

WIRELESS SECURITY SYSTEM FOR COMPUTER WORKSTATIONS

Field of the Invention

[0001] The present invention relates to a security device and security measures against unauthorized access to computers.

[0002] In particular, this invention relates to a mobile wireless device acting as an authorization means to allow a user access to a computer. The computer will also effect one or more desired predetermined security features when the user brings the mobile wireless device out of range of the computer's own wireless device.

Background of the Invention

[0003] Information security is an important concern, not only for governments and military forces, but also for other organizations such as commercial entities. Access to information, particular information held in computers and computing devices, must be controlled in order for organizations to protect their proprietary information.

[0004] One way by which unauthorized access to a computer may occur is when a user leaves the computer unattended, potentially allowing non-authorized persons in the vicinity to access the computer. A common and simple way by which unauthorized access under such circumstances is prevented is by use of a screensaver program with a password requirement. Another commonly used method is the use of a workstation lock.

[0005] Screensaver programs are utility programs usually provided free by computer vendors or at low cost. After a predetermined time of inactivity (usually the duration a keyboard or pointer device is not used), the screensaver program will activate and replace the information displayed on

the computer monitor with another picture or display graphic to hide or mask the original display.

[0006] While the original intention of screensaver program was to prevent frequently used pixels of the monitor's screen from burning out prematurely, screensavers were also found to be useful as a simple security feature. Together with the activation of the screensaver graphic, an option may be selected whereby a password must be entered before the monitor screen reverts to the original display.

[0007] While this may seem as an elegant solution to guard against unauthorized access, in reality, the automatic activation of the screensaver display after a fixed duration has several disadvantages. Firstly, if the duration of inactivity is set at too short a length of time, the screensaver display may activate while the user is mulling over a thought or making a telephone call and while still seated at the computer. This is annoying when it happens and the user has to type in the password many times throughout the workday.

[0008] If the duration of inactivity is set at too long an interval, another person may be able to access the computer while the user is otherwise occupied away from the computer.

[0009] Another way to protect access to a computer is for the user to consciously activate a workstation lock on the computer by pressing a sequence of keystrokes. However, the disadvantage now lies with the user. Over time, most users will tire of having to activate the lock each and every time they are away from the computer. Alternatively, if the user is in a rush, they may forget to activate the workstation lock.

[0010] These disadvantages are clearly present and known in the industry as evidenced by several patents or patent applications for inventions to overcome these disadvantages. The principle of action of these inventions is the same – to sense the presence (or rather, the absence) of a user and then to enable a suitable security measure such as the screensaver program, when the user leaves the computer. The differences between

these inventions lie in the means to determine the presence of the user at the computer.

[0011] For example, Klein has two inventions to this objective: one a method for automatically initiating a computer security mode and/or screen saver mode (US 6,401,209 B1) as well as a system for practicing it (US PTO Publication No 2002/0099960 A1). Klein's invention uses dedicated proximity sensors based on ultrasound, or infrared or other electromagnetic means to detect the proximity of a user.

[0012] The user proximity sensor taught by another invention (Lignoul, US Publication No 2002/0095222 A1) encompasses sensors making use of passive infra-red, reflectance and diffuse reflectance, light beam continuity, capacitance, radio frequency, sound and ultrasound, as well as pressure and weight. These dedicated sensors may also be used in combination to form a "multidimensional sensor". All this dedicated equipment setup to just to detect the presence of a user at a computer.

[0013] The inventions above are aimed primarily at preventing the activation of a computer security measure such as a password-required screensaver program. The invention by Lignoul also has the capability of authenticating the identity of the user for access to the computer.

[0014] These inventions clearly support the idea that a need exists for a system and method for secure access to a computer or computer system by an authorized user. This need should be achieved without unduly burdening the user to have to take tedious measures to conscientiously activate the security measures while away from the computer. At the same time, these measures should not activate while the user is still at the computer. Ideally, solutions should be simple, personal to the user, multifunctional and inexpensive to implement while remaining sufficiently robust against inadvertent breaches of security.

[0015] The present invention seeks to achieve the same objectives as the prior art but at minimal cost to the user.

Summary of the Invention

[0016] The present invention seeks to provide means by which the existing security measures for access to computers may be easily implemented, supplemented or enhanced.

