9906094-9
IPO copy - For reference only

METHOD AND APPARATUS FOR PROTECTING CONTROLS IN GRAPHIC USER INTERFACES OF COMPUTER SYSTEMS

Background of the Invention

1. Field of the Invention

This invention relates to graphical user interfaces of computer systems and, more particularly, to systems and methods for ensuring proper user interaction with such GUI components.

2. Background and Related Art

Even since the computer industry advanced beyond command line interfaces to the now familiar graphical user interface (GUI) technology which employs more user friendly and familiar symbols, command bars, pulldown menus, windows and the like, the popularity of this technology has exploded. Along with this has come an enrichment and sophistication of the various software controls which often even emulate in appearance and operation their hardware counterparts. Thus it is not uncommon to see software control in the form of realistic-appearing three-dimensional buttons, slider bars with shading, lights, and even meters and switches.

This emulation has greatly improved the ease with which end-users now interact with computers and with this hardware paradigm which sometimes bears an almost uncanny similarity to the real hardware counterparts. Some such GUIs, in order to further simulate realism, have even been known to incorporate sound with operation of various buttons or

3 DEC 1999 9906094-9

other controls, such as switch clicks, and even backlighting which changes color upon operation with the switch.

However, one weakness of these GUI systems' controls has never been addressed heretofore, namely the exposure of the controls to unintentional, unauthorized or even malicious interaction.

Hardware, human and machine interfaces often must deal with the problem of inadvertent or malicious activation of controls that can have disruptive effects. One example of this is the design practice in hardware devices of recessing controls and covering them with transparent barriers in order to prevent inadvertent activation.

In software user interfaces, however, protection such for such undesired activation of software controls has been far less sophisticated. Thus, such protection has taken the form only of completely disabling controls preventing activation from the keyboard or mouse, such control state typically being indicated by reducing the contrast of the control and its associated text, e.g., graying out or dimming the control, making it unavailable to the user. Thus, a more sophisticated mechanism was highly desired which could address this problem of inadvertent or malicious activation of software controls.

In prior known methods for addressing the just-described problem, there are numerous disadvantages associated with merely disabling controls by dimming or graying them out. First, the text associated with these control is difficult to read. Moreover, users who have authority to view a control's value but not change it experience difficulty in obtaining the information needed.

Secondly, the dimmed control state provides no indication of how a user with proper authority may make it available for change.

Thirdly, the dimmed control itself provides no mechanism for users who are being protected from themselves, e.g., a way of allowing the user to change the value of the control but only after taking a special overt action to enable the change.

Fourthly, the dimmed control does not provide a mechanism in and of itself for hiding the value displayed from users who lack the authority to view the control state. Thus, improvements were needed which would make it possible to make the control state or value more legible. An interface was further desired which may provide visual clues for how the user might access the control and control surfaces for providing access to the control in close proximity to the control itself. Moreover, a solution to the aforementioned problems was sorely needed which provided for a variety of scenarios, including protection from inadvertent access, view but not change, protection from viewing completely, etc., all within the same visual metaphor, and controlling single controls as well as groups of controls.

Summary of the Invention

When a control is in a protected state, the background color of an area surrounding the control is changed to a color providing good contrast with any control surfaces and text, but differing from the standard background color of the window and any other non-protected controls. This field of surrounding color produces the visual effect of a transparent or translucent shield over the control surface. When the field is in place, the user cannot select the control surface by using a mouse click or tabbing to the control. Access to the control is provided by one of two mechanisms, depending

upon the type of access which is available to the user.

If the user currently has authority to access the control and is being protected from mere accidental activation, clicking on an edge of the color field and shield causes the color field to retract, collapse, or vanish, in one embodiment in an animated fashion with or without accompanying sound indicators, so as to reveal the unprotected control in a state which can now accept user interactions. This is intended to produce the metaphor of opening a transparent shield over a hardware control. The metaphor, in one embodiment, is further reinforced by providing a graphical element which resembles a grip surface. This graphical element may be selected to enable the user to physically slide the surface open to access the underlying control viewable through the color field. This reinforces to the user that a conscious physical step is required to signify he or she truly desires to interact with the control.

