(12) UK Patent Application (19) GB (11) 2 358 946 (13) A

(43) Date of A Publication 08.08.2001

(21) Application No 0002152.7

(22) Date of Filing 01.02.2000

(71) Applicant(s)
Ravinder S Dosanjh
11 Sherdmore Croft, Monkspath, SOLIHULL, West Midlands, B90 4TX, United Kingdom

(72) Inventor(s)
Ravinder S Dosanjh

(74) Agent and/or Address for Service
Ravinder S Dosanjh
11 Sherdmore Croft, Monkspath, SOLIHULL, West Midlands, B90 4TX, United Kingdom

(51) INT CL[7]
G08B 13/14 25/00 , H04M 11/04

(52) UK CL (Edition S)
G4H HNHE H1A H13D H13F H14A H14D
H4K KOB
U1S S2106 S2125 S2188 S2206 S2212

(56) Documents Cited

GB 2328303 A	**GB 2321124 A**	**GB 2310065 A**
GB 2268818 A	**GB 2262372 A**	**GB 2233485 A**
EP 0852367 A2	**EP 0652542 A1**	**WO 96/03728 A1**

(58) Field of Search
UK CL (Edition R) **G4H HNEE HNHE , H4K KOB**
INT CL[7] **G08B , H04M**

(54) Abstract Title
Combating theft of computer equipment and software piracy

(57) A computer hardware or peripheral device having automatic signal generating means which is operative to send a signal from the device to a predetermined destination or to one of a plurality of predetermined destinations, via a communications link to which the device is operatively connected, or via a power transmission pathway, e.g. to locate equipment or software to combat theft of hardware or software piracy.

GB 2 358 946 A

Title: Computer Hardware or Peripheral Device, System for Combating Computer Software Piracy and System for Combating Theft of Portable Computers

Description of Invention

This invention relates in its broadest aspect to a computer hardware or peripheral device, but also relates to a system for combating computer software piracy and a system for combating theft of portable computers.

Most businesses and many households today are equipped with a variety of computer-based equipment, and a large proportion of these businesses and households are connected to a variety of information networks such as the Internet, Intranets, and electronic mail messaging systems.

Bearing in mind the relatively high intrinsic value of computer hardware and the associated software packages, theft of such goods has become a considerable problem over recent years, which results not only in financial loss to the owner insofar as the hardware is concerned, but also may often result in a significant loss of information which was stored on the equipment concerned.

In addition, such theft can often have the effect of releasing confidential information stored on the equipment into the public domain, and whilst many proposals have been put forward in an attempt to combat this problem, none has proved to be especially successful.

In particular, existing security systems concentrate, in general, on mechanical devices which secure the equipment in position, thus making it difficult to remove, and a variety of "post-theft" systems such as ultraviolet marking, the purpose of which is to enable stolen equipment, if found, to be reunited with its owner.

However, whilst it is theoretically possible to "tag" computer equipment with sophisticated tracking devices, such as those which, for example, are used

to locate stolen motor vehicles, this is rarely practical, and the cost is often prohibitive.

It is therefore a primary object of the present invention to provide a computer hardware or peripheral device which is effective to overcome or at least reduce this problem. Further objects of the present invention are to provide a system for combating computer software piracy and to provide a system for combating theft of portable computers, as detailed below.

According to a first aspect of the present invention I provide a computer hardware or peripheral device having automatic signal generating means, which is operative to send a signal from the device to a predetermined destination or to one of a plurality of predetermined destinations, via a communications link to which the device is operatively connected, or via a power transmission pathway.

The automatic signal generating means may be operative to send the signal on or shortly after application of power of the device. Alternatively, the automatic signal generating means may be operative to send the signal as soon as, or shortly after, a communications link is established.

In a preferred embodiment, the predetermined destination corresponds to address information about the location at which the device will normally be used, which, it will be appreciated, may be input into or stored on the device by a user.

Desirably, the signal is sent via a telephonic communications link, such that the source of the signal may be determined by identification of the telephone line. In a preferred embodiment, the signal is telephonic.

