(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 562 769**

(51) Int. CI.:

G06F 21/56 (2013.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.07.2005 E 05782466 (6)**

(97) Fecha y número de publicación de la concesión europea: **18.11.2015 EP 1714229**

(54) Título: **Módulo de seguridad y procedimiento para el control y supervisión de un tráfico de datos de un ordenador personal**

(30) Prioridad:

02.08.2004 DE 102004038040
30.03.2005 DE 102005014837

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2016

(73) Titular/es:

MAHLTIG MANAGEMENT- UND BETEILIGUNGS GMBH (100.0%)
Tollensestrasse 42F
14167 Berlin, DE

(72) Inventor/es:

MAHLTIG, HOLGER

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Módulo de seguridad y procedimiento para el control y supervisión de un tráfico de datos de un ordenador personal

La invención se refiere al campo de dispositivos y procedimientos para garantizar la seguridad de los datos de ordenadores personales.

Estado de la técnica

Los ordenadores personales modernos presentan una complejidad creciente tanto con respecto a su configuración de hardware como también en conexión con el software. No sólo comprenden una pluralidad de aparatos periféricos internos, es decir, dispuestos dentro de la carcasa, y externos, es decir, dispuestos fuera de la carcasa, y otros elementos, por ejemplo generadores de pulsos de reloj, con electrónica de control propia, respectivamente, sino que deben realizar también al mismo tiempo una pluralidad de ciclos. Además, actualmente los ordenadores personales están conectados en red de diferentes maneras con otros ordenadores personales y/u otros medios de procesamiento de datos, por ejemplo servidores, bases de datos, impresoras o similares, a través de redes de comunicación, por ejemplo Internet.

Además de la velocidad del procesamiento de datos y de la transmisión de datos, en este caso la seguridad de los datos tiene una gran importancia. Por una parte, la complejidad creciente tiene como consecuencia que no se pueden evitar modificaciones no deseadas de los datos, ya sea por deficiencias en el software o en virtud de errores de mando. Por otra parte, la conexión en red creciente conduce a que la prevención de accesos no autorizados a los datos, como tienen lugar, por ejemplo, por medio de virus de ordenador. Sea cada vez más difícil.

Los errores graves, los errores de mando y los virus de ordenador se consideran, en general, como diferentes fuentes de errores de datos, que pueden conducir incluso a la pérdida de datos, y los intentos para evitar estas fuentes se basan de manera correspondiente en principios muy diferentes. Por ejemplo, para la reducción de errores de mando se limita el acceso de usuarios a determinados datos, a los que solamente se puede acceder, por ejemplo, después de la entrada correcta de un código de autentificación. Además, un disco duro se puede dividir en segmentos, algunos de los cuales no son accesibles de forma discrecional. También cuando estas medidas de previsión pueden ser implementadas por medio de hardware, limitan el alcance de los datos solamente a los que se puede acceder por vía insegura. Pero estos datos se pueden dañar también todavía, por ejemplo, a través de errores de mando. La mayoría de las veces tales medidas de prevención de seguridad son implementadas, sin embargo, por medio de software, y de esta manera pueden ser eludidas por virus de ordenador, que han anidado en el software.

Los programas convencionales presente en el mercado contra virus de ordenador, los llamados programas de protección contra virus o programas antivirus, funcionan de tal manera que toda la memoria del ordenador personal es chequeada por el programa antivirus. Los datos que se encuentran en la memoria son comparados con códigos de programa de virus de ordenador conocidos, y en el caso de una coincidencia se emprenden medidas de protección, para eliminar estos datos nocivos. Sin embargo, a este respecto en el mejor de los casos, se puede conseguir una protección contra virus de ordenador ya conocidos. De esta manea, los programas antivirus en el caso de virus nuevos no conocidos hasta ahora son igualmente inefectivos que en el caso de errores de mano y errores de software. Además, el existe el peligro de que un programa antivirus, que solamente está depositado como software en la memoria del ordenador personal, se vuelve incluso objetivo de ataque de virus de ordenador.