If the user does not currently have access to the control, a small graphic element is included on or near the colored field, such as a small padlock icon. Clicking on the icon causes a password field to appear, e.g., in a dialog box. Upon entry of the appropriate password and user name, the color field disappears or slides back, collapses, or vanishes in a manner hereinbefore described so as to display the underlying control in a state ready for user interaction by the thus-authorized user or administrator.

If the user lacks authority to view the control, the color of the protected field is set to the current foreground color such that the control appears to be masked out. As previously described, a user is thereby unable to select or interact with the control. Also, as in the case previously described, an icon may be provided so that by selecting it, a user with knowledge of the

access password may thereby remove the cover field to gain access to the control. This access, in one embodiment, is provided in two levels - view access and change access. View access would change the field to a translucent or transparent state for view only of information in the underlying control, whereas change access would remove the field completely to provide full access to the underlying control for user interaction and change.

In still a further alternate embodiment and extensions of the invention, after the control is changed, the protective field will then automatically slide back over the control, thereby restoring the protective state automatically. Further, a protective field may be employed to cover a group of controls all sharing the same access method(s). Still further, a graphic treatment may be employed for a control or group of controls to create the illusion that they are recessed in a well with a transparent opaque field covering them.

Brief Description of the Drawings

Fig. 1 is a high level system architecture drawing of a representative computer system in which the invention may advantageously be employed.

Figs. 2-5 are a sequence of screen captures of the system of Fig. 1, illustrating the sequence of events in effecting authorized user interaction with control areas in accordance with the invention.

Fig. 6 is a flow diagram illustrating the sequence of events described with reference to the figures 2-5.

Figs. 7-10 are a sequence of screen captures of the system of Fig. 1 depicting a sequence of events similar to that of Figs. 2-5 for effecting user interaction with a control area in accordance with the invention wherein the administrative user has not been first authorized for such interaction.

Fig. 11 is a flow diagram depicting the sequence of events illustrated in Figs. 7-10.

Figs. 12-14 is yet another series of screen captures of the system of Fig. 1 depicting interaction with a control area by an administrator who must first be authorized in accordance with the invention.

Fig. 15 is a flow diagram illustrating the sequence of steps depicted in Figs. 12-14 in accordance with the invention.

Detailed Description

Fig. 1 illustrates a preferred embodiment of a computer system which may advantageously employ the improved GUI control protection system of the present invention. The system comprises a CPU 10, read only memory (ROM) 11, random access memory (RAM) 12, I/O adapter 13, user interface adapter 18, communications adapter 14, and display adapter 19, all interconnected via a common address/data and control path or bus 16. Each of the above components accesses the common bus utilizing conventional techniques known to those of ordinary skill in the art, and includes such methods as dedicating particular address ranges to each component in the system, with the CPU 10 being the busmaster. As is further shown in Fig. 1, these external devices such as DASD 15 interface to a common bus 16 through respective adapters such as I/O adapter 13. Other external devices, such as the display 21, similarly use their respective adapter such as display adapter 19 to provide data flow between the bus 16 and the display 21 or other device. Various user interface means are provided for interconnection and use with the user interface adapter 18, which, in the figure has attached thereto representative user input devices such as joy stick 23, mouse 25, keyboard 17, and speaker and/or microphone 27. The system is further provided with a conventional operating system 29 adapted to execute one or more applications 31. Each of these units is well known in as such and accordingly will not be described herein.

The invention admits to implementation on essentially any computer system and corresponding microprocessor, such as the RS/6000 (TM), RISC-based workstations and personal computers of the IBM Corporation executing the AIX (TM) and OS/2 (TM) operating systems, respectively, or similar machines of other vendors, which include for example in the case of

an RS/6000 workstation a 604 PowerPC (TM) RISC chip. (RS/6000, IBM, AIX, OS/2 and PowerPC are trademarks of the IBM Corporation).

