros de configuración de la tarjeta.

Esta es la razón por la cual están previstas medidas para detectar estas modificaciones a fin de impedir la ejecución de una operación cuando se haya detectado una modificación de este tipo.

Un método consiste en verificar después de la transferencia que los datos transferidos son idénticos a los datos fuente. Estos datos pueden ser una parte o la totalidad de un elemento, es decir una parte o la totalidad de los datos que constituyen uno o varios archivos.

Concretamente, después de la transferencia se verifica que cada octeto del elemento inscrito en la memoria volátil es idéntico a cada octeto del elemento fuente, lo que corresponde a una operación de tipo lectura y verificación.

Este método conocido sigue siendo a pesar de todo ineficaz frente a ciertos ataques. Si un atacante sabe perturbar la transferencia, para modificar los datos copiados en la memoria no volátil, y si sabe reproducir esta misma perturbación durante la operación de lectura y verificación, la modificación no puede ser detectada.

En efecto, en este caso, la operación de lectura y verificación no detecta anomalía puesto que ésta verifica únicamente que los datos perturbados durante la copia lo han sido igualmente durante la lectura que precede a la verificación.

El documento EP-1772811-A2 divulga la transferencia de datos entre un anfitrión y una memoria RAM de una tarjeta inteligente, siendo transferidos los datos a través de una memoria tampón de esta tarjeta inteligente. Un control de integridad de los datos transferidos es realizado por medio de un código de control de tipo CRC.

El documento FR-2888960 divulga un método de detección de una falta por perturbación larga durante la transmisión de datos desde o hacia una tarjeta inteligente por medio de una suma de control correspondiente a los datos transmitidos.

Objeto de la invención

El objetivo de la invención es proponer una solución para poner remedio a estos inconvenientes anteriores, proponiendo un método que ofrezca un mejor nivel de aseguramiento de la transferencia de datos entre los componentes del chip.

Resumen de la invención

A tal efecto, la invención tiene por objeto un método para comparar datos fuente registrados en una memoria fuente con datos transferidos copiados desde la memoria fuente en una memoria denominada de destino, en el cual se lee en la memoria fuente un valor de integridad asociado a un elemento fuente tal como un archivo que contenga los datos fuente, en el cual se calcula la integridad de un elemento reconstituido correspondiente al elemento fuente, siendo reconstituido este elemento a partir de los datos transferidos completados en su caso por los datos del elemento fuente distintos a los datos transferidos, y en el cual se decide que los datos transferidos son idénticos a los datos fuente cuando el cálculo de integridad dé un valor idéntico al valor de integridad del elemento fuente.

Durante la copia, los datos fuente son los que transitan por el bus de datos, pero durante la verificación, el valor de integridad es el que transita por el bus de datos. Así pues, los valores que transitan por el bus no son los mismos durante la copia y durante la verificación, de modo que un ataque consistente en aplicar la bus de datos las mismas perturbaciones durante la copia y durante la verificación es completamente ineficaz.

La invención concierne igualmente a un método tal como el definido anteriormente, en el cual el valor de integridad asociado al elemento que contiene los datos fuente y el valor de integridad calculado para el elemento reconstituido son valores de control cíclico de redundancia de los datos.

La invención concierne igualmente a un método tal como el definido anteriormente, en el cual se copia desde la memoria no volátil hacia la memoria volátil, un valor de referencia distinto a los datos que hay que transferir, estando este valor de referencia por una parte prerregistrado en la memoria no volátil y por otra prerregistrado en un software de lectura de la tarjeta inteligente, y en el cual se compara el valor transferido a la memoria volátil con el valor registrado en el software de lectura para determinar si los datos transferidos son idénticos a los datos fuente.

La invención concierne igualmente a un método tal como el definido anteriormente, en el cual la copia del valor predeterminado es efectuada durante la copia de los datos fuente.

Breve descripción de las figuras

- La figura 1 es una representación esquemática de un elemento fuente registrado en una memoria fuente no volátil;

- La figura 2 es una representación esquemática de la transferencia de una parte de los datos del elemento fuente de la figura 1 hacia una memoria volátil.

