(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 543 686**

(51) Int. CI.:

G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.09.2008 E 08165171 (3)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2015 EP 2045749**

(54) Título: **Procedimiento de aseguramiento de un terminal equipado con al menos una interfaz de comunicación**

(30) Prioridad:

28.09.2007 FR 0757934

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.08.2015

(73) Titular/es:

ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

CHARLES, OLIVIER y
VILLE, FRÉDÉRIQUE

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento de aseguramiento de un terminal equipado con al menos una interfaz de comunicación

La invención se refiere al campo de los terminales informáticos y más particularmente a un terminal equipado con al menos una interfaz de comunicación y a un procedimiento de aseguramiento de un terminal de ese tipo.

En el campo de los terminales informáticos, principalmente entre los terminales de tipo ordenador personal o PC (Personal Computer), se desarrolla la utilización de periféricos portátiles, bajo la forma por ejemplo de llaves USB. Estas llaves USB comprenden unas memorias susceptibles de almacenar a la vez unos datos y unos programas. Es necesario en consecuencia, prever unos medios para asegurar el contenido del PC al que dicho periférico se conecta con el fin de evitar cualquier contaminación por un virus informático o un programa no autorizado.

Se han desarrollado hasta el momento diferentes soluciones técnicas para asegurar el contenido del PC.

Una primera solución consiste en inhibir por programación la utilización de ciertos puertos de comunicación tras la configuración e instalación del PC. Esta solución es sin embargo demasiado radical porque impide cualquier utilización ulterior del o de los puertos de comunicación afectados.

Una segunda solución consiste en no autorizar la utilización de un puerto de comunicación más que para ciertos periféricos previamente declarados como autorizados. Esta solución supone disponer de un mecanismo de identificación del periférico y proceder a una declaración previa de los periféricos autorizados. Se convierte en engorrosa y compleja de poner en práctica.

Una tercera solución consiste en poner en práctica un mecanismo denominado HIPS (en inglés “Host Intrusion Prevention System”) de control de acceso a los ficheros almacenados en el PC en función de la identidad del o de los programas susceptibles de acceder a estos ficheros. Un mecanismo de ese tipo es pesado de gestionar puesto que supone definir previamente unos derechos de acceso para cada programa y fichero. Además, tiene el inconveniente de no enmascarar el árbol de los ficheros sino únicamente el contenido de los ficheros. Finalmente, un mecanismo de ese tipo puede ser bordeado por un usuario del PC.

El documento WO 02/087152 describe un conjunto de medios para asegurar un terminal mediante el empleo de reglas de seguridad definidas en relación a unos eventos a detectar.

Uno de los objetivos de la invención es remediar unas insuficiencias e inconvenientes del estado de la técnica y/o aportar en él unas mejoras.

La invención se refiere, según un primer aspecto, a un procedimiento de aseguramiento de un terminal según la reivindicación 1.

La invención utiliza unos eventos detectados para determinar un nivel de privilegios, es decir un conjunto de derechos a atribuir al usuario actual del terminal. A través de estos derechos, es posible controlar el acceso a los recursos físicos y lógicos del terminal.

El hecho de que el segundo conjunto de derechos se determine además en función de un estado de autenticación de un usuario permite reforzar la seguridad del terminal, puesto que el nivel de privilegio se podrá reducir para un usuario no autenticado o por el contrario incrementarlo para un usuario autenticado.

Según un modo de realización, el procedimiento comprende además una etapa de conmutación del modo de funcionamiento actual hacia otro modo de funcionamiento en el que el usuario actual de dicho terminal se beneficia de dicho conjunto de derechos, estando destinada dicha etapa de conmutación a ejecutarse cuando el conjunto de derechos determinado en la etapa de determinación es diferente de un conjunto de derechos atribuidos al usuario actual antes de dicha detección. Mediante un mecanismo simple de conmutación del modo de un funcionamiento a otro, es posible controlar el nivel de privilegio atribuido a un usuario dado que un modo de funcionamiento permite a un usuario beneficiarse del conjunto de los derechos asociados a este modo de funcionamiento y al nivel de privilegio atribuido.

Según el modo de realización particular, la etapa de conmutación comprende una etapa de suspensión, respectivamente de parada, de una primera sesión de trabajo y una etapa de reactivación, respectivamente de arranque, de una segunda sesión de trabajo. La conmutación de una sesión de trabajo a otra se puede utilizar para implementar la invención de modo simple.

Le invención se refiere, según un segundo aspecto, a un terminal según la reivindicación 7.

Según un modo de realización particular, el terminal según la invención comprende unos medios de puesta en práctica de las etapas del procedimiento según la invención.

Las ventajas enunciadas para el procedimiento según la invención se pueden trasladar al terminal según la invención.