Se conoce a partir del documento US 5.289.540 una tarjeta de enchufe que controla un flujo de datos entre unidades de disco y el hardware restante de un ordenador personal. La tarjeta de enchufe es instalada por el sistema operativo del ordenador personal durante la inicialización. El programa utilizado para el control de la tarjeta de enchufe está depositado en este caso en una memoria de trabajo del ordenador personal y verifica los derechos de acceso de un usuario a través de una autentificación por medio de la consulta de un nombre de usuario y de una palabra de paso. De manera similar como en el caso del programa antivirus, también aquí existe el peligro de que el programa utilizado para el control de la tarjeta de enchufe, que se encuentra en la memoria de trabajo del ordenador personal, se modifique en virtud de un error del software, de un error de mando y/o a través de un virus de ordenador. Además, después de una autentificación no se puede partir de que todos los accesos del usuario a los datos puestos a su disposición sean admisibles y sean interpretados sin errores por el software.

El documento US 6.564.326 publica un procedimiento, en el que un coprocesador es incorporado en un ordenador personal con un procesador. El coprocesador supervisa el ordenador personal hasta que se asegura que éste se encuentra en un estado libre de programas nocivos, por ejemplo virus de ordenador. A continuación, el coprocesador se desacopla del tráfico de datos del ordenador personal. El inconveniente en este procedimiento consiste en que no se detectan ni los daños de datos en virtud de errores de mando ni daños de datos en virtud de errores de software. Por otra parte, existe un problema similar que en los programas antivirus en el sentido de que, en efecto, debe conocerse ya qué programas son nocivos y cuáles no.

Se conoce a partir del documento WO 02/27445 A2 un módulo de seguridad para el bloqueo y control de un tráfico de datos de un ordenador personal con varios componentes funcionales, que están implementados, respectivamente, por medio de hardware y/o software. Los componentes funcionales comprenden un módulo lógico programable, una conexión de procesador conectada con el módulo lógico programable, para el intercambio de datos electrónicos con un procesador central del ordenador personal, una conexión de disco duro conectada con el módulo lógico programable, para el intercambio de datos electrónicos con un disco duro del ordenador personal, y n módulo de memoria conectado con el módulo lógico programable, que comprende datos de inicialización para el módulo lógico. El módulo lógico programable controla el tráfico de datos del ordenador personal, en el que por medio de una programación está implementada una instalación de procesamiento y de control para el procesamiento de datos electrónicos, que son intercambiados entre componentes del ordenador personal. El módulo lógico programable trabaja independientemente del ordenador personal y está realizado de manera que se instala automáticamente, de manera que puede intervenir también en el caso de un proceso de arranque del ordenador personal. El módulo lógico programable está configurado de tal manera que puede determinar un intercambio de datos erróneos y/o un intercambio no permitido de datos y, dado el caso, puede intervenir bloqueando.

La invención

El cometido de la invención es indicar un módulo de seguridad y un procedimiento para el control y supervisión de un tráfico de datos de un ordenador personal, que garantizan una seguridad elevada en el funcionamiento del ordenador personal.

Este cometido se soluciona de acuerdo con la invención por medio de un módulo de seguridad de acuerdo con la reivindicación independiente 1.

De acuerdo con la invención, está previsto un módulo de seguridad para el control y supervisión de un tráfico de datos de un ordenador personal con varios módulos funcionales, que están implementados, respectivamente, por medio de hardware y/o software, en el que la pluralidad de módulos funcionales comprende un módulo lógico programable, en el que está implementada por medio de programación una instalación de procesamiento y de control para el procesamiento de datos electrónicos, que son intercambiados entre varios módulos funcionales, una conexión de procesador conectada con el módulo lógico programable para el intercambio de datos electrónicos con un procesador central, una conexión de disco duro conectada con el módulo lógico programable para el intercambio de datos electrónicos con un disco duro del ordenador personal, conexiones de aparatos periféricos conectadas con el módulo lógico programable para el intercambio de datos electrónicos con aparatos periféricos acoplados en el ordenador personal para la entrada de daos y/o salida e datos y un módulo de memoria conectado con el módulo lógico programable, que comprende datos de inicialización para el módulo lógico y en el que el módulo lógico programable está realizado de manera que se inicializa por sí mismo, para hacer que la instalación de procesamiento y de control sea operativa de forma autónoma en el módulo lógico programable con la ayuda de datos de inicialización.

Además, está previsto que en el módulo lógico programable por medio de la programación esté implementada una instalación de comparación comprendida por la instalación de procesamiento y de control para la comparación de datos electrónicos, que son intercambiados entre la pluralidad de componentes funcionales, con los datos de control registrados predeterminados. Esto permite al módulo lógico programable, por ejemplo, determinar un intercambio de datos erróneos y/o un intercambio no permitido de datos y, dado el caso, intervenir para bloquearlos, por ejemplo impidiendo tal intercambio. Dado el caso, los datos de control registrados son adaptados en función de los datos electrónicos entrantes. Así, por ejemplo, se puede reconocer una pulsación determinada de la tecla o una secuencia de datos recibida a través de la conexión a la red por la instalación de comparación y ésta puede activar a continuación una función de control predefinida, cuyo resultado se manifiesta en una adaptación de los datos de control.

