(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 328 017**

(51) Int. Cl.:
G06F 21/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02018607 .8**
(96) Fecha de presentación : **20.08.2002**
(97) Número de publicación de la solicitud: **1296214**
(97) Fecha de publicación de la solicitud: **26.03.2003**

(54) Título: **Procedimiento para la activación de una unidad de control dispuesta en un alojamiento, que está protegida frente a un acceso no autorizado a datos.**

(30) Prioridad: **30.08.2001 DE 101 42 537**

(45) Fecha de publicación de la mención BOPI:
06.11.2009

(45) Fecha de la publicación del folleto de la patente:
06.11.2009

(73) Titular/es: **adp Gauselmann GmbH**
Merkur-Allee 1-15
32339 Espelkamp, DE

(72) Inventor/es: **Gauselmann, Paul**

(74) Agente: **Lehmann Novo, María Isabel**

DESCRIPCIÓN

Procedimiento para la activación de una unidad de control dispuesta en un alojamiento, que está protegida frente a un acceso no autorizado a datos.

La invención se refiere a un procedimiento para la activación de una unidad de control dispuesta en un alojamiento, que está protegida frente a un acceso no autorizado a datos conforme al preámbulo de la reivindicación 1.

A partir de las instrucciones técnicas del aparato de juego "Triomint Top-Spiel" de la compañía NSM es conocida una unidad de control que dispone de un microprocesador con medio de almacenamiento asociado en la forma de EAROM (del inglés "Electrically Alterable Read Only Memory", memoria de sólo lectura alterable eléctricamente), EPROM (del inglés "Erasable Programmable Read-Only Memory", memoria de sólo lectura programable y borrable) y/o RAM (del inglés "Random Access Memory", memoria de acceso aleatorio). Los medios de almacenamiento se aseguran mediante una suma de comprobación. En caso de que este sistema de seguridad reaccione, todos los datos críticos en el medio de almacenamiento son borrados y los procesos de salida del ordenador son bloqueados. Además, la unidad de control comprende un autodiagnóstico, que es activado al ser encendido el aparato de juego. Durante la puesta en marcha, se comprueban entre otras cosas los puntos de entrada y de salida en serie y también se lleva a cabo una prueba de memoria. Si la comprobación da como resultado una desviación respecto a valores predeterminados, el aparato de juego no es puesto en marcha. Es desventajoso aquí sin embargo que el sistema de seguridad previamente citado es activado también cuando existe un defecto en el módulo de memoria. Por otro lado no se detecta el caso en que se desconectan programas auxiliares para la formación de la suma de comprobación, y tampoco cuando los datos son reorganizados y la suma de comprobación del programa modificado es idéntica con la suma de comprobación prefijada.

En el documento EP 1 085 396 A1 se muestra y describe un ordenador personal con un alojamiento, a cuyo ordenador pueden conectarse un teclado y un monitor de modo habitual. En el ordenador personal existe una denominada placa madre con un microprocesador, una memoria RAM así como un área de BIOS (del inglés "Basic Input-Output System", sistema básico de entrada-salida). Junto al microprocesador, en la placa madre hay otro componente con otro procesador y una memoria permanente y no permanente así como una memoria criptográfica. A través de ello es posible establecer áreas relevantes para la seguridad fuera de la estructura central del ordenador personal.

La invención tiene como base la tarea de conformar una unidad de control de tal modo que no sea posible un acceso no autorizado a o una modificación de datos o programas.

El procedimiento conforme a la invención tiene la ventaja de que para una disposición de un sistema de microordenador en un módulo protegido frente a ataques mecánicos y/o eléctricos, sólo pueden ser cargados en la memoria datos por parte de la persona autorizada. Para una persona ajena, debido a la secuencia conforme a la invención de pasos de trabajo consecutivos a llevar a cabo, no es posible cargar programas modificados o con otros valores en la memoria de trabajo protegida. El procedimiento no puede ser descubierto por personas ajenas, ya que al producirse una apertura violenta del módulo protegido los datos en los elementos de memoria de semiconductores preferentemente empleados son borrados.