[0017] Accordingly, in one aspect, the present invention provides a simple method to control computer access wherein a personal, multifunctional wireless device that communicates with the user's compatible computer is used to authenticate as well as indicate the user's presence, hence permitting the user to access the computer.

[0018] According to this first aspect, the present system thus provides: a method of controlling access to a computer; the method comprising installing, in the computer, a wireless device and a control program; equipping at least one mobile device with a unique identity code and a compatible wireless communicator, said at least one mobile device is carried by user; enabling wireless communication between the at least one mobile device and the computer; registering, in a list, at least one authorized user based on the unique identity code of the at least one mobile device according to predetermined rules and access policies; permitting user access by the control program to the computer, when the unique identity code of the at least one mobile device with a compatible wireless communicator is found in the list of authorized users in the computer and is within range of the wireless device;

[0019] and not permitting access when the at least one mobile device with a unique identity code is not found in the list of authorized users or is out of range of the wireless device.

[0020] In another aspect, the present invention provides a system by which the present invention may be practiced, the system comprising:

a computer equipped with a wireless device;
at least one mobile device with a unique identity code and equipped with a compatible wireless communicator; and a control program operable to authenticate the unique identity code of the at least one mobile device

against a list of authorized identity codes stored in the computer for controlling the security system, wherein the computer program permits a user access to the computer after the control program has authenticated the at least one mobile device as an authorized device and when the mobile device's compatible wireless communicator is within operating range of the computer's wireless device.

Brief Description of the Drawings

[0021] Two preferred embodiments of the present invention will now be more fully described, by way of example, with reference to the drawings of which:

[0022] FIG. 1 is a diagram of a computer security system of one embodiment of the present invention based on the Bluetooth wireless communication standard;

[0023] FIG. 2 is the flowchart for the control program for the control program resident in the computer for the Bluetooth embodiment of the present invention.

[0024] FIG. 3 is the diagram of a computer security system of another embodiment of the present invention based on the IrDA wireless communication standard using a mobile phone or a personal digital assistant ; and

[0025] FIG. 4A is the control flowchart for an IrDA-capable mobile wireless device, to enable the practice of the present invention. FIG. 4B is the flowchart for the control program resident in the computer for the IrDA embodiment of the present invention.

Detailed Description of the Drawings

[0026] A detailed description of the present invention will now be given in accordance with two preferred embodiments of the invention. In the

following description, details are provided to describe the preferred embodiments. It shall be apparent to one skilled in the art, however, that the invention may be practiced without such details. Some of these details may not be described at length so as not to obscure the invention.

[0027] There are many advantages of the preferred embodiments of the invention. One advantage of the preferred embodiments is that a user will be "permitted" by the present invention to access the computer as long as he is carrying his personal mobile wireless device on his person. The user can rest assured knowing that when he moves away from his computer, the present invention will enable a security measure so as not to permit other unauthorized users to access the computer.

[0028] In brief, the user has, on his person, a personal multifunctional mobile wireless device with a unique identity code or number. This device is assigned to him in a way whereby the device acts as a means or another form of identification, authenticating the user to the computer system or to other security system. That is, records are kept on the user and the device assigned to him.

[0029] The mobile wireless device can be a mobile phone, a personal digital assistant (PDA) computer equipped with a wireless communicator, or a notebook computer equipped with a wireless communicator. The mobile phone has its own unique identification number and built-in wireless capability. To provide a wireless capability to PDAs or computers that do not have their own built-in wireless capability, a wireless communicator peripheral, such as a plug-in card, with its own unique identification number, can be used.

[0030] The intention and object of the present invention is to provide a simple solution to the problems of the prior art stated above, by means of a personal multifunction device that is carried by a user and the user alone. In contrast to the prior art, the means to authenticate the user and to determine his proximity to the computer is carried by the user himself and is not dependent on hardware at or around the computer to be accessed.

Also, in contrast with the prior art, a multifunction personal device is used, instead of dedicated equipment.

[0031] FIG.1 is a functional block diagram of one embodiment of the present invention in which the mobile wireless device is a Bluetooth-equipped mobile telephone **110**. In this first embodiment, the presence of the user's Bluetooth mobile telephone authenticates the user as an authorized user, may be permitted access to the computer. In accordance with the present invention, the mobile device also indicates the proximity of the user to his computer or to another computer to which he is permitted access.

