Priority text based on the PCT text with handwritten modified passages

A METHOD OF MAKING SECURE AND CONTROLLING ACCESS TO INFORMATION FROM A COMPUTER PLATFORM HAVING A MICROCOMPUTER

The present invention relates to a method of making secure and controlling access to information such as data and/or applications, from a computer platform having a microcomputer.

In general, the strongly developing market for microcomputers, network technology, and low-cost large-capacity recording media has led to conditions that are favorable for increasing communication and/or interchange of information, and also to commercial activities based on making data and/or applications available to potential users on demand and in return for payment, from computer platforms that are fitted with microcomputers, in particular of the personal type.

Unfortunately, by definition, a personal microcomputer is a computing machine designed for a variety of uses (personal or professional applications, games, technical applications, ...), i.e. a computer machine having so-called "open" architecture in the sense that new elements, both software and hardware can readily be added to change the configuration of the machine as a function of users own requirements and/or as a function of the services or applications accessible to users, whether freely or on payment.

As a result, there are computer platforms that operate in a generally non-secure context, which context is even less secure in that there is always parallel activity in the development of piracy techniques. This parallel development of piracy can present problems as a function of the uses, services, and/or applications that may be implemented on such "open" architecture computer platforms.

To solve these problems, numerous solutions have been proposed in the field of security, such as the following, for example:

• installing identity codes to identify users before any communication or interchange of data;

• installing access codes to obtain authorization to access data and/or applications;

• using encoding or encrypting techniques to guarantee that data being transmitted or interchanged is kept confidential or secret; and/or

• certificates to authenticate the origin and the accuracy of data that is being transmitted or exchanged, ...

Unfortunately, even at high levels of sophistication, such solutions turn out to be insufficient, and this can be seen clearly from the particular example concerning the development of commercial activities which, as mentioned above, are based on making information available on request and for payment. Even with all or some of the solutions that have been proposed in the past, such applications cannot be viable if the information is accessed on a computer platform that is not secure.

The reliability of safety checks intended to guarantee that a user is indeed entitled to access the information and/or that the fees corresponding to said access have indeed been paid, for example, can never be complete when said checks are performed in a non-secure environment.

The object of the invention is specifically to propose a method enabling a computer platform to be made secure, in particular while accessing information such as data and/or applications from such computer platforms.

To this end, the invention provides a method of making secure and monitoring access to information from a computer platform having a microcomputer, the method being characterized in that it consists:

• in producing at least one non-rewritable recording medium on which information such as data and/or

applications is recorded in a predetermined logic format, together with operating software for said information;

• in defining authorized users having access rights to the information stored on the recording medium together with possible limits on such access rights;

• in configuring or transforming the computer platform of an authorized user into a secure workstation to prevent any hardware and/or software intrusion seeking to gain undue access to the information or to make use thereof instead of an authorized user and without that user's agreement;

• in loading the operating software from the recording medium into the computer platform, said operating software being read by an appropriate reader of the computer platform;

• in enabling the information stored on the recording medium to be used within the limits of the rights acquired by the authorized user; and

• during said use, in being able to exchange and/or communicate in secure manner data with a network to which the computer platform is connected.

The method defines a generic procedure which makes it possible to make secure a computer platform of the personal microcomputer type in a network, for example, so as to enable data and applications to be accessed and used in complete security by only those users that are entitled thereto, and to do so within the limits of their entitlement.

Such a method does not require physical standards (physical format for media or data) but defines the fundamental elements of hardware and software architecture making it possible to make use of data protected by a specific logic format in complete security.

This architecture is characterized in particular by:

• booting the operating system from a non-rewritable medium;

• data and communications security standards implementing cryptographic algorithms, and secure communications protocols; and

• hardware components for performing secure functions.

The security provided by such a method is of a high level and for small extra cost concerning the hardware and software architecture.

The cost of the hardware components to be added to architecture of a basic or reference personal microcomputer is modest, the components used are standard, and they can be added incrementally to said basic architecture, and the software cost is fixed for each operating system supported, independently of the data and applications that are to be protected.

In general, the method can be implemented on two types of computer platform:

• a closed platform initially designed to integrate the security hardware elements in the basic hardware architecture (on the mother board); and

• an open platform where an additional card is added to provide the hardware and/or software components that are necessary and sufficient to ensure that the method is implemented.

Thus, in an important advantage of the invention, any recording medium, even when duplicated, cannot be used on a machine that does not comply with the method.

In another advantage, when the secure computer platform is in dialog over a network with a controlling server or with another computer platform, that other platform or server knows that the dialog will take place in complete security.

In another advantage of the invention, any publisher of applications is guaranteed that accesses to and uses of the recording media it publishes will indeed be performed in compliance with the conditions laid on users.

