(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 665 946**

(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 15187499 (7)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2018 EP 2996062**

(54) Título: **Módulo de seguridad y procedimiento para dirigir y controlar el 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:
30.04.2018

(73) Titular/es:

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

(72) Inventor/es:

MAHLTIG, HOLGER

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Módulo de seguridad y procedimiento para dirigir y controlar el tráfico de datos de un ordenador personal

La invención se basa en el campo de dispositivos y procedimientos para garantizar la seguridad de los datos de los ordenadores personales.

Estado de la técnica

Los ordenadores personales modernos presentan una creciente complejidad tanto en cuanto a su configuración de hardware como en relación con el software. Estos no solo comprenden una pluralidad de periféricos internos, es decir, dispuestos dentro de la carcasa, y externos, es decir, dispuestos fuera de la carcasa, y otros elementos, por ejemplo secuenciadores, con en cada caso una electrónica de control propia, sino que también deben ejecutar al mismo una pluralidad de procesos. Además, los ordenadores personales actuales, están interconectados por las más diversas vías con otros ordenadores personales y/u otros medios de procesamiento de datos, por ejemplo servidores, bancos de datos, impresoras o similares, a través de redes de comunicación, por ejemplo Internet.

Junto a la velocidad del procesamiento de datos y la transmisión de datos es en este sentido de gran importancia la seguridad de datos. Por un lado, la creciente complejidad tiene como consecuencia que no pueden evitarse cambios indeseados de los datos, ya sea por deficiencias en el software o debido a errores operativos. Por otro lado, la creciente interconexión lleva a que cada vez sea más difícil impedir accesos no permitidos a los datos, tal como tienen lugar, por ejemplo, por medio de virus informáticos.

Los errores de software, errores operativos y virus informáticos se consideran en general fuentes diferentes de errores de datos, que incluso pueden llevar a la pérdida de datos, y los intentos de evitar estas fuentes, se basan por consiguiente en planteamientos muy diferentes. Por ejemplo, para reducir los errores operativos, se limita el acceso de los usuarios a determinados datos, a los que puede accederse libremente por ejemplo solo tras la correcta introducción de un código de autentificación. Un disco duro puede también dividirse en segmentos, de los que algunos no son accesibles a voluntad para el usuario. Incluso cuando estas medidas preventivas pueden implementarse por medio de hardware, limitan únicamente la extensión de los datos a los que puede accederse de manera insegura. En cambio, estos datos pueden aún dañarse, por ejemplo, por errores operativos. En la mayoría de los casos, las medidas de seguridad de este tipo se implementan sin embargo por medio de software, y pueden eludirse por lo tanto por virus informáticos que se han implantado en el software.

Los programas convencionales, existentes en el mercado contra virus informáticos, los denominados programas de protección contra virus o antivirus, funcionan de manera que el programa antivirus explora toda la memoria del ordenador personal. Los datos que se encuentran en la memoria se comparan con códigos de programa de virus informáticos conocidos, y en caso de coincidencia, se efectúan medidas de protección para eliminar estos datos dañinos. En este sentido, sin embargo, en el mejor de los casos puede conseguirse una protección frente a virus informáticos ya conocidos. Por lo tanto, los programas antivirus, en el caso de nuevos virus informáticos, desconocidos hasta el momento, son tan inefectivos como en el caso de errores operativos y de software. Además existe el riesgo de que un programa antivirus, que está implantado únicamente como software en la memoria del ordenador personal, sea en sí el objetivo de un ataque por virus informáticos.

Por el documento US 5.289.540 se conoce una tarjeta insertable que controla un flujo de datos entre unidades de disco y el resto del hardware de un ordenador personal. La tarjeta insertable se abre por el sistema de sistema operativo del ordenador personal durante la inicialización. El programa usado para dirigir la tarjeta insertable está implantado en este caso en una memoria de trabajo del ordenador personal, y comprueba los derechos de acceso de un usuario mediante una autentificación por medio de petición de un nombre de usuario y una clave. Al igual que en el caso del programa antivirus, en este caso existe también el riesgo de que el programa usado para dirigir la tarjeta insertable, que se encuentra en la memoria de trabajo del ordenador personal, se modifique debido a un error de software, un error operativo y/o por un virus informático. Además, después de una autentificación no puede suponerse que todos los accesos del usuario a los datos disponibles para el mismo se interpreten por el software como permitidos y libres de errores.
El documento US 6.564.326 divulga un procedimiento en el que está instalado un coprocesador en un ordenador personal con un procesador. El coprocesador supervisa el ordenador personal hasta que está garantizado que este se encuentra en un estado libre de programas dañinos, por ejemplo virus informáticos. A continuación, el coprocesador se desacopla del tráfico de datos del ordenador personal. La desventaja de este procedimiento consiste en que no se detectan ni daños en los datos debido a errores operativos ni aquellos debido a errores de software. Por otro lado, un problema similar al de los programas antivirus consiste en que debe ya conocerse en concreto qué programas son dañinos y qué programas no lo son.