El módulo de seguridad tiene la ventaja frente al estado de la técnica de que un módulo lógico programable controla y supervisa el tráfico de datos del ordenador personal, que trabaja independientemente del ordenador personal. Esto significa que el procesador central del ordenador personal no puede controlar el módulo lógico programable. Por medio de la verificación de datos del ordenador personal, intercambiados durante el tráfico de datos entre componentes individuales por ejemplo entre el procesador central, el disco duro y los aparatos periféricos, el módulo lógico programable puede impedir cualquier acceso no deseado a los datos en virtud de errores de software, errores de mando y/o virus de ordenador. Puesto que el módulo lógico programable está realizado de manera que se inicializa por sí mismo, puede intervenir controlando y supervisando durante un proceso de arranque del ordenador personal.

En una forma de realización ventajosa de la invención, los módulos funcionales están realizados como un sistema encapsulado. Esto significa que los módulos funcionales están agrupados en un sistema operativo autónomo. De esta manera, se pueden hallar más fácilmente los defectos que aparecen en el módulo de seguridad, y el módulo de seguridad se puede sustituir en tal caso más fácilmente.

En un desarrollo de la invención fácil de usar, la pluralidad de módulos funcionales están implementados en una tarjeta de enchufe. Esto permite un equipamiento de un ordenador personal convencional con el módulo de seguridad, sin tener que modificar la arquitectura del ordenador personal.

En una forma de realización compacta de la invención, la pluralidad de componentes funcionales está implementada en una tarjeta madre del ordenador personal. Por una parte, de esta manera se acortan las vías de tráfico entre el procesador central del ordenador personal y el módulo de seguridad, lo que conduce a un incremento de la velocidad. Por otra parte, se liberan conexiones externas adicionales, por ejemplo conexiones de tarjetas de enchufe, hacia la tarjeta madre.

En un desarrollo preferido de la invención, la pluralidad de componentes funcionales está formada, al menos parcialmente, en un conjunto de chip de la tarjeta madre. De esta manera se reduce al mínimo la necesidad de espacio para el módulo de seguridad, lo que es considerablemente ventajoso, por ejemplo, para la aplicación en un ordenador personal móvil.

En un desarrollo ventajoso de la invención, la pluralidad de componentes funcionales está formada, al menos parcialmente, en un chip Northbridge de la tarjeta de chips de la tarjeta madre. Puesto que los chips Northbridge conectan el procesador central con el hardware restante del ordenador personal, con esta forma de realización se pueden ahorrar, al menos en parte, interfaces desde el módulo de seguridad hacia aparatos periféricos. Con este ahorro está implicada también una elevación de la seguridad, puesto que el módulo de seguridad se puede comunicar ahora directamente con el procesador central, en lugar de dar instrucciones para una comunicación a través de un sistema de bus.

En una configuración ventajosa de la invención, el módulo de memoria está formado en una memoria-RAM del ordenador personal. De esta manera se puede ahorrar total o parcialmente una memoria adicional para el módulo de seguridad, lo que conduce a un tipo de construcción más económica y más compacta.

En un ejemplo de la invención, el módulo lógico programable es un módulo-FPGA (FPGA – “Matriz de Puertas Programable en el Campo”). Esto tiene la ventaja de que para la fabricación del módulo de seguridad, tanto con respecto al módulo lógico programable propiamente dicho como también con respecto a los medios auxiliares de programación necesarios para su programación, se puede recurrir a la tecnología-FPGA conocida. De esta manera se pueden realizar también procesos intensivos de cálculo en lugar de secuencialmente en software paralelamente en hardware y, por lo tanto, economizando tiempo.

En un ejemplo, la invención prevé que la pluralidad de componentes funcionales para aparatos acoplados en la pluralidad de componentes funcionales durante el intercambio de datos estén realizados como componentes funcionales que operan de forma transparente. De esta manera se asegura que el software ejecutado en el ordenador personal no esté influenciado por la presencia del módulo de seguridad. El software para el control del ordenador personal no tiene que adaptarse, por lo tanto, para un uso con el módulo de seguridad. Como otra ventaja de esta forma de realización, un virus de ordenador anidado en el software del ordenador no podría determinar si está presente un módulo de seguridad, que debería ser eludido.