The device may further comprise signal response detector means, which on detection of a particular response to the signal, is operative to send a further signal to a further predetermined destination or to one of a plurality of further predetermined destinations.

In particular, the signal response detector means may be adapted to distinguish between at least ringing and non-ringing responses, such that upon detection of a ringing response, the further signal is caused to be sent.

It will be appreciated that detection of a ringing telephonic response indicates that the computer hardware or peripheral device is not located at the location at which the device is normally used, thus indicating that the device may have been stolen.

Upon detection of a ringing response, which, as indicated above, indicates that the device may have been stolen, the further signal may be sent to a monitoring station, with the further signal being operative to identify the device to the monitoring station. Such identification may include, for example, the make, product and serial number of the device concerned.

In a preferred embodiment, the further signal is also operative to identify to the monitoring station the location of the device, for example by reference to the telephone number of the line to which the device is connected at that time, or other location information, such as Global Positioning System (GPS) data.

The monitoring station may be provided with data storage means, such as an electronic database, which is operative to log some or all such further signals so that the use made of a particular device may be monitored.

In this way, an apparently stolen device may be "tracked".

In a particularly desirable embodiment, the device may further comprise shut down means which is operative, on detection by the signal response detector means of a ringing response, to shut down or disable the device. Shut down may also be effected by a shut down signal from the monitoring station.

The monitoring station may comprise control means which is operative to send a control signal to the device. The control signal may cause the device to perform tasks, such as the deletion of software or the downloading of data to the monitoring station, for example. The control means may also be operative to send software to the device, for subsequent execution on the device.

The device may be adapted to remain shut down or disabled until an appropriate release means is applied, which may take the form of a mechanical release element such as a key or, for example, a particular software package or piece of machine code or software routine. Alternatively, a password may be input to the device, or the control means may be configured to effect the release, by sending appropriate data to the device.

Whilst the signals may preferably be sent via a standard communications link to which the device is operatively connected, such as a telephonic (PSN) link, or, for example, an ISDN link, it is also envisaged by the applicant that the signals could be sent via the mains electricity supply pathways, on the assumption that suitable (e.g. digital) anti-interference measures are taken.

Alternatively or in addition, it is envisaged that the location information could be sent in the form of an electronic mail message, or any other such electronic message delivery system.

It will also be appreciated by those skilled in the art that whilst the device itself may be operative to provide the location information to the monitoring station, it is also quite possible that the monitoring station could be provided with means to trace the source of the incoming signal, thus enabling the location of the apparently stolen device to be identified.

Insofar as the automatic signal generating means and the signal response detector means are concerned, it is envisaged that these may be "built into" the device's hardware, or provided by appropriate firmware inherently supplied with the hardware or by software which may be loaded onto the hardware via computer media such as one or more CD-ROMs, discs or magnetic tape or downloaded, for example, from the Internet.

Thus, the invention also relates to a computer software or firmware package which enables a computer hardware or peripheral device to be operated in the manner described in relation to the first aspect of the present invention.

In accordance with the second aspect of the present invention, I provide a computer hardware or peripheral device having signal generating means which is operative to send a signal from the device to a monitoring station via a communications link to which the device is operatively connected or via a power transmission pathway, wherein the sending of the signal is operative to enable the location of the origin of the signal to be identified to the monitoring station and to identify to the monitoring station at least one piece of software which is loaded or stored on the device.

Preferably, the signal is operative to identify to the monitoring station a serial number or other such identifier of the piece of software. The signal may also be operative to identify the device to the monitoring station.

The signal generating means may be operative to send the signal on or shortly after application of power to the device.

In this way, it will be appreciated that the use of individual software packages may be monitored at the monitoring station.

The signal may also be operative to identify the device itself. Thus, the use of specific software packages on particular devices may be monitored. The device may be identified by its serial number, or by technical data such as its memory capacity, its manufacturer and the CPU, for example.

The present invention thus also provides a system for combating computer software piracy comprising a plurality of computer hardware or peripheral devices substantially in accordance with the second aspect of the present invention, a monitoring station with which the devices may communicate, the monitoring station being provided with detector means operative to detect signals from different locations which identify particular pieces of software.