[0032] The user's computer **120**, which is also equipped to transmit and receive signals according to the Bluetooth standard, communicates with the user's mobile telephone. The computer is able to do so by having with a wireless Bluetooth device, either installed internally or connected as an external device **122**, through a suitable communications port, such as a Universal Serial Bus (USB) port. Alternatively, internal installation of the computer's Bluetooth wireless device and fastening of the computer casing with tamper-proof fasteners is possible and preferred to prevent tampering of this security feature.

[0033] The methods and means by which Bluetooth devices communicate are well known to persons skilled in the art and only a brief description is included here.

[0034] Bluetooth is a radio frequency standard related the IEEE 802.15 specification. Bluetooth was developed for short-range wireless communication between compatible electronic devices. First introduced as a replacement for cables connecting computers and their peripheral devices such as printers, Bluetooth has now found applications in mobile telephones, pagers, headsets and modems as well.

[0035] Bluetooth operates in the 2.4GHz Industrial-Scientific-Medical (ISM) frequency band and can support up to eight devices in its own tiny network (a "piconet"). Its transmission **112** is actually omni-directional **114** and does not require a line-of-sight view with the other devices it is communicating

with. Bluetooth transmissions have a range of up to 10 m and can penetrate solid objects such as walls.

[0036] To ensure reliability of communication in “noisy” environments, Bluetooth devices utilize frequency hopping to minimize the effects of interfering signals.

[0037] Bluetooth devices are designed to connect to each other seamlessly, without any input from the user. Bluetooth devices are also designed to communicate only with compatible devices. For example, a Bluetooth headset will communicate with a Bluetooth mobile telephone and a Bluetooth printer will communicate with a Bluetooth computer.

[0038] To make a connection with another Bluetooth device, a first device continually sends out an inquiry signal to determine if any other Bluetooth devices are in the vicinity and within range. These other Bluetooth devices are usually in an inquiry scan state. When queried with an inquiry from the first device, the second device will respond with an inquiry response which contains information regarding itself, including its unique device identity code. The response messages are collected by the first device. Once a connection is established, the first device will become the “master” unit. The two Bluetooth devices then form a piconet and exchange of information and control data can begin.

[0039] In this embodiment of the present invention, a Bluetooth-capable mobile telephone, personal to a user, communicates with computer similarly equipped with a wireless Bluetooth device. The Bluetooth-capable mobile telephone acts as an authorization means for the user to access and use the computer

[0040] When the user moves away from the computer, the Bluetooth-equipped mobile telephone on his person will continue to communicate with the computer until it is brought out of range; the nominal maximum range for Bluetooth devices is 10 m. When this happens, the computer will effect a predetermined security measure, such as enabling the workstation lock or password-protected screensaver program.

[0041] Unlike conventional communication between two Bluetooth devices, the two devices (mobile telephone and computer) of this particular embodiment of the present invention do not form a piconet. No higher level of communication other than the transmission of the inquiry by the computer and the return of an inquiry response by the mobile telephone is performed. Neither is a higher level of Bluetooth communication needed in this embodiment of the present invention.

[0042] When the computer (acting as the master unit) receives the mobile telephone's (slave unit's) response, a control program, an element of the present invention, compares the unique identity code returned by the mobile telephone with an internal list of authorized addresses. If the internal list used by the control program does not contain the mobile telephone's unique identity code, access to the computer is not permitted by the activation of a predetermined security measure. This breach of security may also be logged by the control program; other security measures such as notification of the network administrator, may also be effected.

[0043] If the unique identity code returned by the mobile telephone is on the internal list of authorized users, access is permitted.

[0044] This cycle of sending, receiving and checking inquiry messages is repeated until the computer is shut down or control program is terminated. Thus, with the present invention, a desired security measure such as locking the computer or activating the screensaver when the user is away from the computer can be automatically performed without requiring further intervention by the user.

[0045] FIG. 2 summarizes the method of the control program of present invention for the Bluetooth embodiment. Upon installation in a standalone computer or computer server, the control program initializes the Bluetooth function **210** to run "on top" of the computer's operating system.