Descripción detallada de la invención

La idea de base de la invención es proceder después de la transferencia a un cálculo de integridad de los datos transferidos, de manera que se detecte si ha tenido lugar una modificación durante la transferencia cuando el valor dado por el cálculo de integridad basado en los datos transferidos no corresponde al valor de integridad asociado a los datos fuente.

El método se aplica al caso de la transferencia de una parte o de la totalidad de los datos de un elemento cuyo valor de integridad está registrado en la memoria fuente.

El valor de integridad es por ejemplo una suma de control de los datos del elemento considerado que generalmente es un archivo. Este valor de integridad puede ser una integridad del tipo LRC, es decir “Longitudinal Redundancy Check” que significa control de paridad cruzado, o bien una integridad de tipo hash.

Este valor de integridad es ventajosamente un valor de CRC, es decir de control cíclico de redundancia que es una prueba de integridad específicamente prevista para la detección de los errores de transmisión de datos. Podrá tratarse de un valor de CRC16 correspondiente a un control cíclico de redundancia sobre 16 indicadores binarios.

En el ejemplo que sigue, el método comprende tres etapas para transferir datos de un elemento fuente presente en la memoria no volátil, representado esquemáticamente en la figura 1, estando indicado en ésta por “ELEMENT_X_NV_MEM, y para verificar que los datos transferidos son idénticos a los datos fuente.

El valor de integridad PI_ELT_X de cualquier elemento ELEMENT_X_NV_MEM ha sido registrado previamente en la memoria no volátil, habiendo sido efectuado éste previamente por ejemplo cuando este elemento ha sido escrito en la memoria no volátil NV_MEM.

Como está representado esquemáticamente en la figura 2, una parte o la totalidad de los datos de este elemento fuente ELEMENT_X_NV_MEM son copiados en primer lugar desde la memoria no volátil NV_MEM hacia la memoria volátil V_MEM. Los datos inscritos en la memoria de destino, es decir la memoria volátil, son indicados por COPY_ELT_X_V_MEM.

Ventajosamente, se efectúa una verificación de la copia correcta de estos datos COPY_ELT_X_V_MEM, comparando cada octeto copiado con cada octeto correspondiente en el elemento fuente ELEMEMT_X_NV_MEM, lo que es una operación de lectura y de verificación.

Esta verificación puede ser efectuada cuando una parte de los datos han sido transferidos para detener la transferencia antes de que todos los datos hayan sido inscritos en la memoria volátil.

En un último tiempo, se verifica la integridad de los datos transferidos. Si la totalidad de los datos del elemento fuente ELEMENT_X_NV_MEM son los que han sido inscritos en la memoria volátil, esta verificación consiste en calcular la integridad de los datos inscritos en la memoria volátil, y en comparar el valor de integridad dado por este cálculo con el valor de integridad PI_ELT_X inscrito en la memoria no volátil NV_MEM.

Si los datos transferidos COPY_ELT_X_V_MEM corresponden solamente a una parte de los datos que constituyen el elemento ELEMENT_X_NV_MEM, entonces se calcula la integridad de un elemento reconstituido. Este elemento es reconstituido a partir de los datos transferidos COPY_ELT_X_V_MEM completados por los datos no transferidos del elemento COPY_ELT_X_V_MEM, es decir las partes rayadas en la figura 2.

Este elemento reconstituido corresponde al elemento fuente ELEMENT_X_NV_MEM del que comprende los datos transferidos COPY_ELT_X_V_MEM tales como quedan inscritos en la memoria volátil V_MEM, y los datos no transferidos tales como están inscritos en la memoria no volátil NV_MEM.

Cuando la transferencia de datos se ha realizado normalmente, los datos fuente inscritos en la memoria no volátil NV_MEM son idénticos a los datos transferidos que quedan inscritos en la memoria volátil V_MEM.

Por consiguiente, en el caso normal, es decir si los datos transferidos no han sido modificados, la integridad del elemento reconstituido es idéntica a la integridad PI_ELT_X del elemento fuente ELEMENT_X_NV_MEM inscrito en la memoria no volátil.