Un ejemplo de realización conforme a la invención se representa en el dibujo. En un diagrama de bloques 1 se representan los elementos conforme a la invención de un módulo de seguridad 2. El módulo de seguridad 2, no representado en más detalle, consta de un alojamiento de dos partes cerrado por todos lados. En el alojamiento está dispuesta una placa de circuito impreso, en la que están dispuestos los componentes necesarios, por ejemplo un microcontrolador 3 con una memoria integrada, un microcontrolador 4 y al menos una memoria de semiconductores 5 así como sensores no representados para la detección de parámetros de entorno y un circuito de borrado. El circuito de borrado está unido a la memoria de semiconductores 5 conformada como componente de almacenamiento de datos. Con los sensores se detecta si tienen lugar ataques mecánicos, ópticos y/o químicos sobre el alojamiento y si se produce una manipulación de la tensión eléctrica de operación y/o de la temperatura ambiente. Para valores de salida, situados fuera del intervalo de operación prefijado, de los sensores, el circuito de borrado es activado por el sistema de sensores, cuyo circuito borra los datos que se encuentran en la memoria de semiconductores 5 conformada como componentes de almacenamiento de datos.

El módulo de seguridad 2 comprende el microcontrolador 3, por ejemplo un AT90S120, como procesador de inicio. El microcontrolador 3 comprende una memoria Flash 6 y una memoria EEPROM 7 (del inglés "Electrically Erasable Programmable Read-Only Memory", memoria de sólo lectura programable y borrable eléctricamente). Tras una programación exitosa de la memoria Flash 6 del microcontrolador 3 y la asignación de un bit de bloqueo no es ya posible una extracción posterior de los datos en la memoria integrada 6, 7 del microcontrolador 3. En la memora 6, 7 del microcontrolador 3 están integradas todas las rutinas para la inicialización y el inicio del procesador principal conformado como microcontrolador 4, así por ejemplo un programa de arranque y un código para un algoritmo de descifrado. El microcontrolador 3 comprende una batería de litio propia no representada, con la que se asegura también en caso de caída del suministro eléctrico que se conservan los contenidos de registro de las memorias 6, 7. El microcontrolador 3 está unido en serie al microcontrolador 4.

El microcontrolador 4, por ejemplo un Motorola MC68331, se emplea como procesador principal. Al microcontrolador 4 está conectada por un lado en paralelo la memoria de semiconductores 5 y por otro lado en serie una interfaz 8

de contacto con el exterior. A la interfaz 8 puede ser conectado un medio de almacenamiento externo. Desde el medio de almacenamiento externo se descargan un programa de carga y un programa de aplicación.

Si la tensión eléctrica externa de alimentación está aplicada al microcontrolador 3, se calcula por parte de éste una suma de comprobación a partir de un espacio de dirección prefijado de la memoria de semiconductores 5 conformada como memoria RAM, estática y protegida con batería. Si no se halla una suma de comprobación prefijada, se carga un programa de arranque, que se encuentra en la memoria Flash 6 del microcontrolador 3, a un área de dirección prefijada de la memoria de semiconductores 5 conformada como memoria RAM estática, con ayuda de la interfaz de depuración (BDM, del inglés "Background Debug Mode", modo de depuración en segundo plano) del microcontrolador 4. Una vez que se ha producido la transferencia del programa de arranque se comprueba si éste ha sido transferido sin errores al área de memoria prevista, conformada como memoria RAM, de la memoria de semiconductores 5. Si se ha producido una transferencia sin errores del programa de arranque a la memoria de semiconductores 5 conformada como memoria RAM, a continuación es iniciado el programa de arranque por el microcontrolador 3 y a continuación es cargado un programa de carga por el microcontrolador 4 a través de la interfaz en serie 8 desde un medio de almacenamiento externo. El programa de carga comprueba la memoria de semiconductores 5 y carga a continuación desde el medio de almacenamiento externo un programa de aplicación.