Por el documento WO 02/27445 A2 es conocido un módulo de seguridad para bloquear y controlar el tráfico de datos de un ordenador personal con varios componentes funcionales, que están implementados en cada caso 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 intercambiar datos electrónicos con un procesador central del ordenador personal, una conexión de disco duro conectada con el módulo lógico

programable, para intercambiar datos electrónicos con un disco duro del ordenador personal, y un 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 programación, está implementado un dispositivo de procesamiento y control para procesar datos electrónicos, que se intercambian entre componentes del ordenador personal. El módulo lógico programable trabaja independientemente del ordenador personal y está realizado de manera que puede autoiniciarse, de modo que también puede intervenir en un proceso de arranque del ordenador personal. El módulo lógico programable está configurado de modo que puede establecer un intercambio de datos erróneos y/o un intercambio no permitido de datos y, dado el caso, puede intervenir de modo que bloquee.

La invención

Es objetivo de la invención proporcionar un módulo de seguridad y un procedimiento para dirigir y controlar el tráfico de datos de un ordenador personal, que garanticen una seguridad elevada durante la operación del ordenador personal. Este objetivo se consigue de acuerdo con la invención mediante un módulo de seguridad según la reivindicación independiente 1.

De acuerdo con la invención, un módulo de seguridad para dirigir y controlar el tráfico de datos de un ordenador personal está dotado de varios componentes funcionales, que están implementados en cada caso por medio de hardware y/o software, en el que los varios componentes funcionales comprenden un módulo lógico programable, en el que, por medio de programación, está implementado un dispositivo de procesamiento y control para procesar datos electrónicos, que se intercambian entre los varios componentes funcionales, una conexión de procesador conectada con el módulo lógico programable para intercambiar datos electrónicos con un procesador central del ordenador personal, una conexión de disco duro conectada con el módulo lógico programable para intercambiar datos electrónicos con un disco duro del ordenador personal, conexiones de periféricos conectadas con el módulo lógico programable para intercambiar datos electrónicos con periféricos acoplados al ordenador personal para la entrada de datos y/o salida de 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 para autoinicializarse para hacer independientemente funcional el dispositivo de procesamiento y control en el módulo lógico programable con ayuda de los datos de inicialización.

El módulo de seguridad tiene, con respecto al estado de la técnica, la ventaja de que un módulo lógico programable dirige y controla el tráfico de datos del ordenador personal, que trabaja de forma independiente del ordenador personal. Esto significa que el procesador central del ordenador personal no puede controlar el módulo lógico programable. Por medio de la comprobación de datos del ordenador personal intercambiados durante el tráfico de datos entre los componentes individuales, por ejemplo entre el procesador central, el disco duro y los periféricos, el módulo lógico programable puede prevenir por lo tanto cualquier acceso indeseado a los datos debido a errores de software, errores operativos y/o virus informáticos. Dado que el módulo lógico programable está realizado para autoinicializarse, este puede intervenir dirigiendo y controlando también en un proceso de arranque del ordenador personal.

En una forma de realización ventajosa de la invención, los componentes funcionales están realizados como un sistema encapsulado. Esto significa que los componentes funcionales están reunidos formando un sistema que opera de manera independiente. De este modo, pueden encontrarse más fácilmente los defectos que aparecen en el módulo de seguridad, y el módulo de seguridad puede cambiarse de forma sencilla en tal caso.

En un perfeccionamiento de más fácil manejo para el usuario de la invención, los varios componentes funcionales están implementados en una tarjeta insertable. Esto permite dotar a un ordenador personal convencional de un módulo de seguridad, sin tener que modificar la arquitectura del ordenador personal.

En una forma de realización compacta de la invención, los varios componentes funcionales están implementados en una placa madre del ordenador personal. Por un lado se acorta con ello el recorrido de tráfico de datos entre el procesador central del ordenador personal y el módulo de seguridad, lo que lleva a un aumento de la velocidad. Por otro lado, se dejan libres conexiones externas adicionales, por ejemplo conexiones de tarjeta insertable, a la placa madre.

En un perfeccionamiento preferido de la invención, los varios componentes funcionales están conformados al menos en parte en un conjunto de chips de la placa madre. Con ello se minimiza el espacio necesario para el módulo de seguridad, lo que es una ventaja considerable por ejemplo para la aplicación en un ordenador personal móvil.