Según una implementación preferida, las diferentes etapas del procedimiento según la invención se ponen en práctica mediante un software o programa de ordenador, comprendiendo este software unas instrucciones de programación destinadas a ejecutarse por un procesador de datos de un terminal informático y concebidas para controlar la ejecución de las diferentes etapas de este procedimiento.

En consecuencia, la invención se refiere también a un programa, susceptible de ejecutarse por un ordenador o por un procesador de datos, incluyendo este programa unas instrucciones para controlar la ejecución de las etapas de un procedimiento tal como se han mencionado anteriormente.

Este programa puede utilizar no importa qué lenguaje de programación, y estar bajo la forma de código fuente, código objeto, o de código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada, o en no importa qué otra forma deseable.

La invención se refiere también a un soporte de informaciones legible por un ordenador o procesador de datos, y que incluye unas instrucciones de programa tal como se ha mencionado anteriormente.

El soporte de informaciones puede ser no importa qué entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM en circuito microelectrónico, o incluso un medio de registro magnético, por ejemplo un disquete (floppy disc) o un disco duro.

Por otro lado, el soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que se puede encaminar a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede ser en particular descargado desde una red del tipo Internet.

Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que se incorpora el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Otros objetivos, características y ventajas de la invención surgirán a través de la descripción a continuación, dada únicamente a título de ejemplo no limitativo, y realizada con referencia a los dibujos adjuntos en los que:

- la figura 1 representa de manera esquemática un terminal según la invención;
- la figura 2 representa un organigrama de un modo de realización del procedimiento según la invención;
- las figuras 3 y 4 representan cada una un diagrama de cambio de estados implementado durante la etapa del procedimiento según la invención.

Le invención se describe en el caso de ejemplo de su aplicación a un terminal formado por un ordenador personal o PC (Personal Computer). La invención es aplicable sin embargo a cualquier tipo de terminal que disponga de una interfaz de comunicación que permita el establecimiento de un enlace con un periférico.

En el contexto de la invención, se considera que hay dos tipos de usuarios para un terminal de ese tipo: los usuarios propietarios y los usuarios inquilinos. A cada uno de estos dos tipos de usuarios se asocia un nivel de privilegios, es decir un conjunto de derechos definido en relación a los recursos físicos y lógicos del terminal: discos duros, periféricos, programas, ficheros y/o datos, etc. Estos derechos se descomponen normalmente, y de manera conocida, en derechos de lectura, derechos de escritura y/o derechos de ejecución. Sin embargo puede concebirse cualquier otra descomposición.

Se utiliza igualmente un nivel de privilegios para definir cuáles son los ficheros, programas y/o datos visibles para el usuario que se beneficia de este nivel de privilegio. Un nivel de privilegios se utiliza además para definir cuáles son los periféricos utilizables por un usuario y para qué tipo de uso. Se pueden definir incluso otros tipos de derechos por un nivel de privilegio.

En el sentido usual del término “propietario”, un único usuario es efectivamente propietario del PC. Se trata de un usuario que tiene una utilización regular y legítima del PC. La invención permite a un usuario de ese tipo beneficiarse de un nivel de privilegio elevado, asociado a su estatuto de utilización propietaria. Sin embargo, para la puesta en práctica de la invención, nada se opone a que varios usuarios, sean estos propietarios o no del PC en el sentido usual del término, puedan beneficiarse por turnos del estatuto de usuario propietario del PC. Aunque, según la invención, en un instante dado, un único usuario se beneficia de este estatuto de usuario propietario.

Los usuarios que no se benefician del estatuto de usuario propietario son todos unos usuarios que tienen el estatuto de usuario inquilino. Se trata por ejemplo de un usuario al que el usuario propietario ha prestado temporalmente su PC. Se atribuye a cualquier usuario inquilino un nivel de privilegio restringido, pero suficiente para que le permita una utilización del PC en tanto que inquilino.

Los derechos definidos para un conjunto de programas, ficheros o datos por el nivel de privilegio asociado a un usuario inquilino son generalmente reducidos con relación a los definidos para este mismo conjunto de programas, ficheros o datos para el nivel de privilegio de un usuario propietario. En particular, se puede prever que los ficheros y directorios visibles por un usuario inquilino sean menos numerosos, o al menos diferentes, a aquellos visibles para un usuario propietario.

Ventajosamente, un usuario que se beneficie del estatuto de usuario propietario puede definir los derechos asociados al estatuto de usuario inquilino.

La invención permite determinar simplemente si un usuario de un terminal debe considerarse como un usuario propietario o como un usuario inquilino mediante la detección de ciertos eventos, ligados o bien al establecimiento de un enlace entre el terminal y un periférico, o bien al estado de autenticación de este usuario.

La invención se describe más en detalle por referencia a la figura 1. El terminal 10, bajo la forma de ordenador personal o PC (Personal Computer), comprende una pantalla 11, un teclado 12, un ratón y una unidad central 20. La unidad central comprende un procesador de datos, una memoria, uno o varios discos duros, una o varias interfaces de comunicación 24, así como uno o varios buses de comunicación que permitan el establecimiento de enlaces de comunicación entre el procesador de datos y las interfaces de comunicación.