Contained with the CPU 10 of Fig. 1, typically is one or more microprocessors which performs the system address, data, and control processing functions necessary for correct operation of the system of Fig. 1. Although the invention admits to application to various microprocessor designs, in the embodiment disclosed herein, the microprocessor takes the form of a PowerPC 604 microprocessor manufactured by the IBM Corporation, which is a species of microprocessor known as a reduced instruction set computer (RISC) microprocessor. Further details regarding the architecture and operation of such a microprocessor may be obtained from the PowerPC 604 RISC Microprocessor Users Manual, Document #MPC604UM/AD, November, 1994, copyright IBM Corporation, which is incorporated herein by reference.

In the context of the invention, the user will view various objects such as a cursor and pop up or pop down menus on the display 21 which may be manipulated by means of various pointing devices such as the mouse 25 and voice activated navigation. Program code associated with the user interface adapter 18 by way of a device driver for the pointing device 25 and microphone 27 in conjunction with operating environment and application code resident in RAM 12 and/or DASD 15 will facilitate and enable movement of a cursor on the display screen 21 responsive to and in association with correlative voice commands spoken into microphone 27.

Turning now to Figs. 2-5, a series of representative screen captures are depicted in Figs. 2-5, illustrating a sequence of events viewable on the display of Fig. 1 in one implementation of the invention. First, in Fig. 2, such a screen display 30 may be seen which is typical of the many GUI-based operating systems and corresponding applications currently

available.

In the screen display, a control area 32 is further depicted comprised of a cover 34 and underlying control 38 (seen in Fig. 5). In the embodiment under discussion, the purpose of the cover 34 is to prevent a user with authority from accidental activation or interaction with the control 38. As may be seen in Fig. 2, the cover 34 is desirably transparent (as symbolized by cross-hatching) so as to permit the user to see through the cover to the underlying control 38. The control will, as desired, include information such as alphanumeric messages (for example the "delete" message 40). The invention is not intended to be so limited, however, and contemplates as part of the control 38 not only a control labeling message such as "delete", "close", etc., but further to include fields which the end-user may fill in information for, slide bars, or any other opportunity for the user to intelligently interact with an area of the computer screen by inputting data by a keyboard, interacting with a pointing device, or the like.

Turning now to Fig. 3, a conventional cursor 37 is shown which is moveable by a pointing device. One problem with prior art GUI systems is that a user may inadvertently click on a control area 38, thereby causing a resulting computer operation when, in fact, such clicking or other interaction with a pointing device or even a keyboard entry was accidental. The present invention is, in part, intended to address this problem. Thus, one purpose of the cover 34 is to permit the end-user to, due to its transparency, view what the meaning of the control 38 is while at the same time preventing interaction with the control by the conventional keyboard entry or pointing device 25 activation without additional overt actions.

Fig. 3 is intended to indicate that when the user desires to interact with the control 38, the user first clicks with the pointing device and cursor 37 on the cover 34 so as to cause a retraction of the cover 34 to expose the underlying control 38 for interaction. It will be noted that in Fig. 3, the

cursor 37 is positioned at a small area in the lower right corner of the control area 32. Although not necessary, one desirable implementation of the invention would provide that only a relatively small area of the cover 34 or area adjacent thereto be activatable so as to cause the removal of the protective shield or cover 34. This is in order to ensure that a highly deliberate action is taken by the administrative user intending to interact with the control 38.

Upon the end-user so interacting with the cover 34, it is thereby caused to retract so as to display the underlying control 38 in a state whereby the user may thereby interact with the control 38 (Fig. 5). After such user action (by means of the click with the cursor 36 positioned on the cover 34), or, more particularly, the particular area intended to cause withdrawal of the cover 34, it may be preferable to provide protective shield or cover animation whereby the user may actually view the cover 34 being retracted from over the control 38. Thus, referring to Fig. 4, if this feature is implemented, it may be seen that in fact the cover 34 is shown at an intermediate state where it is in the process of being removed by such animation from completely covering the control 38 in a "window-shade" metaphor. At the completion of this retraction, the control 38 will thereby be fully exposed as shown in Fig. 5, ready for interaction with the user. As noted, the user then proceeds to either activate the control 38 by clicking on it, or to otherwise interact with information and fields associated with the control 38 by clicking or deleting radio button entries, typing in information in exposed fields, or the like.