En un perfeccionamiento conveniente de la invención, los varios componentes funcionales están conformados al menos en parte en un chip de puente norte del conjunto de chips de la placa madre. Dado que los chips de puente norte conectan el procesador central con el resto del hardware del ordenador personal, con esta forma de realización pueden ahorrarse al menos en parte interfaces del módulo de seguridad con los periféricos. Este ahorro va acompañado también de un aumento de velocidad, dado que el módulo de seguridad puede comunicar ahora directamente con el procesador central, en lugar de depender de una comunicación a través de un sistema de bus.

En una configuración ventajosa de la invención, el módulo de memoria está conformado en la memoria RAM del

ordenador personal. Con ello puede ahorrarse en parte o por completo una memoria adicional para el módulo de seguridad, lo que lleva a un modo de construcción más económico y más compacto.

En una forma de realización preferida de la invención, el módulo lógico programable es un módulo FPGA (FPGA - “Field Programmahle Gate Array”). Esto tiene la ventaja de que para la producción del módulo de seguridad, tanto en cuanto al módulo lógico programable en sí como a los medios auxiliares de programación necesarios para su programación, puede recurrirse a la tecnología de FPGA conocida. Con ello pueden ejecutarse también procesos de cálculo intensivo en lugar de secuencialmente en el software, en paralelo en el hardware, y por lo tanto ahorrando tiempo.

Un perfeccionamiento ventajoso de la invención prevé que en el módulo lógico programable, por medio de la programación, está implementado un dispositivo de comparación comprendido por el dispositivo de procesamiento y control para comparar datos electrónicos, que se intercambian entre los varios componentes funcionales, con datos de control almacenados predeterminados. Esta forma de realización permite al módulo lógico programable establecer por ejemplo un intercambio de datos erróneos y/o un intercambio no permitido de datos y dado el caso tomar acciones de corrección, por ejemplo previniéndose un intercambio de este tipo. Igualmente, los datos de control almacenados pueden adaptarse en función de los datos electrónicos entrantes. De este modo, puede por ejemplo una pulsación de tecla determinada o una secuencia de datos recibida a través de la conexión de red se reconoce por el dispositivo de comparación y este inicia a continuación una función de control predefinida, cuyo resultado se manifiesta en una adaptación de los datos de control.

Preferentemente, una configuración de la invención prevé que los varios componentes funcionales para aparatos acoplados a los varios componentes funcionales, durante el intercambio de datos, estén realizados como componentes funcionales de operación transparente. De este modo se garantiza que el software en marcha en el ordenador personal, no se vea afectado por la presencia del módulo de seguridad. El software para dirigir el ordenador personal no tiene que estar adaptado por lo tanto para un uso con el módulo de seguridad. Como una ventaja adicional de esta forma de realización, un virus informático anidado en el software del ordenador personal no podría establecer si está presente un módulo de seguridad que deba eludirse.

Es también parte de la invención un procedimiento para dirigir y controlar el tráfico de datos de un ordenador personal con ayuda de un módulo de seguridad descrito anteriormente, en el que una conexión de procesador del módulo de seguridad, conectada con un módulo lógico programable del módulo de seguridad, está en comunicación con un procesador central del ordenador personal para intercambiar datos electrónicos, a una conexión de disco duro conectada con el módulo lógico programable del módulo de seguridad está acoplado un disco duro del ordenador personal para intercambiar datos electrónicos, a conexiones de periféricos del módulo de seguridad, conectadas con el módulo lógico programable, están acoplados periféricos para la entrada de datos y/o salida de datos y el módulo lógico programable está conectado con un módulo de memoria, que comprende datos de inicialización para el módulo lógico programable, y comprendiendo el procedimiento las siguientes etapas:

- un dispositivo de procesamiento y control se hace funcional en el módulo lógico programable del módulo de seguridad por medio de autoinicialización del módulo lógico programable, usándose los datos de inicialización del módulo de memoria, y
- un tráfico de datos desde y/o hacia el disco duro del ordenador personal así como un tráfico de datos entre los periféricos para la entrada de datos y/o salida de datos y el procesador central del ordenador personal se ejecutan exclusivamente a través del módulo de seguridad y se dirigen y controlan por medio del dispositivo de procesamiento y control.

Ventajosamente, el procedimiento está configurado de modo que el tráfico de datos desde y/o hacia el disco duro del ordenador personal así como el tráfico de datos entre los periféricos para la entrada de datos y/o salida de datos y el procesador central del ordenador personal se ejecutan a través del módulo de seguridad de manera transparente para el procesador central, el disco duro y los periféricos para la entrada de datos y/o salida de datos.