The method of the invention makes it possible to make access to information secure and to control it, with the method comprising overall three main stages.

The first stage concerns producing at least one non-rewritable recording medium, i.e. a medium whose content is capable of being read only without any possibility of said contents being modified or altered, said medium carrying information to be protected which it is desired to make available to potential users, generally in return for payment, from computer platforms having a microcomputer of the personal type, for example.

In this first stage, the information to be protected is defined, such as data and/or applications, the operating systems for said information, and a set of security and control parameters.

The control parameters are necessary to enable the software that makes use of the data and/or the applications to operate on user computer platforms, while the security parameters are necessary to make use of the recording medium secure and also to make the use of information stored on the recording medium secure.

The security parameters for making use of a recording medium secure are, for example and in non-limiting manner:

- an identity parameter specific to the ~~medium~~ method;
- an authentication parameter for authenticating the contents of the recording medium, such as an encrypted signature, for example, as calculated from certain information stored on the recording medium; and
- a security table containing decoding algorithms in encrypted form.

The security parameters for making use of the information stored on the recording medium secure may be, for example, and in non-liming manner:

- a parameter relating to the security level required to be able to make use of the recording medium; and

• ~~at least~~ one identity parameter specific to the data and/or ~~each~~ application stored on the recording medium.

Thereafter, all of the above information is formatted using a predetermined logic format, and some or all of the information is encoded or encrypted to provide better protection in application of the scheme defined by the above-mentioned security table. It should be observed that these operations are transparent relative to the data and/or applications that are to be protected.

Thereafter, the information is stored on a non-rewritable recording medium which is advantageously a medium having large storage capacity and low cost, for example a CDROM (a non-erasable digital optical disk) or a DVD (a digital video disk).

The second stage relates to making secure the computer platforms from which the recordings can be used and operated in complete security.

In general, the method consists in implementing a hardware security device with at least ROM-type memory to record therein the security and control software, together with a management controller.

Two cases then need to be considered, the case of computer platforms having so-called "closed" architecture and the case of computer platforms having so-called "open" architecture. A computer platform is said to be of closed architecture when the machine has been specially designed or adapted to implement the method, i.e. it is already made secure by integrating the hardware security device and the associated software. In contrast, an open architecture platform is not secure for implementing the method, and under such circumstances it is necessary to make it secure by implanting the hardware security device in the form of an electronics card together with the associated software.

At this stage, it should be observed that a purely software security solution is by definition fragile,

which is why the method also provides for the presence of a hardware device which makes security more reliable.

The essential function of the hardware security device and of the associated software is to prevent any hardware and/or software intrusion seeking to make unauthorized use of the recording medium ~~to gain free access~~ and to the information stored on the medium or to enable use by a user other than an authorized user and without that user's agreement, and to provide continuous monitoring that the method is running under the required security conditions.

The third stage concerns a potential user of a recording medium accessing and using it from an appropriately secure computer platform.

To illustrate this third stage, an example is described below in which the first stage is performed by a publisher of applications that gives users recording media for free, but that requires use to be paid for in application of a conventional billing process.

When the publisher supplies a recording medium, the user is also given a portable medium such as a smart card, for example.

On the smart card, the publisher records a certain amount of information, for example and in non-limiting manner:

- an identity code specific to the user known as a PIN CODE, which code is nevertheless not required to implement the method;
- keys for decoding or decrypting information stored on the recording medium;
- the security level required to make use of the information; and
- the identity parameter specific to the data and/or applications, corresponding to the parameter recorded on the medium.

The recording medium and the portable medium are inserted into appropriate readers with which the user's

secure computer platform is fitted, and the platform can be put into operation.

This is done by means of monitoring software stored in the hardware security device and which is executed to control putting the machine into operation. When switched on, the hardware security device initializes itself and passes from one state to another state on the basis of time criteria. In general, if it does not receive any information or orders within a determined length of time, execution of the method is automatically stopped.

Initially, the ~~hardware security device and the associated~~ software identifies the recording medium. To do this, the identity parameter specific to the recording medium is read from the medium and compared with the parameter prerecorded in the hardware security device. These two parameters are verified by the management controller, and if they are not identical or do not satisfy a predetermined relationship, then execution of the method is automatically stopped, the recording medium ~~becomes~~ is unusable, and the machine is no longer secure in the sense that the hardware security device and the associated software are no longer accessible. Otherwise, if the verification is satisfactory, then the recording medium has been correctly identified, but that is not sufficient to access and use the data and/or applications stored thereon, since the contents of the medium may have been modified.