In keeping with the need for the protection from inadvertent interaction with the control 38 while at the same time permitting the user to recognize the purpose of the control 38, as noted, the cover 34 is desirably transparent so that it appears to be a cover viewable by the end-user while at the same time permitting the user to see through the cover 34 to the extent necessary to view the label or other information associated with the

control 38. Thus, in one embodiment, the cover may simply be a lightly shaded cover, with the control 38 itself comprising only a portion of the cover 34 as desired and also as desired of a different graphic design or color which may be viewable through the cover 34. Rather than an automatic animated retraction or instant retraction of the cover 34 upon user interaction therewith, if desired, the user may alternatively be required to physically remove the cover 34 from its position over and protecting the control 38. This may be done by requiring the user to physically move the cursor 36 which causes corresponding movement of the cover 34 sufficiently to expose the control 38. This provides yet an additional level of protection against inadvertent user interaction with the control 38, (otherwise permitted by perhaps an inadvertent clicking on the cover 34) by causing the user to physically remove the cover 34 by movement of the cursor 36. This ensures the user is acting out his or her intention to place the control 38 in a state whereby user action will be accepted and effective.

Turning now to Fig. 6, depicted therein is a representative flow diagram of the sequence just described. This sequence desirably will be implemented in program code so as to cause the GUI of the system of Fig. 1 to respond in a manner just described. It will be appreciated that this feature may be implemented in the operating system itself of Fig. 1, or, alternatively in one or more applications requiring protected user interaction in the manner described.

Fig. 6 is a flow diagram of the sequence of actions of invention previously described with reference to Figs. 2-5 which may be implemented in program code for the system of Fig. 1. First, detection will be made that the user has activated the control cover, 41. The system will then cause withdrawal of the cover from over the control 43, signifying the control is ready for user interaction. It will be recalled that this may be implemented in an animated fashionor instantly. The user will then

interact with the control, as shown at reference numeral 45, whereupon the cover will be replaced over the control, 49.

In the implementation hereinbefore described with reference to Figs. 1-6, an underlying assumption has been that the administrative user has been authenticated, e.g., has the permission and authority to cause removal of the cover 34 so as to place the control 38 in a state ready for further user interaction. However, it will be readily appreciated that this may not desirably be the case. Alternatively, in an embodiment of the invention depicted with reference to Figs. 7-11, it has been assumed that a situation exists in which the administrative user should not be permitted such access and interaction with the control 38 without first requiring an authentication step.

Turning now to Fig. 7, and comparing it to Fig. 2, it will be noted that a locking mechanism 42 has been provided therein, symbolized by a padlock or the like. In a similar manner to that of Fig. 3 wherein the user causes the cursor 36 to activate the cover 34 or a grip surface, as shown in Fig. 8, the user, by means of a pointing device, may cause the cursor 37 to interact with this locking mechanism 42 by, for example, clicking on it. In response to this, a user authentication subscreen 44 (Fig. 9) may be caused to appear. In this subscreen 44, the administrative user is prompted for information as desired in order to authenticate that he or she should be permitted to interact with the control 38. Thus, in the implementation shown in Fig. 9, such user is prompted for a user name and password of an administrative account with sufficient authority to enable the user to interact with the control 38. In a specific implementation of this alternate embodiment, the end-user may be so required to provide his or her password in order to interact with the control 38, having to do with actions associated personally with the end-user. However, in this embodiment, it is also fully contemplated by the invention that such authentication steps depicted with reference to Figs. 7-11 may be intended

to ensure authentication of an administrator per se, so as to verify that the administrator has authority to make changes or delete another user's account or other information associated with the control area 32. Upon the administrator or user providing the necessary information prompted for by the user authentication subscreen 44, the control 38 will thereby be made available for interaction, as shown in Fig. 10 in like manner to the steps described in Figs. 2-6. Thus, upon the user providing the information prompted in the subscreen 44, the cover 34 may be either automatically removed from over the control 38 (either in an animated fashion or instantly) or, in the alternative, the user or administrator may thereby be authenticated so as to permit a manual removal of the cover 34 from over the control 38 by physically removing the cover 34 with the pointing device and cursor 37 in the manner previously described.