En una configuración ventajosa adicional del procedimiento, los datos del tráfico de datos ejecutado a través del módulo de seguridad se comparan en el módulo de seguridad por medio de un dispositivo de comparación con datos comparativos almacenados predeterminados. Puede ser además ventajoso cuando la autoinicialización del módulo lógico programable tiene lugar al conectarse una tensión de servicio.

Descripción de ejemplos de realización preferidos

La invención se explica en detalle a continuación por medio de ejemplos de realización haciendo referencia a un dibujo. En este caso, la única Figura 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 componentes funcionales que comprenden un módulo lógico programable 2, una conexión de procesador 3, una conexión de disco duro 4, conexiones de periféricos 5 y un módulo de memoria 6. El módulo de seguridad 1 está instalado en un ordenador personal 10, que está equipado con un procesador central o un microprocesador 11, un disco duro 12, una memoria 14 y periféricos 13. En el caso del ordenador personal 10 puede tratarse de cualquier tipo de sistema informático 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 - “Personal Digital Assistent” (asistente digital personal)).

El módulo lógico programable 2 puede estar conformado por medio de cualquier tipo de módulo lógico programable (también denominado PLD - “Programmable Logic Device” (dispositivo lógico programable)), que puede programarse para procesar datos electrónicos que se intercambian entre los varios componentes funcionales. En este caso puede tratarse tanto de un módulo lógico programable varias veces como de un módulo lógico programable solo una vez. En el caso de los módulos lógicos programables varias veces, la programación tiene lugar por medio de células de memoria comprendidas por el módulo lógico programable 2, por ejemplo células de memoria SRAM, EPROM, EEPROM y/o flash. Preferentemente, para el módulo lógico programable 2 se usa un módulo FPGA (FPGA - “Field Programmable Gate Array” (disposición de puertas programables en campo)). Como módulo lógico programable 2 puede usarse sin embargo también un módulo CPLD (CPLD - “Complex Programmable Logic Device” (dispositivo lógico programable complejo) o un módulo ASIC (ASIC - “Application Specific Integrated Circuit” (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 denominado ordenador multiprocesador, la conexión de procesador 3 puede diseñarse para poder dirigir un intercambio de datos o bien solo con uno o bien con dos o más de los varios microprocesadores. La conexión de procesador 3 puede estar también diseñada para producir una conexión indirecta entre el módulo lógico programable 2 y el microprocesador 11. Por ejemplo, esta conexión puede tener lugar a través de un controlador, en particular un controlador de disco duro. Con ello se garantiza que el microprocesador intercambie su información igual que antes a través del controlador con los periféricos. Esto es importante, por ejemplo, en formas de realización de la invención en las que, si bien tiene lugar una consulta del microprocesador 11 al disco duro 2 a través del módulo de seguridad 10, en cambio el microprocesador 11 no percibe la presencia del módulo de seguridad 10, es decir, cuando los componentes funcionales del módulo de seguridad 1 para el intercambio de datos entre el microprocesador 11 y el disco duro 12 operan de manera transparente. Para ello, el módulo de seguridad 10 finge, ante el microprocesador 11, funciones del disco duro 12. Es decir, el módulo de seguridad 10 tiene que enviar a través de la conexión de 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 que se produce una conexión con uno o varios disco(s) duro(s) 12 del ordenador personal 10. En el caso del disco duro 12 puede tratarse de un disco duro de cualquier tecnología disponible, en particular cualquier tamaño constructivo aleatorio y/o capacidad de memoria, por ejemplo puede este comprender también un denominado MicroDrive. La transmisión de datos desde y hacia el disco duro 12 puede tener lugar por medio de una norma de comunicación cualquiera, habitual del tráfico, por ejemplo una norma IDE, una norma EIDE o una norma SATA (IDE - “Integrated Drive Electronics”, EIDE - “Enhanced IDE”, SATA - “Serial Advanced Technology Attachments”).

Las conexiones de periféricos 5 pueden comprender conexiones de cualquier tipo de periféricos 13, que pueden controlarse por un ordenador personal 10. En particular, en este sentido se trata de periféricos para la entrada de datos, por ejemplo un teclado, un ratón, un escáner o similar, y de periféricos para la salida de datos, por ejemplo una tarjeta gráfica, una impresora, una tarjeta de sonido o similares. Sin embargo, pueden estar presentes también conexiones de periféricos 5 con periféricos, que además de para la entrada de datos sirven también para la salida de datos, por ejemplo con aparatos de almacenamiento interno (es decir, que se encuentran dentro de una carcasa del ordenador personal 10) o con aparatos de memoria externos (es decir, que se encuentran fuera de una carcasa del ordenador personal 10) así como con tarjetas de red con por ejemplo funcionalidad de módem, ISDN y/o LAN.