En el marco de la invención, se considera cualquier interfaz de comunicación que permita el establecimiento de un enlace, cableado o inalámbrico, con un periférico. Una interfaz de este tipo es por ejemplo una interfaz USB (Universal Serial Bus), una interfaz Ethernet, una interfaz PCMCIA (Personal Computer Memory Card International Association), un puerto de interfaz IEEE1394, etc.

La unidad central comprende igualmente un software de gestión que implementa un procedimiento según la invención cuando este software se ejecuta por el procesador de datos de la unidad central. Este software de gestión comprende tres módulos de programación:

- un primer módulo 21, denominado módulo de autenticación, que permite la autenticación de un usuario del PC, por ejemplo por medio de una palabra clave y de un código de acceso o nombre de usuario;
- un segundo módulo 22, denominado módulo de conmutación, que permite efectuar los cambios de nivel de privilegio;
- un tercer módulo 23, denominado módulo de detección, que permite detectar o bien el establecimiento de un enlace entre un periférico y el PC a través de una de las interfaces de comunicación del PC, o bien la interrupción del enlace establecido entre un periférico y el PC a través de una de las interfaces de comunicación del PC.

En el caso del ejemplo descrito, el módulo de detección 23 efectúa una supervisión de una o de varias de las interfaces de comunicación del PC.

En el caso de que la interfaz 24 de comunicación supervisada permita el establecimiento de un enlace cableado con un periférico 30, es decir en el caso de una conexión por cable o de una conexión por inserción directa —por ejemplo, de una llave USB— una conexión de ese tipo es detectable eléctricamente. Por ejemplo, si la interfaz de comunicación es una interfaz USB con una toma de acuerdo con el estándar USB, la inserción de una llave USB en esta toma provoca el establecimiento de un enlace eléctrico entre la llave y esta interfaz de comunicación. El establecimiento de un enlace de ese tipo mediante conexión es detectable en la interfaz física y el evento eléctrico detectado se señaliza al software controlador asociado a la interfaz de comunicación.

En el caso en el que la interfaz 24 de comunicación supervisada permita el establecimiento de un enlace inalámbrico con un periférico 30, por ejemplo un enlace de radio, la entrada de un periférico en el perímetro de detección de radio de la interfaz no es suficiente para comprometer la seguridad del terminal. No existe el riesgo hasta que hay un establecimiento de un enlace por radio, debido a la posibilidad de transferir unos datos a través de este enlace de radio. En una situación de ese tipo, es por tanto el establecimiento de un enlace de radio el que es el elemento a detectar para la puesta en práctica de la invención.

Generalizando, el módulo de detección 23 se concibe para detectar la aparición de un evento entre los dos eventos siguientes:

- un establecimiento, a través de la interfaz 24 de comunicación del PC, de un enlace entre un periférico 30 y el PC 10 (evento designado en este caso por “E1”); o
- una interrupción de un enlace establecido entre un periférico 30 y el PC 10 a través de una interfaz 24 de comunicación del PC (evento designado en este caso por “E2”).

En caso de detección de uno de estos eventos, el módulo de detección 23 está concebido para enviar al módulo de conmutación 22 un mensaje de notificación para señalizarle la naturaleza del evento detectado, es decir si se ha detectado un establecimiento o una interrupción.

El módulo de detección 23 está preferentemente integrado en el o los pilotos de interfaz de comunicación asociados a las interfaces de comunicación a supervisar. Puede estar igualmente integrado en un módulo del sistema operativo del PC. En todos los casos, arranca automáticamente con el arranque del PC, de manera que pueda detectar cualquier evento que intervenga sobre una de las interfaces de comunicación a supervisar tanto durante el arranque del PC, como después del arranque de este PC. A la inversa, el módulo de detección 23 es activo el mayor tiempo posible, principalmente hasta la activación del procedimiento de parada del PC.

El módulo de autenticación 21 se concibe para permitir a un usuario propietario del PC autenticarse y por lo tanto darse a conocer en tanto que usuario propietario del PC. Una vez autenticado, un usuario en ese tipo se beneficia entonces de un nivel de privilegios asociado a su estatuto de propietario. Inversamente, un usuario no autenticado no podrá beneficiarse de un mismo nivel de privilegios que un usuario propietario, más que en ciertas condiciones que serán descritas más adelante. En los otros casos, un usuario no se beneficia más que del nivel de privilegios asociado al estatuto de usuario inquilino. Este nivel de privilegios confiere al usuario actual del PC unos derechos más restringidos que los conferidos por el nivel de privilegios asociado al estatuto de usuario propietario.