El programa de carga comprende también un software de descifrado. Durante la descarga del programa de aplicación cifrado desde el medio de almacenamiento se produce un descifrado del software de aplicación. Antes del comienzo de la descarga del software de aplicación, por parte de programa de carga es descargado desde el microcontrolador 3 un código, que es necesario para que el algoritmo de descifrado pueda descifrar el software de aplicación. Una vez realizada la descarga del software de aplicación, el programa de carga inicia el software de aplicación.

En caso de un fallo de tensión eléctrica de alimentación externa, el microcontrolador 3 es alimentado con energía eléctrica desde una batería de litio.

Si la tensión eléctrica de alimentación externa está aplicada, por parte del microcontrolador 3 se utiliza la interfaz de depuración del microcontrolador para la comprobación de la memoria de semiconductores 5. A partir de un espacio de dirección prefijado de la memoria de semiconductores 5 se calcula una suma de comprobación. Ésta es comparada con una suma de comprobación prefijada y en caso de coincidencia el microcontrolador 3 lleva a cabo una reinicialización de sistema, a través de la cual el microcontrolador 4 empieza con el programa de carga. El programa de carga lleva a cabo una comprobación de la memoria de semiconductores 5 e inicia a continuación el programa de aplicación.

REIVINDICACIONES

1. Procedimiento para la activación de una unidad de control, que está dispuesta en un alojamiento con protección frente a un acceso no autorizado a datos,

- en que la unidad de control dispuesta en el alojamiento comprende un primer microcontrolador (3) conformado como procesador de inicio, un segundo microcontrolador (4) conformado como procesador principal, al menos una memoria de semiconductores (5) conformada como medio de almacenamiento y una interfaz (8), a la que puede conectarse un medio de almacenamiento externo por fuera del alojamiento,

- en que el segundo microcontrolador (4) está unido a través de un sistema de bus con la memoria de semiconductores (5), así como con el primer microcontrolador (3) y la interfaz (8) respectivamente en serie, y el primer microcontrolador (3) tiene una memoria Flash (6) y una memoria EEPROM (7), en que

  a) el primer microcontrolador (3) calcula primeramente una suma de comprobación a partir de un espacio de dirección prefijado de la memoria de semiconductores (5) conformada como memoria RAM, estática y protegida con batería, y si no se halla la suma de comprobación prefijada, se carga un programa de arranque existente en la memoria Flash (6) del microcontrolador (3) a un área de dirección prefijada de la memoria de semiconductores (5) conformada como memoria RAM estática con ayuda de la interfaz de depuración del segundo microcontrolador (4),