Thereafter, the security hardware device and the associated software verify the integrity of the contents of the recording medium. To this end, the encrypted signature stored on the medium is read and the security hardware compares it with a signature as recalculated by itself or by the CPU of the computer platform on the basis of information taken from the recording medium, said signature subsequently being encrypted by the security hardware.

If the comparison between the two encrypted signatures does not give a satisfactory result, then the hardware security device deduces that the contents of the recording medium has been modified, i.e. that it is not the same as the contents which was originally produced. Implementation of the method is then stopped, the computer platform is no longer secure, and, preferably, operation of the computer platform is blocked. In other words, the user must then restart the computer platform under normal conditions of operation but without any possibility of accessing or using the recording medium, the hardware security device and the associated software becoming inaccessible. Otherwise, the security hardware recognizes the integrity of the ~~information stored on the~~ recording medium, i.e. that the medium complies with the medium as produced.

Thirdly, the security hardware ~~and the associated software~~ verify the security level required to be able to make use of the data and/or applications on the recording medium. To this end, the security level recorded on the computer's portable medium is read and compared with that recorded on the medium. If the security level is not satisfactory, then the computer platform is blocked as above.

Fourthly, the security hardware ~~and the associated software~~ verify whether the user is authorized to use the data and/or applications stored on the recording medium. To this end, the hardware security device reads ~~at least one~~ the parameter specific to ~~an~~ the application, ~~for example~~, and recorded on the user's portable medium, and it compares it with the corresponding parameter as recorded on the recording medium. This comparison can be for identity or for a predetermined relationship. If this verification does not give a satisfactory result, the computer platform is blocked, as before.

Fifthly, the hardware security device ~~and the associated software~~ verify that the basic software of the

computer platform has not been modified, for the purpose of detecting whether there has been any breach in the security of the method. If such a breach is detected, using known techniques, then the computer platform is blocked, as before.

Otherwise, and sixthly, the hardware security device and the associated software will curb the basic software of the computer platform, particularly when the platform is of open architecture, i.e. the hardware security device will, so to speak, put locks into place to inhibit certain functions of the basic software such as those which could normally give access to the recording medium, and will put into place new functions as required for proper running and use of the data and/or applications from the recording medium, once the checks performed thereon and on the user have been validated.

Before beginning a second stage of the boot process, the hardware security device and the associated software install in a standard form independent of the hardware environment, an interface for giving access to all of the security functions to be used in particular by the operating system when it starts after being loaded from the recording medium.

So far, the first stage of the process for starting or booting has made it possible to check the recording medium and the user's access rights, but it is now necessary to perform security checks to verify the integrity of the computer platform both with respect to hardware and with respect to software.

To this end, the boot software is loaded from the recording medium and is executed to verify that the security conditions which have been satisfied by the recording medium when checked by the computer platform, are also satisfied by the computer platform when checked by the recording medium.

Thus, the boot software checks the following in particular:

• that the hardware security device is properly installed;

• that the basic software of the computer platform has indeed been curbed;

• that the identity parameter specific to the ~~medium~~ method and recorded in the security hardware device does indeed correspond with that which is recorded on the recording medium; and

• that the authentication parameter for the contents of the recording medium corresponds to that which has likewise been recorded on the recording medium.

Once all of those checks have been performed, it can be said that the computer platform is certain that it is accessing and using a recording medium that complies with the medium that was produced, and conversely that the recording medium is certain that it is being used by a computer platform that is properly secure and by a user who is properly authorized, and that it is being used within the rights that have been acquired by the user.

Under such conditions, the operating system can be loaded from the recording medium. Nevertheless, since the operating system is independent from the operating system of the computer platform, particularly when the computer platform is of "open" architecture, it may be necessary to make use of configuration software which is read from the recording medium. The general function of this configuration software is to store in the hardware security device all of the parameters that are necessary and sufficient to enable the operating system for the data and/or applications as stored on the recording medium can be executed by the operating software of the computer platform.

The operating software can ~~then~~ therefore be loaded ~~into the computer platform~~ from the recording medium to enable the user to make use of the data and/or applications, ~~stored on the recording medium, where the user is authorized to access them, and this can be done~~ in complete security

not only for the user but also for the publisher of recording media.

During such use, security is ensured by the operating software that has been loaded from the recording medium, or by the applications themselves, and for this purpose, reliance is made on the above-mentioned interface that is installed by the hardware security device and the associated software at the end of the first stage of the boot process.

To reinforce the security of the method, it is preferable for the operating system for the data and/or applications to comply also with the security functions that applied during the boot stage, for example by preventing initialization of software that has not been previously checked or by preventing access to a peripheral that is not provided for by the method.

~~Thus, in order to implement the method of the~~ invention, the user's computer platform must be made secure, and the user must have available not only the recording medium on which there are recorded at least the data and/or applications to which the user seeks access, together with the operating software for said data and/or applications, but must also have available a memory card defining, in particular, conditions for accessing the ~~recording medium~~.