El módulo de software de autenticación 21 se arranca tras la iniciativa de un usuario del PC. Este usuario introduce entonces, en una interfaz de usuario apropiada, los datos de autenticación solicitados por el módulo 21. Después del análisis de estos datos de autenticación, y en caso de autenticación con éxito, el usuario actual del PC es reconocido por el módulo de autenticación 21 mencionado como un usuario propietario del PC.

A la inversa, un usuario reconocido por el módulo de autenticación 21 como un usuario propietario del PC, puede decidir invalidar su autenticación. En este caso este usuario arranca el módulo de autenticación 21 e informa a una interfaz de usuario apropiada para transmitir su demanda de invalidación. Cuando se acepta su demanda de invalidación, se asocia un estatuto de usuario inquilino al usuario actual del PC.

En caso de autenticación con éxito, como en caso de aceptación de una demanda de invalidación, el módulo de autenticación 21 está concebido para enviar al módulo de conmutación 22 un mensaje de notificación para señalizarle la naturaleza del evento tratado por el módulo de identificación 21, es decir si ha tenido lugar una autenticación o una invalidación de autenticación. Estos dos eventos son designados respectivamente por “A1” (autenticación) y “A2” (invalidación de una autenticación).

El módulo de conmutación 22 comunica con los módulos 21 y 23 y recibe principalmente y trata los mensajes de notificación emitidos por estos dos módulos. En particular, el módulo de conmutación 22 está concebido para determinar, a continuación de la recepción del mensaje de notificación, el nivel de privilegio, es decir un conjunto de derechos a atribuir a un usuario del terminal. El nivel de privilegio determinado depende principalmente del evento notificado por medio del mensaje de notificación recibido. El módulo de determinación se describe más en detalle en el presente documento a continuación.

El módulo de conmutación 22 está concebido igualmente para provocar una conmutación de un modo de funcionamiento actual, en el que el usuario actual del terminal se beneficia de un conjunto de derechos asociados al nivel de privilegio actual, hacia otro modo de funcionamiento en el que el usuario actual del terminal se beneficia de un conjunto de derechos asociados al nivel de privilegio determinado. Esta conmutación no se efectúa más que cuando el nivel de privilegio determinado en la etapa de determinación es diferente del nivel de privilegio actual, antes de la recepción del mensaje de detección.

De manera práctica y conocida, un nivel de privilegio dado, es decir un conjunto de derechos definidos en relación con uno o unos recursos del terminal, se asocia a una sesión de trabajo y la conmutación de un nivel de privilegio a otro se efectúa durante la conmutación de una sesión de trabajo a otra, y esta conmutación se efectúa mediante interrupción (o bien mediante cierre completo, o bien simplemente suspensión) de la sesión de trabajo actual y posteriormente la apertura (sea arranque de una nueva sesión de trabajo o la reactivación de una sesión de trabajo previamente suspendida) de otra sesión de trabajo.

La noción de “sesión de trabajo” se utiliza en este caso en su sentido usual, siendo bien conocida esta noción para los usuarios del sistema operativo Windows®. Corresponde, de manera conocida, a un período de tiempo durante el que los recursos físicos o lógicos son accesibles para un usuario y se concede a un usuario del terminal un conjunto de derechos, derechos que se definen en relación a los recursos.

El procedimiento según la invención se describe más en detalle por referencia a la figura 2.

En la etapa 100, el PC es arrancado por un usuario. Los módulos de software 22 y 23 son arrancados automáticamente por el sistema operativo. Se abre una primera sesión de trabajo: asociada a un primer nivel de privilegios designado por “NProp”, que es el de un usuario propietario. Este nivel de privilegios es el nivel de privilegios por defecto. Se selecciona por tanto por defecto un conjunto de derechos.

En la etapa 110, el módulo de conmutación 22 está en un estado en el que es apto para recibir un mensaje de notificación procedente del módulo de autenticación 21 o del módulo de detección 23. Con la recepción de un mensaje de ese tipo, el módulo de conmutación ejecuta la etapa 120 siguiente.

En la etapa 120, el módulo de conmutación 22 determina un nivel de privilegios, nivel que es función del evento notificado a través del mensaje recibido y de un estado actual en un autómata que modeliza los cambios de nivel de privilegios según los eventos notificados.

Este autómata se representaba esquemáticamente en la figura 3. Comprende cuatro estados, representados por unos rectángulos y referenciados 31, 32, 33, 34. Se asocia un nivel de privilegios a cada uno de estos estados: a los estados 31, 32 y 33 se asocia el nivel de privilegios “NProp”, que es el de un usuario propietario, mientras que al estado 34 se asocia un nivel de privilegios designado por “NInq” que es el de un usuario inquilino. Cada transición posible entre dos de estos estados se representa por una flecha y se asocia a uno o varios de los eventos entre los eventos “E1”, “E2”, “A1”, “A2”.