[0046] The user can then opt to manually lock **212** the system or start registering authorized users by registering the unique identity codes for their wireless devices. This may be done manually, by keying in the names

and identification codes into the internal list. Alternatively, registration may be done by bringing these authorized wireless devices, in turn, proximal to the computer and allow the control program to utilize the Bluetooth function to begin finding and communicating with them. The control program will locate **214** Bluetooth devices in the vicinity by sending out inquiries **216** and then collecting responses **218** containing the unique identity codes of devices in the vicinity.

[0047] The control program will then compare these unique identity codes with those in its internal list **220**. If the unique identity of a device is not found on the internal list, the administrator may choose to register it or allow the control program may register it **222** as an authorized user according to predetermined rules and access policies.

[0048] After users have been registered, the user or administrator can then cause the computer to “sniff” for other Bluetooth devices **224**. This “sniffing” is not the same “sniffing” as that native in the Bluetooth specification but is one effected, at a higher level, by the control program.

[0049] For this function, the control program activates a sniffing timer **226** that sends out inquiry messages **228** periodically, say every 12 seconds. The responses **230** from any compatible Bluetooth devices in range are collected and the unique identification codes are checked **232** against the list of authorized users in the internal list.

[0050] If the current user’s unique identity code is in the internal list, access to the computer or workstation is permitted. If the authorized unique identity code ceases to be received, say in the situation of the wireless device moving out of range, the operating system will effect a predetermined security measure **234**. These predetermined security measures can include application of a workstation lock or password-protected screensaver program.

[0051] This embodiment of the present invention may initially be confused with another invention, Bluetooth Based Security System, by Sundeep (US 2002/0194500 A1) but the differences are clear. Sundeep’s invention uses a wireless system, preferably Bluetooth, to prevent the physical loss of

small high-value electronic devices such as notebook and laptop computers from a location protected by the invention.

[0052] In contrast, the present invention is aimed at using personal multifunction wireless communication devices such as mobile phones to permit access to a computer system and to prevent such access when the device is out of range of the computer's own wireless device.

[0053] While the present invention can be implemented with Bluetooth-equipped mobile devices and computers, another embodiment of the present invention is the use of infrared wireless devices (FIG. 3) instead of Bluetooth devices.

[0054] Infrared wireless communication devices, such as those adhering to the Infrared Data Association (IrDA) standards may be used. IrDA devices have several advantages over Bluetooth devices. IrDA communications is a line of sight, point to point transmission at a narrow 30-degree angle. It also has a much shorter range of up to 1 m compared to Bluetooth. Bluetooth's long, omni-directional transmission may render it more vulnerable to unintentional interference with other Bluetooth devices, causing data packets to be dropped.

[0055] With its more directional transmission, a mobile device equipped for IrDA communications such as a mobile telephone **30** or Personal Digital Assistant (PDA) **32** can be used as by a user to authenticate his identity and to indicate his proximity to a similarly-equipped computer **36**.

[0056] At present, many mobile phones, PDAs and notebook computers are equipped with built-in IrDA communication ports for the exchange of data such as contact information, screen graphics or games, between compatible IrDA devices.

[0057] The directional nature of IrDA transmissions itself is a low-level form of security as the user has to place his the IrDA port **302** (or **322**) of his personal mobile device within the 1 m range computer's IrDA port **362**. The two ports also must face each other within the narrow cones **304** and **324** of infrared transmission.

[0058] While directionality and short-range are characteristics of IrDA devices, an Israeli company, Infra-Com, has claimed a non-directional infrared system where "the infrared radiation is transmitted by one of the units in a manner generally insensitive to the position of the other unit" (Ruziak, WO0136233A1). Such systems may also be conceivably incorporated into the present invention.

[0059] As with the Bluetooth embodiment of the present invention, the control program will compare the unique identity code of the IrDA mobile device against an internal list of approved user identities. However, a person skilled in the art will appreciate that, as the IrDA standard does not provide any native or inherent form of security such as encryption of the transmitted data, authentication and encryption. As such, the possession of the unique identity code must be performed by higher level protocols and applications such as the control program.