Por el contrario, cuando los datos han sido modificados durante la transferencia, es decir durante la copia, el cálculo de la integridad del elemento reconstituido da un valor que difiere de PI_ELT_X, lo que por tanto permite detectar esta anomalía o modificación.

Como se indicó anteriormente, la etapa de lectura y verificación es opcional en la medida en que ésta es ineficaz frente a una perturbación aplicada al bus de transferencia de manera idéntica durante la copia y durante la operación de lectura y verificación. Sin embargo, esta etapa permite detectar lo más pronto posible una perturbación puntual experimentada por el bus de datos, para detener el proceso lo más pronto posible en caso de anomalía.

El método de acuerdo con la invención permite así detectar una perturbación aplicada al bus de datos: como éste comprende una verificación por control de integridad, los datos transferidos para esta verificación, a saber el valor PI_ELT_X, no son los mismos que los datos transferidos para la copia. Un ataque consistente en aplicar al bus las mismas perturbaciones durante la copia y durante la verificación es por tanto completamente ineficaz.

Éste puede ser completado todavía por una operación denominada de falsa lectura efectuada durante la copia de los datos fuente de la memoria no volátil NV_MEM hacia la memoria volátil V_MEM. En este caso, se prevé un valor de referencia predeterminado, indicado por VR_NV_MEM que está prerregistrado en la memoria no volátil para toda la vida de la tarjeta, y que igualmente está integrado en el código del programa de lectura de la tarjeta. Este valor corresponde por ejemplo a un octeto de datos.

Antes de efectuar la copia, se determina aleatoriamente un rango, indicado por i, para la falsa lectura.

La copia es lanzada después, comenzando por los primeros octetos de los datos fuente ELEMENT_X_NV_MEM, que son transferidos uno tras otro hacia la memoria volátil.

Pero el octeto de orden i transferido es el octeto denominado de falsa lectura, es decir el octeto correspondiente al valor de referencia VR_NV_MEM. Una vez que este octeto ha sido transferido, la copia toma de nuevo su curso normal, transfiriendo sucesivamente el octeto de orden i de los datos fuente ELEMENT_X_NV_MEM, y después los octetos siguientes.

Una vez que el octeto de falsa lectura ha sido inscrito en la memoria volátil VR_V_MEM, éste puede ser comparado con el valor integrado en el programa de lectura de la tarjeta, siendo este último necesariamente idéntico a VR_NV_MEM. Esto permite determinar ciertas perturbaciones que intervengan durante la transferencia.

Este mecanismo adicional permite una detección lo más pronto posible de ciertas perturbaciones que de cualquier modo serían detectadas por el control de integridad. Pero gracias a este mecanismo, las perturbaciones pueden ser detectadas antes del final de la copia de los datos en la memoria volátil, lo que por consiguiente es más seguro puesto que la transferencia puede ser detenida entonces inmediatamente, es decir antes del final de la copia de los datos en la memoria volátil.

Hay que observar también que en el ejemplo descrito anteriormente, la etapa opcional de lectura y de comparación tiene lugar antes que la etapa de control de integridad de los datos transferidos. Pero esta etapa opcional puede ser puesta en práctica también después de la etapa de control de integridad, en la medida en que, en ciertos casos, ésta puede detectar errores no detectados por el control de integridad.

La invención aporta diferentes ventajas puesto que permite contrarrestar eficazmente un ataque por perturbación del bus de datos, y es poco onerosa en tiempo de ejecución. Finalmente, ésta no necesita prever datos suplementarios que haya que registrar en la o las memorias de la tarjeta inteligente.

REIVINDICACIONES

1. Método para comparar datos fuente registrados en una memoria fuente (NV_MEM) de una tarjeta inteligente con datos transferidos (COPY_ELT_X_V_MEM) copiados desde la memoria fuente (NV_MEM) en una memoria denominada de destino (V_MEM) de esta tarjeta inteligente, en el cual se lee en la memoria fuente (NV_MEM) un valor de integridad (PI_ELT_X) asociado a un elemento fuente (ELEMENT_X_NV_MEM) tal como un archivo que contiene los datos fuente,

caracterizado porque:

se calcula la integridad de un elemento reconstituido correspondiente al elemento fuente (ELEMENT_X_NV_MEM), siendo reconstituido este elemento a partir de los datos transferidos (COPY_ELT_X_V_MEM) completados en su caso por los datos del elemento fuente (ELEMENT_X_NV_MEM) distintos a los datos transferidos si los datos transferidos (COPY_ELT_X_V_MEM) corresponden solamente a una parte de los datos que constituyen el elemento fuente (ELEMENT_X_NV_MEM) y porque se decide que los datos transferidos (COPY_ELT_X_V_MEM) son idénticos a los datos fuente cuando el cálculo de integridad da un valor idéntico al valor de integridad del elemento fuente (PI_ELT_X).

2. Método de acuerdo con la reivindicación 1, en el cual el valor de integridad (PI_ELT_X) del elemento que contiene los datos fuente y el valor de integridad calculado para el elemento reconstituido son valores de control cíclico de redundancia de los datos.

3. Método de acuerdo con las reivindicaciones 1 o 2, en el cual se copia desde la memoria fuente (NV_MEM) hacia la memoria de destino (V_MEM), un valor de referencia (VR_NV_MEM) distinto a los datos que hay que transferir, estando este valor de referencia por una parte prerregistrado en la memoria fuente (NV_MEM) y por otra prerregistrado en un software de lectura de la tarjeta inteligente, y en el cual se compara el valor transferido (VR_V_MEM) en la memoria de destino (V_MEM) con el valor registrado en el software de lectura para determinar si los datos transferidos (COPY-ELT_X_V_MEM) son idénticos a los datos fuente.

4. Método de acuerdo con la reivindicación 3, en el cual la copia del valor predeterminado es efectuada durante la copia de los datos fuente.

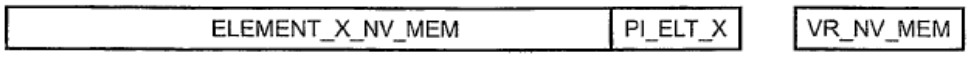
ELEMENT_X_NV_MEM
PI_ELT_X
VR_NV_MEM

FIG. 1

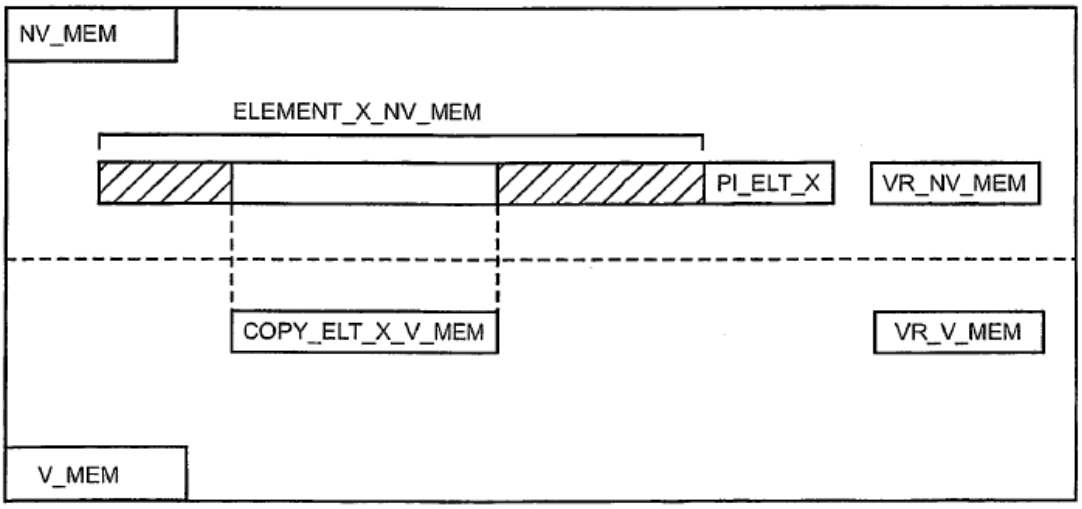
NV_MEM
ELEMENT_X_NV_MEM
PI_ELT_X
VR_NV_MEM
COPY_ELT_X_V_MEM
VR_V_MEM
V_MEM

FIG. 2