Este autómata refleja el hecho de que cada uno de los estados 31, 32, 33, 34 se asocia a un par de valores de variables de estado binarias:

- la primera variable binaria representa el hecho de que se establezca o no un enlace entre el PC y un periférico a través de la interfaz de comunicación a supervisar,
- la segunda variable representa al hecho de que el usuario actual esté autenticado o no. De ese modo:
- el estado 31 corresponde a un estado en el que se ha establecido un enlace entre el PC y un periférico de este PC y el usuario actual está autenticado;
- el estado 32 corresponde a un estado en el que no se ha establecido un enlace entre el PC y un periférico de este PC y el usuario actual está autenticado;
- el estado 33 corresponde a un estado en el que no se ha establecido un enlace entre el PC y un periférico de este PC y el usuario actual no está autenticado;
- el estado 34 corresponde a un estado en el que se ha establecido un enlace entre el PC y un periférico de este PC y el usuario actual no está autenticado.

De la definición de estos estados, se deriva naturalmente la definición de las transiciones posibles entre estos estados, puesto que según el estado notificado, hay cambio del valor de una de las dos variables de estado binarias.

El autómata representado en la figura 3 puede implementarse mediante generación de una tabla que define, para estado y para cada evento posible, el nuevo estado actual. Un ejemplo de una tabla de ese tipo se da en el presente documento a continuación.

Estado actual	Evento notificado			
	E1	E2	A1	A2
31	31	32	31	34
32	31	32	32	33
33	34	33	32	33
34	34	33	31	34

Destaca claramente de esta tabla que cuando el estado actual es por ejemplo el estado 33, el nuevo estado actual será:

- el estado 34 si se notifica la aparición del evento “E1”;
- el estado 33 si se notifica la aparición del evento “E2”;
- el estado 32 si se notifica la aparición del evento “A1”;
- el estado 33 si se notifica la aparición del evento “A2”.

En otros términos, la figura 3 representa de manera gráfica las transiciones posibles entre los estados 31, 32, 33, 34 tal como se definen en la tabla del presente documento a continuación.

El nuevo nivel de privilegios (nivel de privilegios actual) se deduce a continuación del nuevo estado actual, por ejemplo mediante la utilización de la tabla de correspondencia siguiente:

Estado actual	Nivel de privilegios
31	NProp
32	NProp
33	NProp
34	NInq

Durante la primera ejecución de la etapa 120, el estado actual es el estado 32, es decir que a continuación del arranque del terminal, el usuario actual del terminal se beneficia por defecto del estatuto de usuario propietario.

En la etapa 130, el módulo de conmutación efectúa un cambio de modo de funcionamiento, mediante el cierre de la sesión actual y posteriormente la abertura de una nueva sesión, cuando el nuevo nivel determinado en la etapa 120 es diferente del nivel de privilegios actual, asociado a la sesión actual.

Posteriormente el procedimiento se prosigue en la etapa 110, siendo ejecutadas las etapas 110 a 130 cíclicamente hasta la parada del PC.

Según un modo de realización particular, se activa una temporización de una duración predefinida a continuación de la llegada al estado 32, temporización al cabo de la cual el nuevo estado actual es el estado 34, asociado al nivel de privilegios “NInq” si, durante este periodo, no se establece ningún enlace entre el PC y un periférico supervisado por el módulo de detección 23, es decir el evento E1 no ha sido detectado durante este periodo. De esta manera, un terminal inutilizado durante una cierta duración conmuta automáticamente a un modo de funcionamiento en el que el nivel de privilegio es reducido. Esto limita el riesgo de utilización del terminal por una persona no autorizada. Por el contrario, en tanto que el enlace entre el periférico y el PC se mantenga y este usuario esté autenticado, situación que corresponde al estado 31, no se efectúa ninguna conmutación, beneficiándose el usuario del terminal en ese estado del estatuto de usuario propietario.

El principio de la invención se generaliza a la supervisión de varias interfaces de comunicación. En este caso, se prevé un módulo de detección por interfaz de comunicación a supervisar. Por el contrario, solo es necesario un módulo de conmutación en este caso y cada uno de los módulos de detección se concibe para enviar a este módulo de conmutación un mensaje de notificación en caso de detección de la aparición de uno de los eventos E1 o E2.

El principio de la invención se generaliza igualmente a la utilización simultánea de varios periféricos. Esta variante implica la presencia de varias interfaces de comunicación cuando solo puede estar establecido un enlace en un momento dado con un periférico. Sin embargo, según la naturaleza de la interfaz de comunicación utilizada, y principalmente en el caso de un enlace inalámbrico entre una interfaz y un periférico, se puede concebir que se establezcan simultáneamente varios enlaces de comunicación con un periférico con una interfaz de comunicación única.

El autómata utilizado en este caso se modifica para tener en cuenta una pluralidad de eventos de tipo E1 o E2. Este nuevo autómata se ilustra en la figura 4, en el caso en el que se considera que se pueden establecer simultáneamente dos enlaces de comunicaciones con una o dos de las interfaces de comunicación a supervisar.