Descripción de ejemplos de realización preferidos

A continuación se explica en detalle la invención con la ayuda de ejemplos de realización con referencia a un dibujo. En este caso, la figura única muestra una representación esquemática de un módulo de seguridad con un módulo lógico programable.

De acuerdo con la figura, un módulo de seguridad 1 presenta varios módulos funcionales, que comprenden un módulo lógico programable 2, una conexión de procesador 3, una conexión de disco duro 4, conexiones de aparatos periféricos 5 y un módulo de memoria 6. El módulo de seguridad 1 está incorporado en un ordenador personal 10, que está equipado con un procesador central o bien un microprocesador 11, un disco duro 12, una memoria 14 y aparatos periféricos 13. En el ordenador personal 10 se puede tratar de cualquier tipo de sistemas de ordenador con un procesador central y un disco duro. Por ejemplo, el ordenador personal 10 puede comprender un ordenador móvil, por ejemplo un ordenador portátil o un PDA (PDA – “Asistente Digital Personal”).

El módulo lógico programable 2 puede estar formado por medio de un tipo discrecional de módulos lógicos programables (también llamados PLD – “Dispositivo Lógico Programable”), que pueden ser programados para procesar datos electrónicos, que son intercambiados entre varios componentes funcionales. En este caso se puede tratar tanto de un módulo lógico programable varias veces como también de un módulo lógico programable sólo una vez. En los módulos lógicos programables varias veces, la programación se realiza por medio de células de memoria comprendidas por el módulo lógico programable 2, por ejemplo células de memoria SRAM, EPROM, EEPROM y/o Flash. Con preferencia se utiliza para el módulo lógico programable 2 un módulo FPGA (FPGA = “Matriz de Puertas Programable en el Campo”. No obstante, como módulo lógico programable 2 se puede utilizar también un módulo CPLD (CPLD – “Dispositivo Lógico Programable Complejo”) o un módulo-ASIC (ASIC – “Circuito Integrado Específico de la Aplicación”).

La conexión de procesador 3 conectada con el módulo lógico programable 2 sirve para el intercambio de datos entre el módulo de seguridad 1 y el microprocesador 11 del ordenador personal 10. Cuando el ordenador personal 10 comprende varios microprocesadores, es decir, cuando se trata de un llamado ordenador multi-procesadores, la conexión del procesador 3 puede estar diseñada para poder conducir un intercambio de datos solamente con uno o con dos o más de los microprocesadores. La conexión del procesador 3 puede estar diseñada también para establecer una conexión indirecta entre el módulo lógico programable 2 y el microprocesador 11. Por ejemplo, esta conexión se puede realizar a través de un controlador, en particular un controlador de disco duro. De esta manera, se garantiza que el microprocesador intercambie sus informaciones como anteriormente a través del controlador con los aparatos periféricos. Esto es especialmente importante, por ejemplo, en formas de realización de la invención, en las que se realiza una consulta del microprocesador 11 en el disco duro 2, en efecto, a través del módulo de seguridad 10, pero el microprocesador 11 no se percata de la presencia del módulo de seguridad 10, cuando los componentes funcionales del módulo de seguridad 1 operan de forma transparente para el intercambio de datos entre el microprocesador 11 y el disco duro 12. A tal fin, el módulo de seguridad 10 debe simular funciones del disco duro 12 frente al microprocesador 11. Es decir, que el módulo de seguridad 10 debe emitir a través de la conexión del procesador 3 señales al microprocesador 11, que el microprocesador 11 interpreta que proceden del disco duro 12.

Con el módulo lógico programable 2 está conectada, además, la conexión de disco duro 4, a través de la cual se establece una conexión con uno o varios disco(s) duro(s) 12 del ordenador personal 10. En el disco duro 12 se puede tratar de un disco duro 12 se cualquier tecnología disponible, en particular de cualquier tamaño de construcción y/o capacidad de memoria, por ejemplo puede comprender también un llamado MicroDrive. La transmisión de datos desde y hacia el disco duro se puede realizar por medio de una norma de comunicación discrecional, de venta en el comercio, por ejemplo de una Norma IDE, EIDE o SATA (IDE “Electrónica de Controlador Integrado”, EIDE – IDE Mejorada”, SATA – “Accesorio Tecnológico Avanzado en Serie”).