[0060] For the IrDA embodiment of the present invention, a circumstance analogous to that of the Bluetooth embodiment's out of range situation will happen when the infrared communication between the mobile device and the computer is broken. This may happen either by the cessation of transmission by the mobile device or by a change in the relative positions of the two devices such that one device cannot receive the transmission of the other device.

[0061] When this happens, the predetermined security measure is activated to not permit access to the computer.

[0062] To practise this IrDA embodiment of the present embodiment, the mobile device's own operating system must be modified to transmit a unique identity code. For the case of a mobile phone, this code can be the phone's own International Mobile Equipment Identifier (IMEI).

[0063] After the IrDA wireless device's operating system has been modified and the control program loaded into the computer, the administrator can begin to register the list of approved users by keying in the names of the authorized users together with their unique identification codes. Alternatively, he can face the infrared ports of the IrDA devices he wants

registered towards the infrared port of the computer. He then activates the control program given in FIGS. 4A and B, with the first part of the control program illustrated in FIG. 4A, in the computer to automatically register the wireless devices.

[0064] The computer does this by opening an infrared communications port **420** to emulate a serial port for the computer. Again, like that for the Bluetooth control program, the user can choose to manually lock the computer **422** or start looking for a first compatible infrared transmission **424**.

[0065] The control program does this by reading the emulated serial port **426** and waits for the transmission of a unique identification code by a compatible wireless device.

[0066] The automatic registration function performed by the control program resident in the computer allows the program to obtain the phone's IMEI **402** and starts a timer **404**. The control program then captures wireless device's unique identification code. For a mobile phone, it will transmit **406** its IMEI as its unique identification code.

[0067] If a positive acknowledgement is received by the wireless device from the computer, the transmission of the unique identification code is repeated **408** by the wireless device. If an acknowledgement is not received, the wireless device's operating system stops the IrDA transmission of its unique identification code **410**.

[0068] The control program will then compare the unique identity codes received with those in its internal list **428**. If the unique identity of a device is not found on the list, the control program may register it **430** as an authorized user by the network administrator according to predetermined rules and access policies.

[0069] After the authorized users and their unique identification codes have been registered, the control program will continually "sniff" **432** for unique identification codes transmitted by compatible IrDA devices (FIG 4A, **406**) by reading its emulated serial port **434**. The control program will then save

the code received in the internal list **436** before sending a return acknowledgement signal **438**.

[0070] The control program will then compare the current identification code against those in its internal list **440** and will take the appropriate security measure **442** if an unauthorized code is received or an unauthorized code has not been received, signaling an out-of-range situation.

[0071] With the prevalence of IrDA-equipped devices such as mobile telephones, PDAs, and notebook computers, the use of such personal devices, suitably modified with a control program, is a viable means by which to practise the present invention. For such devices that do not have built-in IrDA ports, an IrDA communications card may be used to provide such a capability to practise the present invention.

[0072] A person skilled in the art will appreciate that, depending on the wireless devices and wireless communications used in the present invention, modifications may be readily made to the devices to practise the invention. It is foreseeable that the present invention may also be implemented using other industry wireless communication standards which may be developed in the future. For the Bluetooth embodiment of the present invention, few or no modifications are required as the two communicating devices (mobile wireless device and computer) do not need to even form a piconet.

[0073] For the control program resident in the computer, the program may be readily coded in a variety of computer programming languages, depending on the operating system used. The control program may be resident in hardware such as read-only memory (ROM), as a file in the start-up folder for the operating system or built directly into the operating system.

[0074] There are advantages and disadvantages to each option. If resident in ROM, the control program will load faster at start-up of the computer and cannot be easily tampered with. However, updating new versions or releases of the control program will be more laborious. In addition, a

control program written for Microsoft's® Windows® operating system will not work on a Linux® system,

[0075] Another means by which the control program may be run is to build it into the operating system. This allows the control program be as secure from tampering as being resident in ROM. However, it also carries the penalty of being more difficult to modify when upgrades need to be made to the program.

[0076] The preferred implementation of the control program is that placing it in the startup folder of the operating system. To prevent users from modifying the program, the system administrator may protect it through appropriate network rights settings.