Se definen dos nuevos estados 31bis y 34bis y los niveles de privilegio asociados a los diferentes estados se definen esta vez según la tabla del presente documento a continuación.

Estado actual	Nivel de privilegios
31	NProp
32	NProp
33	NProp
34	NInq
31 bis	NProp
34bis	NInq

La tabla que define las transiciones entre estados se da en el presente documento a continuación.

Estado actual	Evento notificado			
	E1	E2	A1	A2
31	34bis	32	31	34
32	31	32	32	33
33	34	33	32	33
34	34bis	33	31	34
31bis	31bis	34	31bis	34bis
34bis	34bis	31	31bis	34bis

La invención se generaliza a un número cualquiera de enlaces de comunicación, el número de estados en el autómata es 2(1+n) en la que n es el número de enlaces de comunicación tenidos en cuenta.

La parte del autómata que define las transiciones entre los estados 31, 34 por un lado, y 31bis, 34bis por otro lado cuando se detecta un evento E1 o E2 puede en efecto ser replicado un número cualquiera de veces: de ese modo se añade, cada vez que debe ser tenido cuenta un nuevo enlace de comunicación, una pareja de estados 31ter, 34ter, posteriormente 31cuater, 34cuater, etc. Las transiciones entre los estados 31bis, 34bis por un lado y 31ter,

34ter por otro lado se definen de manera idéntica a las transiciones entre los estados 31, 34 por un lado y 31bis, 34bis por otro lado, y así sucesivamente para cada nuevo par de estados añadido.

La invención es aplicable a cualquier terminal informático que disponga de al menos una interfaz de comunicación con un periférico de almacenamiento de datos.

REIVINDICACIONES

1. Procedimiento de aseguramiento de un terminal (10) equipado con al menos una interfaz (24) de comunicación, comprendiendo el procedimiento,

- una etapa (110) de análisis de los enlaces establecidos con el terminal con el fin de detectar o bien un establecimiento de un enlace entre un periférico (30) y dicho terminal por medio de dicha interfaz de comunicación, o bien una interrupción de un enlace de ese tipo,
- una etapa de implementación de medios de autenticación de un usuario del terminal,
- una etapa para atribuir a un usuario no autenticado por dichos medios de autenticación un primer conjunto de derechos definidos en relación a los recursos físicos y lógicos del terminal de los que se beneficia,
- una etapa (130) de conmutación, a continuación de una detección de un establecimiento de un primer enlace entre un periférico (30) y dicho terminal, desde un primer modo de funcionamiento en el que el usuario se beneficia del primer conjunto de derechos hacia un segundo modo de funcionamiento en el que el usuario actual de dicho terminal se beneficia de un segundo conjunto de derechos más restringido que el primer conjunto de derechos,
- una etapa (130) de conmutación, a continuación de una autenticación de dicho usuario por dichos medios de autenticación, desde el segundo modo de funcionamiento en el que el usuario se beneficia del segundo conjunto de derechos hacia un tercer modo de funcionamiento en el que el usuario actual de dicho terminal se beneficia del primer conjunto de derechos.

2. Procedimiento según la reivindicación 1, que comprende además, cuando el terminal está en el segundo modo de funcionamiento,

- una etapa (130) de conmutación desde el segundo modo de funcionamiento hacia el primer modo de funcionamiento en caso de detección de una interrupción de dicho enlace.

3. Procedimiento según la reivindicación 1, en el que se selecciona un conjunto de derechos por defecto en el arranque de dicho terminal.

4. Procedimiento según la reivindicación 2, en el que las etapas de conmutación comprenden una etapa de suspensión, respectivamente de parada, de una primera sesión de trabajo y una etapa de reactivación, respectivamente de arranque, de una segunda sesión de trabajo.

5. Programa informático que comprende unas instrucciones de códigos de programa para la ejecución de las etapas de un procedimiento según una cualquiera de las reivindicaciones 1 a 4 cuando dicho programa se ejecuta por un procesador de datos.

6. Soporte de registro legible por un procesador de datos en el que se registra un programa que comprende unas instrucciones de códigos de programas para la ejecución de las etapas de un procedimiento según una cualquiera de las reivindicaciones 1 a 4.

7. Terminal equipado con al menos una interfaz de comunicación, que comprende,

- unos medios (23) de análisis de los enlaces establecidos con el terminal con el fin de detectar o bien un establecimiento de un enlace entre un periférico (30) y dicho terminal por medio de dicha interfaz de comunicación, o bien una interrupción de un enlace de ese tipo,
- unos medios (21) de autenticación de un usuario del terminal,
- unos medios para atribuir a un usuario no autenticado por dichos medios de autenticación, un primer conjunto de derechos definidos en relación a los recursos físicos y lógicos del terminal,
- unos medios de conmutación (130), a continuación de una detección de un establecimiento de un primer enlace entre un periférico (30) y dicho terminal, desde un primer modo de funcionamiento en el que el usuario se beneficia del primer conjunto de derechos hacia un segundo modo de funcionamiento en el que el usuario actual de dicho terminal se beneficia de un segundo conjunto de derechos más restringido que el primer conjunto de derechos,
- una etapa de conmutación (130), a continuación de una autenticación de dicho usuario por dichos medios de autenticación, desde el segundo modo de funcionamiento en el que el usuario se beneficia del segundo conjunto de derechos hacia el primer modo de funcionamiento en el que el usuario actual de dicho terminal se beneficia del primer conjunto de derechos.