Las conexiones de aparatos periféricos 5 pueden comprender conexiones de cualquier tipo de aparatos periféricos 13, que pueden ser activados por un ordenador personal 10. En particular, en este caso se trata de aparatos periféricos para la entrada de datos, por ejemplo un teclado, un ratón, un escáner o similar, y se trata de aparatos periféricos para la salida de datos, por ejemplo una tarjeta gráfica, una impresora, una tarjeta de sonido o similar. No obstante, también pueden estar presentes conexiones de aparatos periféricos 5 con aparatos periféricos, que sirven, además de para la entrada de datos, también para la salida de datos, por ejemplo hacia aparatos de memoria internos (es decir, que se encuentran dentro de una carcasa del ordenador personal 10) o hacia aparatos de memoria externos (es decir, que se encuentran fuera de una carcasa del ordenador personal 10) así como hacia tarjetas de la red, por ejemplo con funcionalidad de Modem, ISDN y/o LAN.

Especialmente las tarjetas de la red representan una fuente importante de datos nocivos, por que el ordenador personal 10 está conectado a través de ellas con redes de comunicación. Además, el ordenador personal 10 puede enviar por medio de una tarjeta de red de manera inadvertida, por ejemplo en virtud de errores de software o de virus de ordenador, mensajes a otros sistemas de ordenador conectados en la red de comunicaciones, por ejemplo por medio de Email. Por lo tanto, en una forma de realización de la invención, está previsto que todo el tráfico de datos entre el microprocesador 11 y el ordenador personal 10 y las tarjetas de la red se realice a través del módulo de seguridad 1 y se controle y/o supervise por el módulo lógico programable 2. En este caso, pueden estar presentes tarjetas de la red con normas o protocolos de comunicaciones discrecionales.

En particular, puede estar previsto que una o varias tarjetas de la red presenten dos o más llamadas direcciones-MC (MAC – “Control de Acceso de Medios”). La dirección MAC es una dirección, que se predetermina en cada tarjeta de la red durante su fabricación y con la que se activa la tarjeta de la red en un plano de transmisión de una red de comunicaciones, que está debajo del plano de transmisión, en el que se utilizan las llamadas direcciones-IP (IP – “Protocolo de Internet”). Para poder activar un ordenador personal opcionalmente en un plano de gestión del sistema o en un plano del sistema operativo, éstos deben poder activarse de una manera inequívoca a través de una dirección-MAC en función del plano de la tarjeta de la red o dirección-IP del ordenador. Para ahorrar una tarjeta de red adicional para la gestión del sistema y una conexión de cable adicional necesaria para ello y para no tener que modificar el direccionamiento-IP existente, es ventajosa la presencia de varias direcciones-MAC.

Las conexiones del módulo de seguridad 1, que comprenden la conexión del procesador 3, la conexión del disco duro 4 y las conexiones de los aparatos periféricos 5, pueden estar diseñadas como conexiones sencillas. No obstante, también comprenden circuitos, al menos en parte, complicados, que realizan, por ejemplo, una adaptación del protocolo y/o adaptación del nivel de señales a intercambiar. El módulo de seguridad 1 está equipado con medios de codificación y/o medios de descodificación para convertir señales entre diferentes normas de comunicaciones utilizadas en el ordenador personal 10. Los medios de codificación y/o descodificación pueden estar configurados como partes del módulo lógico 2 programable y/o de las conexiones.

Por último, el módulo de memoria 6 sirve para acondicionar datos de inicialización para el módulo lógico 2 programable. En este caso, al menos una parte del módulo de memoria 6 puede estar diseñado como módulo de memoria no volátil, para no perder un contenido de memoria después de la desconexión de la tensión de funcionamiento. Los datos de inicialización están disponibles en cualquier momento para el módulo lógico 2

programable, en particular inmediatamente después de la aplicación de la tensión de funcionamiento y sirven para que el módulo de seguridad 1 pueda actuar independientemente de componentes de memoria externos, por ejemplo la memoria-RAM del ordenador personal 10. En el módulo de memoria no volátil se puede tratar de cualquier tipo de módulos de memoria, que mantiene su contenido también después de la desconexión de la tensión de funcionamiento. Por ejemplo, el módulo de memoria 6 puede comprender una memoria Flash. Se puede tratar también de un módulo de memoria volátil en principio, que es alimentado por una fuente de energía propia, por ejemplo una batería. El módulo de memoria no volátil puede estar integrado también en el módulo lógico 2 programable.