En particular, las tarjetas de red 1 representan una fuente importante de datos dañinos, porque 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 forma involuntaria, por ejemplo debido a errores de software, errores operativos o virus informáticos, mensajes a otros sistemas informáticos conectados a la red de comunicación, por ejemplo por medio de correo electrónico. En una forma de realización de la invención, está por lo tanto previsto que todo el tráfico de datos entre el microprocesador 11 del ordenador personal 10 y las tarjetas de red (no representadas) tenga lugar a través del módulo de seguridad 1 y se dirige y/o controla por el módulo lógico programable 2. En este sentido pueden estar presentes tarjetas de red con cualquier norma o protocolo de comunicación.

En particular puede estar previsto que una o varias de las tarjetas de red presenten dos o más denominadas direcciones MAC (MAC - “Media Access Control” (control de acceso al medio)). La dirección MAC es una dirección que se adjudica a cada tarjeta de red durante su producción y con la que la tarjeta de red se dirige a un plano de transmisión de una red de comunicación, que se encuentra por debajo del plano de transmisión en el que se usan las denominadas direcciones IP (IP - “Internet Protocol” (protocolo de Internet”). Para poder dirigir un ordenador personal opcionalmente a un plano de administración de sistemas o un plano de sistema operativo, estos tienen que poder dirigirse unívocamente a través de una dirección MAC dependiente del plano de la tarjeta de red o dirección IP del ordenador. Para ahorrar una tarjeta de red adicional para la administración de sistemas y una conexión por cable adicional necesaria para ello y 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 de procesador 3, la conexión de disco duro 4 y las conexiones de periféricos 5, pueden estar diseñadas como conexiones simples. Sin embargo, estas pueden también comprender, al menos en parte, circuitos más complicados, que efectúan por ejemplo una adaptación de protocolo y/o nivel de señales que van a intercambiarse. El módulo de seguridad 1 está equipado con medios de codificación y/o decodificación, para convertir señales entre diferentes normas de comunicación usadas en el ordenador personal 10. Los medios de codificación y/o decodificación pueden estar diseñados como partes del módulo lógico programable 2 y/o de las conexiones.

Por último, el módulo de memoria 6 sirve para proporcionar datos de inicialización al módulo lógico programable 2. En este caso, al menos una parte del módulo de memoria 6 estará diseñado como módulo de memoria no volátil para no perder su contenido de memoria después de desconectar la tensión de servicio. Los datos de inicialización se encuentran disponibles para el módulo lógico programable 2 en cualquier momento, en particular inmediatamente después de la aplicación de una tensión de servicio, y sirve 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 caso del módulo de memoria no volátil, puede tratarse de cualquier tipo de módulos de memoria que conserve su contenido también después de desconectar la tensión de servicio. Por ejemplo, el módulo de memoria 6 puede comprender una memoria flash. Puede tratarse también de un módulo de memoria en principio volátil, que se alimenta por una fuente de energía propia, por ejemplo una batería. El módulo de memoria no volátil puede estar también integrado en el módulo lógico programable 2.

Además del 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 programable 2, durante el funcionamiento, puede implantar datos para su uso posterior. Para ello, sin embargo puede consultarse también una parte de la memoria 14 del ordenador personal 10, reservándose esta parte en la autoinicialización del módulo lógico programable 2 para el módulo de seguridad 1 y pudiendo disponer libremente el microprocesador 11 solo de la parte restante de la memoria 14. De manera similar, puede solicitarse también una parte de la capacidad de memoria del disco duro 12 por el módulo de seguridad 1.

Los periféricos 13, el disco duro 12 y/o el microprocesador 11 pueden abordarse 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 insertable PCI, pueden ahorrarse con ello conexiones físicas separadas en el módulo de seguridad 1.

Para que el módulo de seguridad 1 realice de la manera más completa posible su función de control y dirección, en una forma de realización, todo el tráfico de datos entre el microprocesador 11, el disco duro 12 y los periféricos 13 se conduce a través del módulo de seguridad 1. Por motivos de velocidad puede ser ventajoso que determinados datos se intercambien sin el desvío a través del módulo de seguridad 1. Por ejemplo, en el caso de presencia de varios discos duros, el disco duro con datos menos importantes puede estar conectado también de manera directa con el microprocesador 11.

Para que el módulo de seguridad 1 pueda controlar y dirigir el tráfico de datos del ordenador personal 10, en primer lugar, los componentes funcionales del módulo de seguridad 1 deben desplazarse a un estado de partida definido. Para ello, después de aplicar una tensión de servicio, tiene lugar una inicialización del módulo lógico programable 2, en la que se prepara un dispositivo de procesamiento y control en el módulo lógico programable 2 y se le suministran datos de inicialización. El dispositivo de procesamiento y control sirve para dirigir todos los componentes funcionales del módulo de seguridad 1 independientemente del microprocesador 11.