Fig. 11 is a flow diagram illustrating the sequence of events described with reference to Figs. 7-10 which may be implemented in program code in the system of Fig. 1. First, program code will sense activation by the end-user of the locking mechanism, 51. The user will then input and the system receive such input which is user authorization information (e.g., password, etc.), 53. The system will then cause withdrawal of the cover from the control, 55, again either in animated or instant fashion. The user will then interact with the control with such interaction being sensed by the system, 57. Finally, the cover will be replaced over the control, 59.

Yet a further embodiment of the invention is shown with reference to Figs. 12-14. In this instance it will first assumed that an end-user may lack authority to even view the control or status information and the administrative rights to control interaction with the control area 32 without authentication of administrative rights. In such a case, again, the control area 38 may have superimposed thereon the cover 34 which will operate in the manner previously described. However, it will be noted that the

information regarding the administrative rights (otherwise shown, for example, as reference numeral 46 in Fig. 7) has been obscured by a darkened field 48. It will further be known by a darkened field 48 in Fig. 12. It will be further be noted that as in the case of Fig. 2, a locking device 50, which again may be a padlock metaphor, is provided associated with the administrative rights information 46 and the obscuring blackened field 48. Upon the administrator interacting with the locking device 50 (in a manner similar to that of Fig. 7), e.g., clicking on the portion of the field associated with the locking device 50 and authenticating with an administrative user counted password (similar to the steps described with reference to Fig. 9), it will noted in Fig. 13 that the obscuring cover 48 is removed, thereby exposing the administrative rights which this administrator may have. In the case of Fig. 13, it will noted from the control area 32 that this particular authenticated administrative user may only have view authority with respect to the control area 32. However, in the alternative, as shown in Fig. 14, the control area 32 is ready for interaction by the administrator inasmuch as the cover 34 (Fig. 2) has been removed to expose the control 38, thereby signifying that this particular authenticated administrator account has provided the administrator with change authority so that he or she may interact with the control 38 as desired in a manner previously described.

Fig. 15 is a flow diagram which may be implemented in program code similar to that of the flow diagrams of Fig. 6 and Fig. 11, whereby this sequence of events may be caused to occur by means of the operating system, wherein one or more applications are running on the operating system in the computer of Fig. 1.

Fig. 15 is a flow diagram illustrating the sequence of steps hereinbefore described with reference to Figs. 11-14, and which may be implemented in program code in the system of Fig. 1 wherein authenticated administrative user input is desired. First, the administrator

locking device is activated and sensed in the system, 61. Administrator authorization information is then input and sensed by the system, 63. Next, in response to this administrative user input, a determination is made of whether the administrator has authority for view only or change authority, as shown at decision block 65. If view authority only was granted, the administrator then proceeds to view the desired information as permitted by the system, 67. On the other hand, if the administrative user has changed authority, flow exits to the right of block 69, whereupon the protective cover is withdrawn from the control. The administrative user may then interact with the control, 71, whereupon the protective cover is again replace over the control, 73.

It will be understood from the foregoing description that various modifications and changes may be made in the preferred embodiment of the present invention without departing from its true spirit. It is intended that this description is for purposes of illustration only and should not be construed in a limiting sense. The scope of this invention should be limited only by the language of the following claims.

Claim(s)

1. A method for managing a control area in a graphical user interface (GUI) of a computer system comprising:

displaying said control area;

displaying a cover having first and second positions relative to said control area alternately preventing and permitting, respectively, user interaction with said area.

2. The method of Claim 1 comprising moving with a pointing device said cover between said first and said second positions.

3. The method of Claim 2 wherein said moving of said cover comprises:

contacting said cover with a cursor moveable with said device; and

moving said cover with said cursor from said first to said second or said second to said first position.

4. The method of Claim 2 wherein said moving of said cover comprises:

animated movement of said cover on said GUI from said first to said second position, including visibly observable positions therebetween.

5. The method of Claim 4 wherein said control area defines an area of information; and

said cover is transparent, thereby permitting user perception of said



information when said cover is in said first or said second position.

6. The method of Claim 5 wherein said user interaction is taken from a group comprising:

entering said information;

deleting said information;

or altering said information.

7. The method of Claim 6 wherein said cover has displayed and associated therewith a user activatable lock mechanism alternately permitting or denying said moving of said cover.