8. Terminal según la reivindicación 7, que comprende unos medios de implementación de las etapas del procedimiento según una cualquiera de las reivindicaciones 2 a 4.

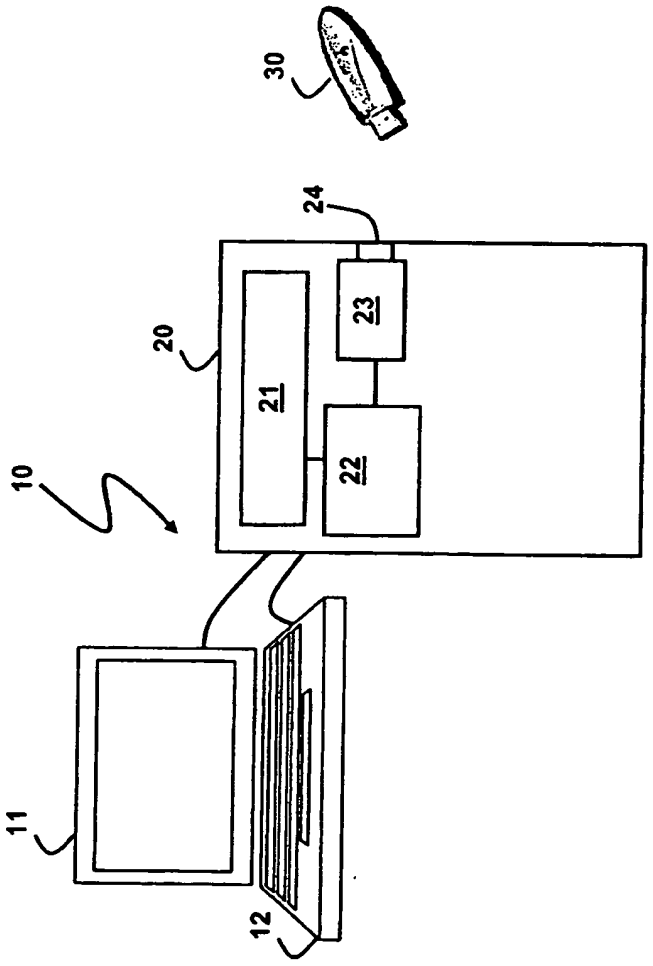

Fig. 1

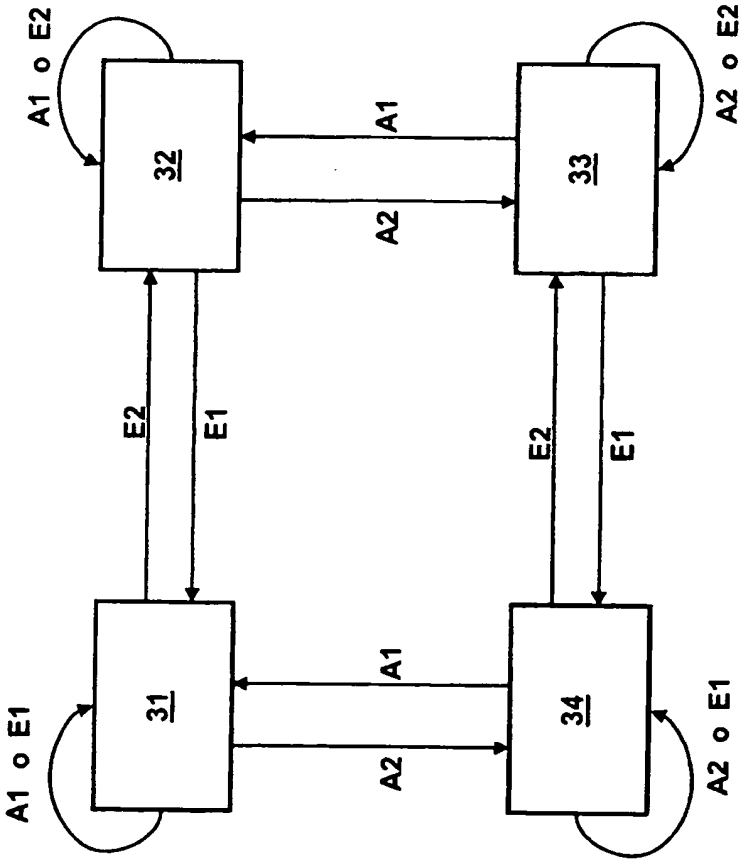
A1 o E2
A2 o E2
32
33
A1
A2
E2
E1
E2
E1
31
34
A1
A2
A1 o E1
A2 o E1