El módulo lógico programable 2, después de la inicialización, puede recibir datos a través de las conexiones y comparar con datos implantados en el módulo de memoria 6, para ejecutar como reacción a lo mismo una acción, por ejemplo generar una advertencia cuando van a borrarse datos importantes.

Un proceso importante es la inicialización del disco duro 12 por medio de rutinas de programa almacenadas en BIOS, un programa mediador entre el software y el hardware de un ordenador personal. Durante un proceso de inicialización del ordenador personal 10 (denominado también proceso de arranque) se solicitan a través de un controlador del disco duro datos técnicos del disco duro 12, por ejemplo la capacidad de memoria del disco duro en cuestión. Esta consulta se recibe a través de la conexión de procesador 3 desde el módulo lógico programable 2 y se responde con ayuda de datos implantados en el módulo de memoria 6, referentes al disco duro 12. Cuando por ejemplo una región del disco duro 12 está ocupada por el módulo de seguridad 1, entonces se comunica al microprocesador 11 una capacidad de memoria de disco duro que está reducida la capacidad de memoria de la región ocupada.

Un acceso del microprocesador 11 al disco duro 12 tiene lugar según esto de modo que se reciben instrucciones del microprocesador 11 en el disco duro 12 en primer lugar desde el módulo lógico programable 2 a través de la conexión de procesador 3. Estas instrucciones se comprueban entonces por medio del dispositivo de procesamiento y control y se comparan con los datos implantados en el módulo de memoria 6. Cuando el dispositivo de procesamiento y control establece que no está permitida una acción correspondiente a la instrucción, es decir,

cuando el microprocesador 11 intenta llevar a cabo una acción no autorizada, por ejemplo acceder a una zona del disco duro 12 no accesible para el mismo, entonces esta instrucción no se transmite al disco duro 12. En su lugar, se transmite al microprocesador 11, a través de la conexión de procesador 3, un aviso de error, que es idéntico a un aviso de error del disco duro 12. De esta manera se finge ante el microprocesador 11 que ha tenido lugar un intercambio de datos entre él y el disco duro 12. El aviso de error puede ser por ejemplo un mensaje que informe de que la región en cuestión del disco duro 12 faltaría. Instrucciones permitidas y datos se transmiten inalterados a través de la conexión de disco duro 4 al disco duro 12. Esto significa que el módulo lógico programable 2, la conexión de procesador 3 y la conexión de disco duro 4 operan de forma transparente.

Se procede de manera similar, con un intercambio de datos con los periféricos 13 para la entrada de datos y/o salida de datos. Una entrada de datos puede tener lugar por ejemplo por medio de un teclado. En este caso al pulsar una tecla o una combinación de teclas, se envía en primer lugar una señal a través de esto a una conexión de periféricos 5 del módulo de seguridad 1. La señal se descodifica ahí o se transmite directamente al módulo lógico programable 2. Si el dispositivo de procesamiento y control del módulo lógico programable 2, debido a los datos almacenados en el módulo de memoria 6, establece que la ejecución de una instrucción asociada con la combinación de teclas lleva a una acción no autorizada, entonces se ignora la señal o bien por completo y/o se muestra visualmente una advertencia correspondiente a través de otro aparato periférico, por ejemplo a través de un monitor. De esta manera puede darse también una orden al dispositivo de procesamiento y control en sí, usando esta exclusivamente dentro del dispositivo de procesamiento y control para iniciar una rutina de software, pero la pulsación de tecla no se transmite al microprocesador 11. De este modo, se impide también que un software dañino que está en marcha en el microprocesador 11 supervise la operación del dispositivo de procesamiento y control.

Las características de la invención divulgadas en la descripción anterior, las reivindicaciones y el dibujo pueden tener importancia tanto individualmente como en cualquier combinación para la realización de la invención en sus distintas formas de realización.