Adicionalmente al módulo de memoria no volátil, el módulo de memoria 6 puede comprender también un módulo de memoria volátil propio, por ejemplo una memoria-RAM, en la que el módulo lógico 2 programable puede depositar datos durante el funcionamiento para la utilización posterior. No obstante, a tal fin se puede utilizar también una parte de la memoria 14 del ordenador personal 10, siendo reservada esta parte de la inicialización automática del módulo lógico 2 programable para el módulo de seguridad 1 y pudiendo disponer el microprocesador 11 libremente solamente de la parte restante de la memoria 14. De manera similar, también una parte de la capacidad de memoria del disco duro 12 puede ser reclamada por el módulo de seguridad 1.

Los aparatos periféricos 13, el disco duro 12 y/o el microprocesador 11 pueden ser activados a través de un sistema de bus del ordenador personal 10. En particular, en una forma de realización del módulo de seguridad 1 como tarjeta de enchufe-PCI, se pueden ahorrar de esta manera conexiones físicas separadas en el módulo de seguridad 1.
Para que el módulo de seguridad 1 realice lo más ampliamente posible su función de control y de supervisión, se conduce en una forma de realización todo el tráfico de datos entre el microprocesador 11, el disco duro 12 y los aparatos periféricos 13 a través del módulo de seguridad 1. Por razones de velocidad puede ser ventajoso que determinados datos sean intercambiados sin desvío sobre el módulo de seguridad 1. Por ejemplo, en presencia de varios discos duros, el disco duro puede estar conectado con datos menos importantes también por vía directa con el microprocesador 11.

Para que el módulo de seguridad 1 pueda controlar y supervisar el tráfico de datos del ordenador personal 10, deben desplazarse en primer lugar los módulos funcionales del módulo de seguridad 1 a un estado de partida definido. A tal fin, después de la aplicación de una tensión de funcionamiento se lleva a cabo una inicialización del módulo lógico 2 programable, en la que se prepara una instalación de procesamiento y de control en el módulo lógico 2 programable y se alimenta con datos de inicialización. La instalación de procesamiento y de control sirve para controlar todos los módulos funcionales del módulo de seguridad 1 independientemente del microprocesador 11.

El módulo lógico 2 programable está en condiciones después de la inicialización de recibir datos a través de las conexiones y se compararlos con datos depositados en el módulo de memoria 6, para realizar una gestión como reacción de ello, por ejemplo generar una instrucción de alarma, cuando deben borrarse datos importantes.

Un proceso importante es la inicialización del disco duro 12 por medio de rutinas de programas registrada en el BIOS, en un programa intermedio entre el software y el hardware de un ordenador personal. Durante un proceso de inicialización del ordenador personal 10 (llamado también proceso-Boot) se consultan a través de un controlador de dicho duro datos técnicos el disco duro 12, por ejemplo con respecto a la capacidad de memoria de disco duro. Esta consulta es recibida a través de la conexión del procesador 3 desde el módulo lógico 2 programable y es contestada con la ayuda de datos relacionados con el disco duro 12, depositados en el módulo de memoria 6. Cuando, por ejemplo, una zona del disco duro 12 está ocupada por el módulo de seguridad 1, se comunica al microprocesador 11 una capacidad de memoria de disco duro, que está reducida en la capacidad de memoria de la zona ocupada.

Un acceso del microprocesador 11 al disco duro 12 se realiza de acuerdo con ello de tal manera que las instrucciones del microprocesador 11 al disco duro 12 son recibidas en primer lugar por el módulo lógico programable 2 a través de la conexión el procesador 3. Estas instrucciones son verificadas entonces por medio de la instalación de procesamiento y de control y son comparadas con datos depositados en el módulo de memoria 6. Cuan do la instalación de procesamiento y de control establece que no es admisible una gestión correspondiente a la instrucción, es decir, cuando el microprocesador 11 trata de realizar una gestión no permitida, por ejemplo acceder a una zona del disco duro 12 no accesible para él, entonces no se transmite esta instrucción al disco duro 12. En su lugar, se transmite al microprocesador 11 a través de la conexión del procesador 3 un mensaje de error, que es idéntica con un mensaje de error del disco duro 12. De esta manera se simula al microprocesador que ha tenido lugar un intercambio directo de datos entre él y el disco duro 12. El mensaje de error puede ser, por ejemplo, un mensaje que informa de que la zona respectiva del disco duro 12 no está presente. Las instrucciones y los datos admisibles se transmiten inalterados a través de la conexión de disco duro 4 al disco duro 12. Esto significa que el módulo lógico 2 programable, la conexión de procesador 3 y la conexión del disco duro 4 operan de forma transparente.