[0077] A prototype of the present system has been implemented in a Nokia 7650 mobile phone that has its own built-in Bluetooth communicator capability running on the Symbian operating system. The operating system has been set to enable the phone to be "discoverable" so as to cause it to continually transmit the Bluetooth communicator's unique identity code. A computer system, running on Microsoft's® Windows® XP® operating system has the control program of the present invention coded in C# deployed on the .Net framework. An external MSI Bluetooth device connected to the USB port of the computer and controlled by the control program, allows the invention to be practised.

[0078] The present invention takes advantage of a hitherto non-obvious combination and use of a personal multifunction wireless device, such as a mobile telephone, with either one of two proven and current industry standards for wireless communication, to act as an element of a security system for computer access. The Bluetooth and IrDA standards can both be used in the present invention to enable a user to both access a computer and to activate suitable security means upon departure from the computer.

[0079] This invention may be implemented and practiced at low cost and wireless capabilities, in the form of internal cards or external attachments, can be readily retrofitted to existing mobile telephones and computers.

[0080] The present invention therefore provides a system comprising a mobile device, a computer and a control program, with a method, to controls access to computers and that automatically prevents unauthorized access when the user is away, that overcomes, or at least alleviates, the problems of the prior art.

[0081] A person skilled in the art will recognize that the present invention may be easily implemented in new computer systems, or may be used to supplement or enhance the security measures in existing computer systems.

[0082] It will be appreciated that although a few preferred embodiments have been described in detail, various modifications and improvements can be made by a person skilled in the art without departing from the scope of the present invention.

Claims

1. A security system for controlling access to a computer, the security system comprising:
a computer equipped with a wireless device;
at least one mobile device with a unique identity code and equipped with a compatible wireless communicator; and
a control program operable to authenticate the unique identity code of the at least one mobile device against a list of authorized identity codes stored in the computer for controlling the security system, wherein the computer program permits a user access to the computer after the control program has authenticated the at least one mobile device as an authorized device and when the mobile device's compatible wireless communicator is within operating range of the computer's wireless device.
2. A security system according to Claim 1, wherein the wireless device is a Bluetooth wireless device.
3. A security system according to Claim 1, wherein the at least one mobile device is a Bluetooth-equipped personal digital assistant.
4. A security system according to Claim 1, wherein the at least one mobile device is a Bluetooth-equipped computer.
5. A security system according to Claim 1, wherein the at least one mobile device is a Bluetooth-equipped mobile phone.
6. A security system according to Claim 1, wherein the at least one wireless device is an IrDA wireless device.
7. A security system according to Claim 1, wherein the at least one mobile is an IrDA personal digital assistant.

8. A security system according to Claim 1, wherein the at least one mobile device is an IrDA computer.
9. A security system according to Claim 1, wherein the at least one mobile is an IrDA mobile phone.
10. A method of controlling access to a computer, the method comprising:
installing, in the computer, a wireless device and a control program;
equipping at least one mobile device with a unique identity code and a compatible wireless communicator, said at least one mobile device is carried by user;
enabling wireless communication between the at least one mobile device and the computer;
registering, in a list, at least one authorized user based on the unique identity code of the at least one mobile device, according to predetermined rules and access policies;
permitting user access by the control program to the computer, when the unique identity code of the at least one mobile device with a compatible wireless communicator is found in the list of authorized users in the computer and is within range of the wireless device;
and
not permitting access when the at least one mobile device with its unique identity code is not found in the list of authorized users or is out of range of the wireless device.
11. The method of Claim 10, wherein the installing step further comprising permitting the control program to control the computer.
12. The method of Claim 10, wherein the enabling step further comprising modifications to the at least one mobile device to enable wireless communication with the computer.

13. The method of Claim 12, wherein the enabling step further comprising sniffing, continually, by the computer's wireless device, for the at least one mobile device with compatible wireless communicator, when the computer's wireless device and the at least one mobile device's wireless communicator meet Bluetooth communication standards.
14. The method of Claim 12, wherein the enabling step further comprising activating the computer's wireless device and the at least one mobile device's wireless communicator, when the computer's wireless device and the at least one mobile device's wireless communicator meet IrDA communication standards.
15. The method of Claim 10, wherein the not permitting access step further comprising activating a workstation lock of the computer.
16. The method of Claim 10, wherein the not permitting access step further comprising activating a password protected screensaver program of the computer.