In this way, the use of copied software may be detected, with the system thus providing an effective anti-piracy method.

Preferably, the monitoring station, on receipt of a signal identifying that a particular piece of software is not at a registered location, or not being used with a licensed device, is operative to send a shut down signal to the device from which the signal was sent, so as to shut down or disable the device.

The detector means may be operative to detect signals from different locations but which identify the same piece of software. In such a case, the monitoring station, on receipt of at least two such signals , is operative to send a shut down signal to at least one of the devices from which the signal was sent.

The monitoring station may comprise control means substantially as described in relation to the first aspect of the present invention.

According to a third aspect of the present invention I provide a system for combating theft of a portable computer comprising

(a) programming into a computer details of the location where the computer will normally be used,

(b) causing the computer to compare, during use thereof, the programmed details with details of its actual location,

(c) causing the computer, in the event of a discrepancy between said details, to send a signal to a monitoring station, the signal identifying to the monitoring station the location and identity of the computer, and

(d) causing the monitoring station to check the identity details against a list or database of details of stolen computers.

Preferably, the details of the location of the computer are provided by a telephone number of a line to which the computer is in use connected. However, other information such as GPS data may be provided.

The signal may be sent as soon as the discrepancy is detected, or after a specified number of further uses of the computer.

The various aspects of the present invention will now be described in greater detail.

Insofar as the first aspect of the present invention is concerned, the computer hardware or peripheral device to be protected is provided with automatic signal generating means, in the form of a piece of computer software, as may be provided on a CD-ROM or downloaded from the Internet. The automatic signal generating means thus provided is operative to send a telephonic signal, on or shortly after application of power to the device, the signal being sent to a predetermined destination corresponding to address information relating to the location at which the device will normally be used, with this information having previously being input to the device by its user.

Signal response detector means, also provided with the device, is adapted to distinguish between at least ringing and non-ringing responses, with a further signal being sent from the device upon detection of a ringing response.

It will be appreciated that if the device is being used at its normal location (i.e. the device has not been stolen) a non-ringing response will be detected, typically in the form of an engaged tone. If, on the other hand, the device is not being used at its normal location, it is likely that a ringing response will be detected, thus indicating that the device may have been stolen. Should this occur, a further signal is sent to a monitoring station, the further signal being operative to identify the device (for example its make, the type of product and its serial number) and its location to the monitoring station. From this, the stolen device may be retrieved, with the identity and location information conveniently first being passed to the police.

The second aspect of the present invention provides a system for combating computer software piracy, and operates in a somewhat similar manner to the first aspect of the invention, in that the computer hardware or peripheral device concerned generates and sends a signal to a monitoring station, and wherein sending of this signal enables the location of the origin of the signal to be identified and identifies to the monitoring station a serial

number or other such identifier of at least one piece of software which is loaded or stored on the device.

In this way, the use of individual software packages may be monitored at the monitoring station. Moreover, by connecting a plurality of such devices to a monitoring station, it is possible to detect the use of copied software, by detection of incoming signals identifying the same piece of software, but where the signals have different sources.

Insofar as the third aspect of the present invention is concerned, a user, wishing to protect a portable computer, first programs into the computer details of the telephone number of the line to which the computer will normally be connected, such that the computer, during use, may compare these programmed details with details of its actual location. In the event of a discrepancy between the programmed and actual details, a signal is sent from the computer to a monitoring station to identify the location and identity of the computer to the monitoring station, and the monitoring station then checks the identity details against a list or database of details of stolen computers.

It will be appreciated that the term "computer" is meant to include a variety of items which incorporate a microprocessor. Such items comprise digital televisions, video recorders and satellite decoders, for example, each of which is connected to a communications link.

In the present specification "comprise" means "includes or consists of" and "comprising" means "including or consisting of".

The features disclosed in the foregoing description, or the following claims, or the accompanying drawings, expressed in their specific forms or in terms of a means for performing the disclosed function, or a method or process for attaining the disclosed result, as appropriate, may, separately, or in any combination of such features, be utilised for realising the invention in diverse forms thereof.