  b) el primer microcontrolador (3) inicia el programa de arranque,

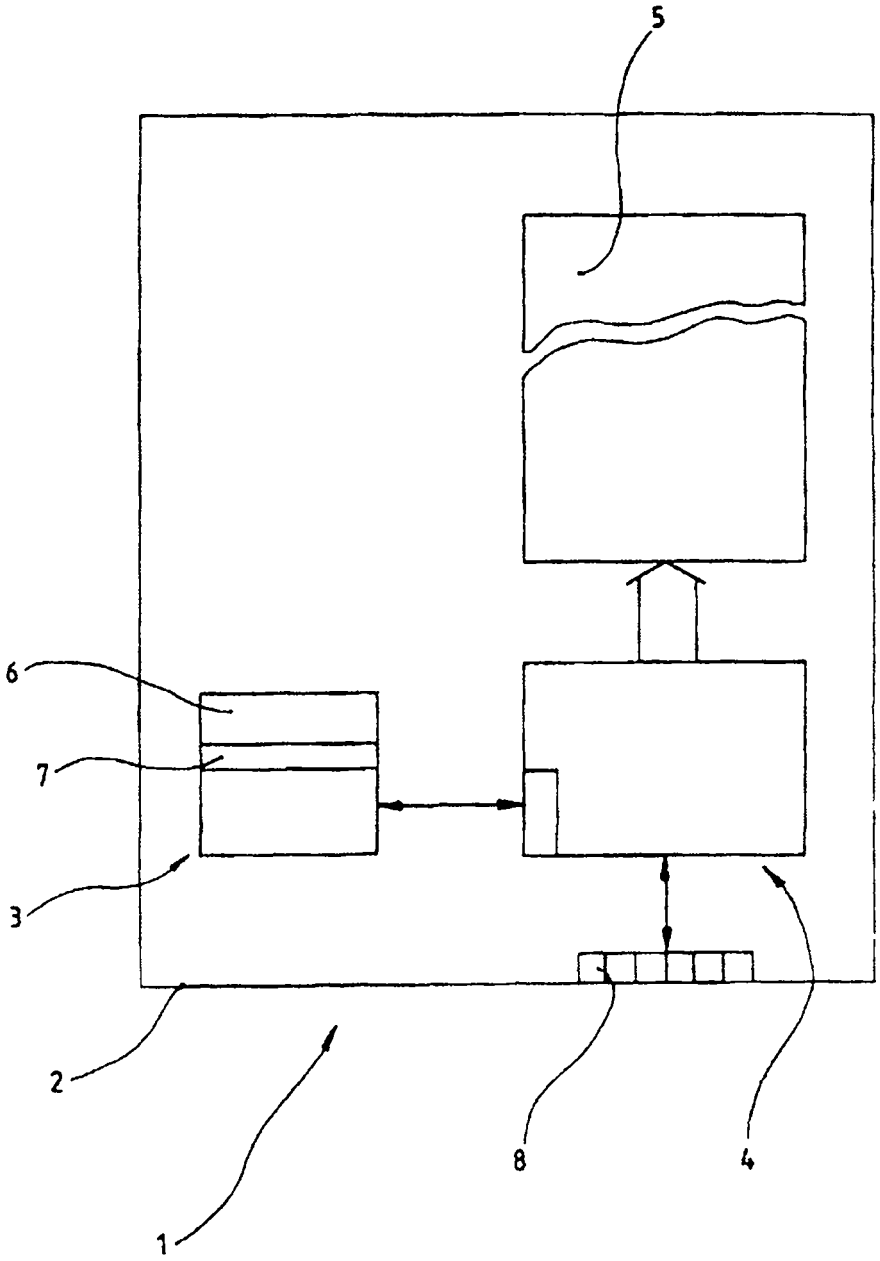
  c) el segundo microcontrolador (4) carga un programa de carga a través de la interfaz en serie (8) desde el medio de almacenamiento externo,

  d) el programa de carga comprueba la memoria de semiconductores (5) y a continuación el programa de carga carga un programa de aplicación desde el medio de almacenamiento externo,

  e) el primer microcontrolador (3) calcula una suma de comprobación a partir de un espacio de dirección prefijado de la memoria de semiconductores (5) con ayuda de la interfaz de depuración del segundo microcontrolador (4) y dicha suma es comparada con una suma de comprobación prefijada y en caso de coincidencia el primer microcontrolador (3) lleva a cabo una reinicialización de sistema, a través de la cual se inicia el segundo microcontrolador (4) con el programa de carga,

  f) el programa de carga lleva a cabo una comprobación de la memoria de semiconductores (5) e inicia el programa de aplicación.

2. Procedimiento según la reivindicación 1, **caracterizado** porque en una memoria Flash (6) del segundo microcontrolador (3) está depositado un código y porque el programa de carga descifra con ayuda del código programas de aplicación cifrados descargados desde el medio de almacenamiento externo y los deposita descifrados en la memoria de semiconductores (5).


5
6
7
3
2
1
8
4