8. The method of Claim 7 further including:

activating said lock mechanism; and

entering a password, thereby permitting said moving of said cover.

9. The method of Claim 8 further including:

displaying an administrative user area including an administrative user lock mechanism;

activating said administrative user area lock mechanism; and

entering an administrative user password, thereby permitting a first state wherein an administrator may thereby cause with said pointing device said movement of said cover and said user interaction.

* C L M S *

10. The method of Claim 9 wherein said entering of said administrative user password thereby alternatively permits a second state denying said user interaction and permitting only said user perception of said information

11. Apparatus for managing a control area in a graphical user interface (GUI) of a computer system comprising:

means for displaying said control area;

means for displaying a cover having first and second positions relative to said control area alternately preventing and permitting, respectively, user interaction with said area.

12. The apparatus of Claim 11 comprising means for moving with a pointing device said cover between said first and said second positions.

13. The apparatus of Claim 12 wherein said means for moving of said cover comprises:

means for contacting said cover with a cursor moveable with said device; and

means for moving said cover with said cursor from said first to said second or said second to said first position.

14. The apparatus of Claim 12 wherein said means for moving of said cover comprises:

means for animated movement of said cover on said GUI from said first to said second position, including visibly observable positions therebetween.

15. The apparatus of Claim 14 wherein said control area defines an area of information; and

said cover is transparent, thereby permitting user perception of said information when said cover is in said first or said second position.

16. The apparatus of Claim 15 wherein said user interaction is taken from a group comprising:

entering said information;

deleting said information;

or altering said information.

17. The apparatus of Claim 16 wherein said cover has displayed and associated therewith a user activatable lock mechanism alternately permitting or denying said moving of said cover.

18. The apparatus of Claim 17 further including:

means for activating said lock mechanism; and

means for entering a password, thereby permitting said moving of said cover.

19. The apparatus of Claim 18 further including:

means for displaying an administrative user area including an administrative user lock mechanism;

means for activating said administrative user area lock mechanism;

* C L M S *

and

means for entering an administrative user password, thereby permitting a first state wherein an administrator may thereby cause with said pointing device said movement of said cover and said user interaction.

20. The apparatus of Claim 19 wherein said means for entering of said administrative user password thereby alternatively permits a second state denying said user interaction and permitting only said user perception of said information.

21. A computer program product comprising a computer usable medium having program code means embodied in the medium for managing a control area in a graphical user interface (GUI) of a computer system, the program code means including:

program code means for displaying said control area;

program code means for displaying a cover having first and second positions relative to said control area alternately preventing and permitting, respectively, user interaction with said area.

22. The computer program product of Claim 21 comprising program code means for moving with a pointing device said cover between said first and said second positions.

23. The computer program product of Claim 22 wherein said program code means for moving of said cover comprises:

program code means for contacting said cover with a cursor moveable with said device; and

program code means for moving said cover with said cursor from said first to said second or said second to said first position.

24. The computer program product of Claim 22 wherein said moving of said cover comprises:

program code means for animated movement of said cover on said GUI from said first to said second position, including visibly observable positions therebetween.

25. The computer program product of Claim 24 wherein said control area defines an area of information; and

said cover is transparent, thereby permitting user perception of said information when said cover is in said first or said second position.

26. The computer program product of Claim 25 wherein said user interaction is taken from a group comprising:

entering said information;

deleting said information;

or altering said information.

27. The computer program product of Claim 26 wherein said cover has displayed and associated therewith a user activatable lock mechanism alternately permitting or denying said moving of said cover.

28. The computer program product of Claim 27 further including:

program code means for activating said lock mechanism; and

program code means for entering a password, thereby permitting said moving of said cover.

29. The computer program product of Claim 28 further including:

program code means for displaying an administrative user area including an administrative user lock mechanism;

program code means for activating said administrative user area lock mechanism; and

program code means for entering an administrative user password, thereby permitting a first state wherein an administrator may thereby cause with said pointing device said movement of said cover and said user interaction.

30. The computer program product of Claim 29 wherein said program code means for entering of said administrative user password thereby alternatively permits a second state denying said user interaction and permitting only said user perception of said information.