CLAIMS:

1. A computer hardware or peripheral device having automatic signal generating means which is operative to send a signal from the device to a predetermined destination or to one of a plurality of predetermined destinations, via a communications link to which the device is operatively connected, or via a power transmission pathway.

2. A computer hardware or peripheral device according to claim 1 wherein the automatic signal generating means is operative to send the signal on or shortly after application of power to the device, or as soon as, or shortly after, a communications link is established.

3. A computer hardware or peripheral device according to claim 1 or claims 2 wherein the predetermined destination corresponds to address information about a location at which the device will normally be used.

4. A computer hardware or peripheral device according to claim 2 or claim 3 further comprising signal response detector means which, on detection of a particular response to the signal, is operative to send a further signal to a further predetermined destination or to one of a plurality of further predetermined destinations.

5. A computer hardware or peripheral device according to claim 3 or claim 4 wherein the automatic signal generating means is operative to send a telephonic signal and wherein the signal response detector means is adapted to distinguish between at least ringing and non-ringing responses.

6. A computer hardware or peripheral device according to claim 5 wherein detection of a ringing response causes the further signal to be sent.

7. A computer hardware or peripheral device according to claim 6 wherein the further signal is sent to a monitoring station, and wherein the further signal is operative to identify the device to the monitoring station.

8. A computer hardware or peripheral device according to claim 7 wherein the further signal is operative to identify to the monitoring station the location of the device.

9. A computer hardware or peripheral device according to claim 6, claim 7 or claim 8 wherein the device further comprises shut down means which is operative, on detection by the signal response detector means of a ringing response, to shut down or disable the device.

10. A computer hardware or peripheral device having signal generating means which is operative to send a signal from the device to a monitoring station via a communications link to which the device is operatively connected or via a power transmission pathway, wherein sending of the signal is operative to enable the location of the origin of the signal to be identified to the monitoring station and to identify to the monitoring station at least one piece of software which is loaded or stored on the device.

11. A computer hardware or peripheral device according to claim 10 wherein the signal is operative to identify to the monitoring station a serial number or other such identifier of the piece of software.

12. A computer hardware or peripheral device according to claim 10 or claim 11 wherein the signal generating means is operative to send the signal on or shortly after application of power to the device.

13. A system for combating computer software piracy comprising a plurality of computer hardware or peripheral devices according to claim 10, claim 11 or claim 12, further comprising a monitoring station with which the devices may communicate, the monitoring station being provided with detector means operative to detect signals from different locations which identify particular pieces of software.

14. A system according to claim 13 wherein the monitoring station, on receipt of a signal identifying that a particular piece of software is not at a registered location, is operative to send a shut down signal to the device from which the signal was sent, so as to shut down or disable the device.

15. A system for combating theft of a portable computer comprising:

(a) programming into a computer details of the location where the computer will normally be used,

(b) causing the computer to compare, during use thereof, the programmed details with details of its actual location,

(c) causing the computer, in the event of a discrepancy between said details, to send a signal to a monitoring station, the signal identifying to the monitoring station the location and identity of the computer, and

(d) causing the monitoring station to check the identity details against a list or database of details of stolen computers.

16. A system according to claim 15 wherein the details of the location of the computer are provided by a telephone number of a line to which the computer is in use connected.

17. Any novel feature or novel combination of features described herein.

The Patent Office
COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

13.

Application No: GB 0002152.7 **Examiner:** Mike Davis
Claims searched: 1-9 **Date of search:** 12 April 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): G4H (HNHE, HNEE), H4K (KOB)

Int Cl (Ed.7): G08B, H04M

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2328303 A	(DASHCROWN)	1 at least
X	GB 2321124 A	(NORSK DATA)	"
X	GB 2310065 A	(CASTELL ET AL)	"
X	GB 2268818 A	(HARTBROOK...)	"
X	GB 2262372 A	(BACHE)	"
X	GB 2233485 A	(MOORE)	"
X	EP 0852367 A2	(SIEMENS...)	"
X	EP 0652542 A1	(NEDAP)	"
X	WO 96/03728 A1	(KANG)	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.