REIVINDICACIONES

1. Módulo de seguridad (1) para dirigir y controlar el tráfico de datos de un sistema informático con un procesador central (ordenador personal) (10), con varios componentes funcionales, que están implementados en cada caso por medio de hardware y software, comprendiendo los varios componentes funcionales:

- un módulo lógico programable (2), que dirige y controla el tráfico de datos del ordenador personal (10), en el que, por medio de programación, está implementado un dispositivo de procesamiento y control para procesar datos electrónicos, que se intercambian entre los componentes del ordenador personal,
en el que
el dispositivo de procesamiento y control sirve para dirigir todos los componentes funcionales del módulo de seguridad (1) independientemente del microprocesador (11),
en el que
el módulo lógico programable (2) está realizado para autoinicializarse al conectarse una tensión de servicio,
en el que
el módulo lógico programable (2) está diseñado de modo que puede detectar un intercambio de datos no permitido y dado el caso adoptar acciones de corrección;
- una conexión de procesador (3) conectada con el módulo lógico programable (2) para intercambiar datos electrónicos con un procesador central (11) del ordenador personal (10);
- conexiones de periféricos (5) conectadas con el módulo lógico programable (2) para intercambiar datos electrónicos con periféricos (13) acoplados al ordenador personal (10) para la entrada de datos 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
en el módulo lógico programable (2), por medio de la programación, está implementado un dispositivo de comparación comprendido por el dispositivo de procesamiento y control, para comparar datos electrónicos, que se intercambian entre componentes del ordenador personal, con datos de control almacenados predeterminados; y
en el que
los datos de control almacenados pueden adaptarse en función de los datos electrónicos entrantes, en el que una secuencia de datos recibida se reconoce por el dispositivo de comparación y este activa a continuación una función de control predefinida, cuyo resultado se manifiesta en una adaptación de los datos de control, en el que la secuencia de datos se recibe desde el teclado o a través de la conexión de red del ordenador personal.

2. Módulo de seguridad (1) según la reivindicación 1, **caracterizado porque** los varios componentes funcionales están realizados como un sistema encapsulado, de modo que los componentes funcionales están reunidos formando un sistema que opera de manera independiente.

3. Módulo de seguridad (1) según la reivindicación 1, con un dispositivo de comparación, implementado en el módulo lógico programable (2) por medio de la programación, comprendido por el dispositivo de procesamiento y control, para comparar datos electrónicos que se intercambian entre los varios componentes funcionales, con datos de control almacenados predeterminados.

4. Módulo de seguridad (1) según una de las reivindicaciones 1 a 3, **caracterizado porque** los varios componentes funcionales están implementados en una tarjeta insertable.

5. Módulo de seguridad (1) según una de las reivindicaciones 1 a 4, **caracterizado porque** los varios componentes funcionales están implementados en una placa madre del ordenador personal (10).

6. Módulo de seguridad (1) según la reivindicación 5, **caracterizado porque** los varios componentes funcionales están implementados al menos en parte en un conjunto de chips de la placa madre.

7. Módulo de seguridad (1) según la reivindicación 6, **caracterizado porque** los varios componentes funcionales están conformados al menos en parte en un chip de puente norte del conjunto de chips de la placa madre.

8. Módulo de seguridad (1) según una de las reivindicaciones anteriores, **caracterizado porque** el módulo de memoria (6) está conformado en la memoria RAM del ordenador personal (10).

9. Módulo de seguridad (1) según una de las reivindicaciones anteriores, **caracterizado porque** el circuito está conectado con una tarjeta de red, que presenta otra dirección MAC asignada de forma fija, dirección de control de acceso al medio.

10. Módulo de seguridad (1) según una de las reivindicaciones anteriores, **caracterizado porque** los datos de control almacenados pueden adaptarse en función de los datos electrónicos entrantes.

11. Módulo de seguridad (1) según una de las reivindicaciones anteriores, **caracterizado porque** el ordenador personal (10) es un ordenador móvil, por ejemplo un ordenador portátil o un asistente digital personal.

12. Procedimiento para dirigir y controlar el tráfico de datos de un ordenador personal (10) con ayuda de un módulo de seguridad (1) según una de las reivindicaciones anteriores, en el que una conexión de procesador (3) del módulo de seguridad (1), conectada con un módulo lógico programable (2) del módulo de seguridad (1), está en comunicación con un procesador central (11) del ordenador personal (10) para intercambiar datos electrónicos, a una conexión de disco duro (4) conectada con el módulo lógico programable (2) del módulo de seguridad (1) está acoplado un disco duro (12) del ordenador personal (10) para intercambiar datos electrónicos, a conexiones de periféricos (5) del módulo de seguridad (1), conectadas con el módulo lógico programable (2), están acoplados periféricos (13) para la entrada de datos y/o salida de datos y el módulo lógico programable (2) está conectado con un módulo de memoria (6), que comprende datos de inicialización para el módulo lógico programable (2), y comprendiendo el procedimiento las siguientes etapas:

- un dispositivo de procesamiento y control se hace funcional en el módulo lógico programable (2) del módulo de seguridad (1) por medio de autoinicialización del módulo lógico programable (2), usándose los datos de inicialización del módulo de memoria (6); y
- un tráfico de datos desde y/o hacia el disco duro (12) del ordenador personal (10) así como un tráfico de datos entre los periféricos (12) para la entrada de datos y/o salida de datos y el procesador central (11) del ordenador personal (10) se ejecutan exclusivamente a través del módulo de seguridad (1) y se dirigen y controlan por medio del dispositivo de procesamiento y control.