Fig. 3

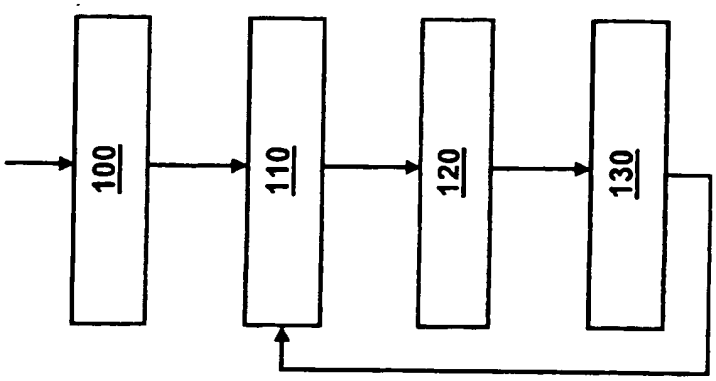
100
110
120
130

Fig. 2

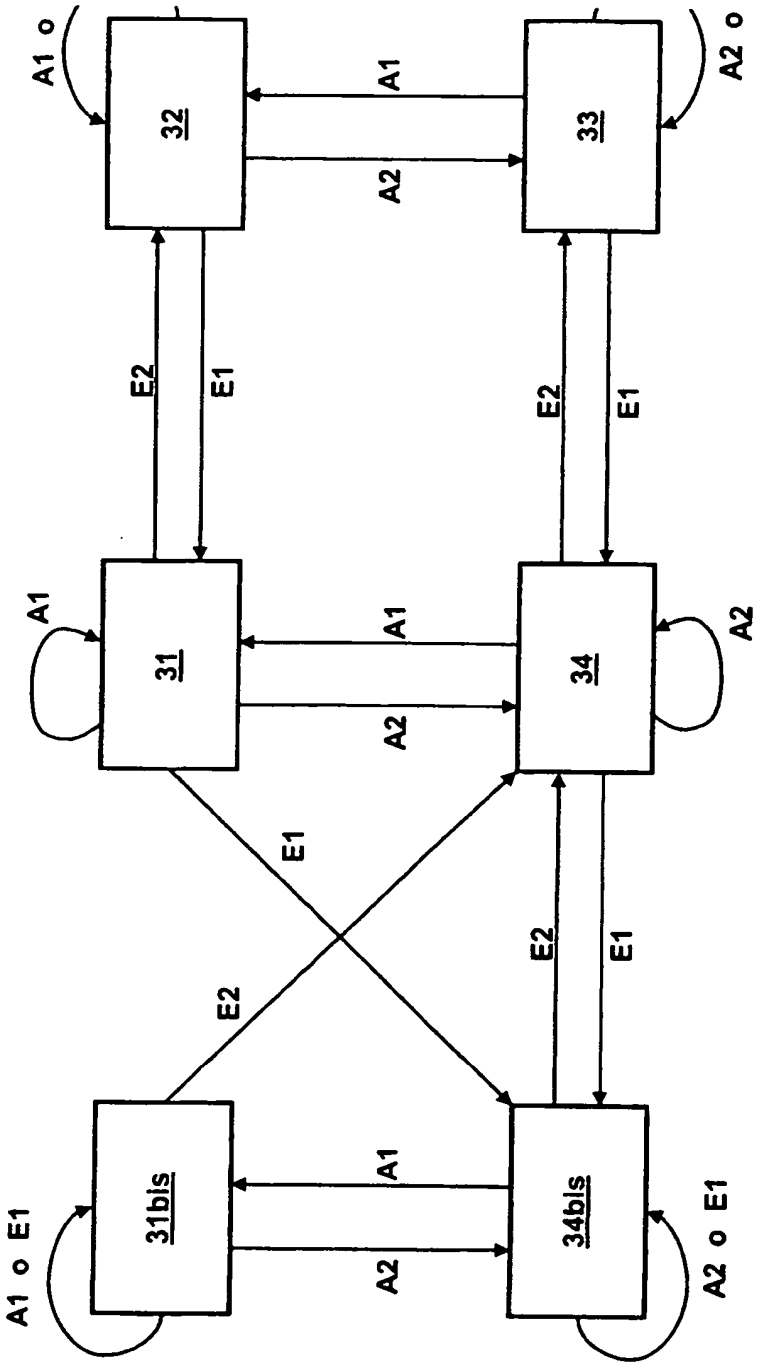
A1 o
32
A1
A2
33
A2 o
E2
E1
E2
E1
A1
31
A1
A2
34
A2
E1
E2
E2
E1
A1 o E1
31bis
A1
A2
34bis
A2 o E1

Fig. 4