CLAIMS

1/ A method of making secure and monitoring access to information from a computer platform having a microcomputer, the method being characterized in that it consists:

• in producing at least one non-rewritable recording medium on which information such as data and/or applications (in a predetermined logic format) is recorded, together with operating software for said information;

• in defining authorized users having access rights to the information stored on the recording medium together with possible limits on such access rights, ~~and issuing each user with a portable medium of the smart card type on which information concerning the assigned rights is recorded;~~

• ~~in inserting a recording medium and a portable medium in readers fitted to the computer platform;~~

• in configuring or transforming the computer platform of an authorized user into a secure workstation to prevent any hardware and/or software intrusion seeking to gain undue access to the information or to make use thereof instead of an authorized user and without that user's agreement, ~~said transformation stage consisting in causing the computer platform to execute security functions on the basis of parameters recorded on the recording medium, the portable medium, and the computer platform;~~

• in loading the operating software from the recording medium ~~into the computer platform~~, once all of ~~the security functions have been satisfied;~~

• in enabling the information stored on the recording medium to be used within the limits of the rights acquired by the authorized user; and

• during said use, in being able to exchange and/or communicate in secure manner data with a network to which the computer platform is connected.

, said operating software being read by an appropriate reader of the computer platform ;

2/ A method according to claim 1, characterized in that the stage of producing a non-rewritable recording medium consists in defining the information to be protected, the operating system for said information, a set of check parameters to enable the operating software loaded from the recording medium to operate, and a set of security parameters for making use of the recording medium secure, and for enabling the information stored on said medium to be used. ~~And in recording all said information in a predetermined software format on the recording medium.~~

3/ A method according to claim 2, characterized in that ~~to make use of the recording medium secure,~~ it consists in defining security parameters such as an identity parameter specific to the ~~recording medium~~ method and an authentication parameter for authenticating the contents of the recording medium, in the form of an encrypted signature, ~~for example~~ to make use of the medium secure.

4/ A method according to claim 2 or 3, characterized in that ~~in order to make use of the recording medium,~~ it consists in defining security parameters such as a parameter concerning the security level required ~~to access the information of the recording medium,~~ and a parameter specific to ~~said information,~~ the data and/or applications in order to make use of the recording medium.

5/ A method according to any one of claims 2 to 4, characterized in that it consists in encoding or encrypting all or part of the information ~~on the recording medium~~, and also in storing on the recording medium a security table containing decoding algorithms in encrypted form.

~~6/ A method according to claim 5, characterized in that~~ it consists in recording on the ~~portable~~ medium keys for decoding or ~~decrypting~~ the information stored on the ~~recording medium.~~

7~~/ A method according to any preceding claim~~, characterized in that it consists in recording on the portable medium of ~~each~~ user parameters such as the security level required to use the information on the recording medium, and the identity of ~~said~~ information, ~~these two parameters corresponding to those recorded on the recording medium~~.

6 2 to 5

8~~/~~ A method according to any preceding claim~~,~~ characterized in that the stage of configuring or transforming a computer platform into a secure workstation consists~~x~~

- in integrating in said platform a hardware security device and associated ~~checking~~ software~~x~~

~~- in recording on the hardware security device the identity parameter specific to the recording medium, and the identity parameter of the information of the recording medium, and~~

- ~~in causing the checking software to identify~~ the identity parameter specific to the recording medium by comparing corresponding parameters recorded on the recording medium and the hardware security device, the identity parameter of the information on the recording medium by comparing the corresponding parameters recorded on the recording medium and the hardware security device, and the level required to use the information by comparing the corresponding parameters on the recording medium and on the portable device, to ensure that the recording medium does indeed comply with the medium that ~~was produced~~.

⟹ claim 7 (see the dactylographied translation).

8 9~~/~~ A method according to any preceding claim, characterized in that, prior to loading the operating software from the recording medium, it consists in verifying from boot software loaded from the recording medium, that the security conditions which have been

to prevent any hardware and/or software intrusion in order to implement security functions on the basis of the above-mentioned parameters.

satisfied by said medium when monitored by the computer platform are also satisfied by the platform when monitored by said medium.

9 8
10/ A method according to ~~any preceding~~ claim, characterized in that it consists in making the operating system stored on the recording medium independent from the operating system of the computer platform, and in loading, where necessary, configuration software from said recording medium to provide the parameters required for executing the operating system stored on said medium.

10
11/ A method according to any preceding claim, characterized in that, after the operating system has been loaded from the recording medium, it consists in causing said system to execute security functions relating both to the recording medium and to the computer platform, in order to reinforce the security for implementing the method.