De manera similar se procede con un intercambio de datos con los aparatos periféricos 13 para la entrada de datos y/o la salida de datos. Se puede realizar una entrada de datos, por ejemplo, por medio de un teclado. En este caso, cuando se pulsa una tecla o una combinación de teclas se emite en primer lugar una señal a este respecto a una conexión de aparatos periféricos 5 del módulo de seguridad 1. La señal es descodificada allí o es transmitida

directamente al módulo lógico 2 programable. Si la instalación de procesamiento y de control del módulo lógico 2 programable establece en virtud de los datos registrados en el módulo de memoria 6 que la ejecución de una instrucción asociada con la combinación de teclas conduce a una gestión no permitida, entonces o bien se ignora totalmente la señal y/o se representa una instrucción de aviso correspondiente sobre otro aparato periférico, por ejemplo a través de un monitor. Pero de esta manera se puede emitir también una instrucción a la instalación de procesamiento y de control propiamente dicha, siendo utilizada ésta exclusivamente dentro de la instalación de procesamiento y de control para el arranque de una rutina de software, pero la pulsación de la tecla no se transmite al microprocesador 11. De esta manera se impide también que un software nocivo ejecutado en el microprocesador 11 supervise el manejo de la instalación de procesamiento y de control.

Las características publicadas en la descripción anterior, en las reivindicaciones y en el dibujo pueden ser importantes tanto individualmente como también en combinación discrecional para la realización de la invención en sus diferentes formas de realización.

REIVINDICACIONES

1.- Módulo de seguridad (1) para el control y supervisión de un tráfico de datos de un ordenador personal (10) con varios módulos funcionales, que están implementados, respectivamente, por medio de hardware y/o software, que comprenden:

- un módulo lógico programable (2), en el que está implementada por medio de programación una instalación de procesamiento y de control para el procesamiento de datos electrónicos, que son intercambiados entre componentes del modelador personal,
- una conexión de procesador (3) conectada con el módulo lógico programable (2) para el intercambio de datos electrónicos con al menos un procesador central (11) del ordenador personal (10);
- una conexión de disco duro (4) conectada con el módulo lógico programable (2) para el intercambio de datos electrónicos con un disco duro (14) del ordenador personal (10);
- conexiones de aparatos periféricos (5) conectadas con el módulo lógico programable (2) para el intercambio de datos electrónicos con aparatos periféricos (13) acoplados en el ordenador personal (10) para la entrada de daos y/o salida de datos; y
- un módulo de memoria (6) conectado con el módulo lógico programable (2), que comprende datos de inicialización para el módulo lógico (2)

en el que el módulo lógico programable (2) está realizado de manera que se inicializa por sí mismo, y también durante un proceso de arranque del ordenador personal puede intervenir controlando y supervisando;
en el que el módulo lógico (2) controla y supervisa el tráfico de datos del ordenador personal (10),
en el que el módulo lógico programable (2) está configurado de tal forma que puede determinar un intercambio no permitido de los datos y, dado el caso, puede intervenir para corregirlos;
en el que en el módulo lógico programable (2) por medio de la programación está implementada una instalación de comparación comprendida por la instalación de procesamiento y de control, para la comparación de datos electrónicos, que son intercambiados entre componente del ordenador personal, con datos de control registrados predeterminados; y
en el que los datos de control registrados pueden ser adaptados en función de los datos electrónicos introducidos, siendo reconocida una secuencia de datos recibida por el dispositivo de comparación y activando éste a continuación una función de control predefinida, cuyo resultado se manifiesta en una adaptación de los datos de control, siendo recibida la secuencia de datos desde el teclado o desde la tarjeta de la red del ordenador personal.

2.- Módulo de seguridad (1) de acuerdo con la reivindicación 1, caracterizado por que la pluralidad de módulos funcionales están realizados como un sistema encapsulado, de manera que los módulos funcionales están agrupados en un sistema que opera de forma autónoma.

3.- Módulo de seguridad (1) de acuerdo con la reivindicación 1 ó 2, caracterizado por que la pluralidad de módulos funcionales está implementada en una tarjeta madre del ordenador personal (10).