13. Procedimiento según la reivindicación 12, **caracterizado porque** el tráfico de datos desde y/o hacia el disco duro (12) del ordenador personal (10) así como el tráfico de datos entre los periféricos (13) para la entrada de datos y/o salida de datos y el procesador central (11) del ordenador personal (10) se ejecutan a través del módulo de seguridad (1) de manera transparente para el procesador central (11), el disco duro (12) y los periféricos (13) para la entrada de datos y/o salida de datos.

14. Procedimiento según la reivindicación 12 o 13, **caracterizado porque** los datos del tráfico de datos ejecutado a través del módulo de seguridad (1) en el módulo de seguridad (1) se comparan por medio de un dispositivo de comparación con datos comparativos almacenados predeterminados.

15. Procedimiento según una de las reivindicaciones 12 a 14, **caracterizado porque** la autoinicialización del módulo lógico programable (2) tiene lugar al conectarse una tensión de servicio.

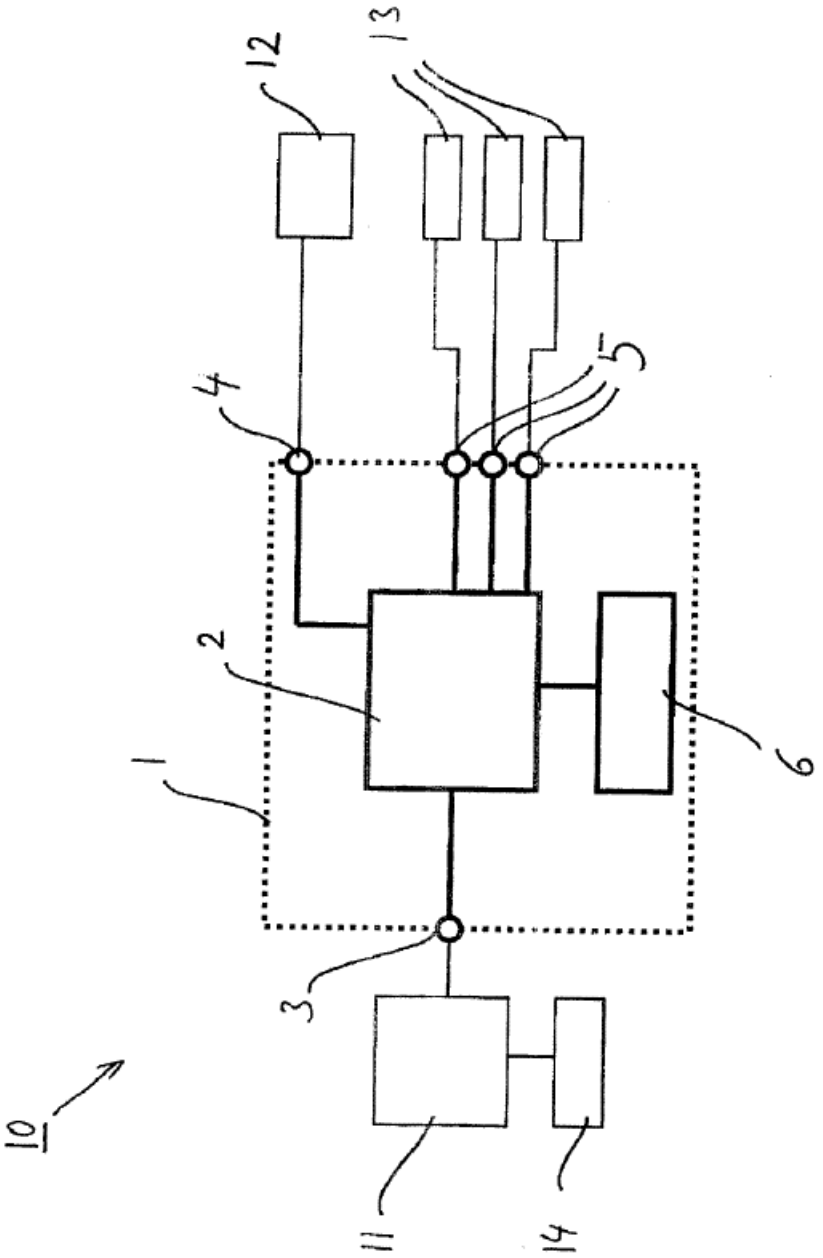

Fig.