4.- Módulo de seguridad (1) de acuerdo con la reivindicación 3, caracterizado por que la pluralidad de módulos funcionales está implementada, al menos parcialmente, en un conjunto de chips de la tarjeta madre.

5.- Módulo de seguridad (1) de acuerdo con la reivindicación 4, caracterizado por que la pluralidad de módulos funcionales está implementada, al menos parcialmente, en un chip Northbridge del conjunto de chips de la tarjeta madre.

6.- Módulo de seguridad (1) de acuerdo con una de las reivindicaciones anteriores, caracterizado por que el módulo de memoria (6) está formado en una memoria-RAM del ordenador personal (10).

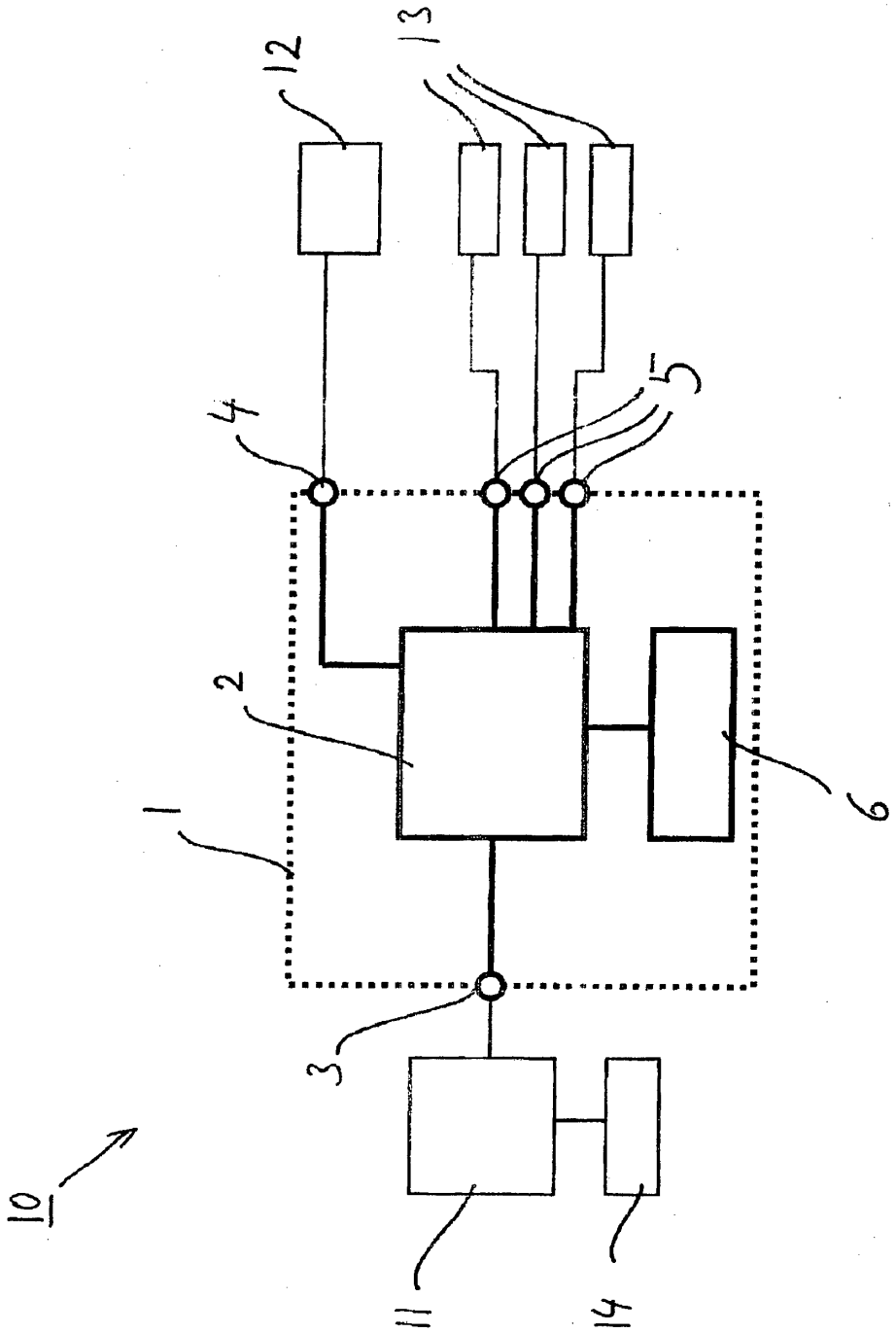

Fig.