METHOD AND SYSTEM FOR DISABLING FEATURES OF A MOBILE DEVICE

Field of the Invention

[0001] The present invention relates to a mobile device. In particular, the invention relates to a method and system for temporary disabling features of a mobile device.

Background

[0002] With rising concerns over security, many facilities restrict or prohibit the use mobile electronic devices, or at least some features of the mobile electronic devices. These mobile electronic devices are generally bundled with lots of features and applications. However, it is a challenge to enforce such restriction ever since the mobile devices are getting smaller in size and yet multi-functional.

[0003] The most straightforward solution to such restriction is to prohibit all such mobile devices with the restricted features to be carried into the restricted areas. All individuals are required to hand over their mobile devices before entering the restricted areas. Security officers are often appointed at the entrance checkpoint of the restricted area to perform checking to restrict owners of any such mobile devices from entering the restricted areas. However, such method often causes a crowd at the entrance checkpoint. Besides, it requires additional storage space to keep the handed over devices temporary and safely.

[0004] In most situations, the restricted areas restrict only certain features to be used within the restricted areas. Therefore, it may not be practical to prohibit the mobile device because the non-restricted features on the same device may be essential to the users within the restricted areas.

Summary

[0005] The present invention describes a method and system for enabling/disabling a restriction state of a mobile device having applications and features, wherein working states of the applications and features are identified by status values on the mobile device and usage on one or more of the applications and features is restricted during the restriction state. In one aspect, the method and system comprises a software agent executable on the mobile device, wherein the software agent is adapted for receiving a first command signal to enable the restriction state, wherein the first command signal comprises restriction status values; replacing the status values with the restriction status values, thereby forcing the applications and features in the working states defined by the restriction status values; maintaining the restriction status values in the mobile device during the restriction state; and receiving a second command signal to disable the restriction state.

[0006] In one embodiment, the software agent may further verify an authenticity of the second command signal against the first command signal. The authenticity may include a password.

[0007] In another embodiment, the software agent may be executed at startup of the mobile device.

[0008] In yet another embodiment, wherein maintaining the restrictions status values in the mobile device may comprise checking recursively if the status values are the restriction status values; and replacing the status values with the restriction status values if the status values are not the same as the restriction status values.

[0009] In yet a further embodiment, the software agent may be adapted for storing present status values prior to the step of replacing the status values with the restrictions status values and restoring the status values to the present status values.

[0010] In another embodiment, the first command signal may include a prescribed time period, and the restriction state is disabled after expiration of the prescribed time period.

[0011] In yet another embodiment, the first signal and/or second signal is received via a wireless link. It is possible that the first and second command signals are in a form of short messaging service message.

[0012] In an alternative embodiment, the first command signal and/or the second command signal can be created via entering commands through the software agent manually.

[0013] In accordance with another aspect of the present invention, the system provides a software agent enables a restriction state that forcing the applications and features in a restricted working state. The software agent operates to replace working status values of the applications and features with a restriction status values and to maintain the restrictions status values. The restriction state is enabled when a first command signal is received. The restriction state is disabled when a second command signal is received by the software agent.

Brief Description of the Drawings

[0014] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0015] **FIG. 1** illustrates a schematic block diagram of a mobile communication device in accordance with one embodiment of the present invention;

[0016] **FIG. 2** illustrates a process for enabling/disabling a restriction state on a mobile communication device in accordance with one embodiment of the preset invention; and

[0017] FIG. 3 illustrates a process for controlling applications and features of a mobile communication device in accordance with one embodiment of the present invention.

Detailed Description

[0018] In line with the above summary, the following description of a number of specific and alternative embodiments is provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0019] FIG. 1 illustrates a schematic block diagram of a mobile communication device **100** in accordance with one embodiment of the present invention. The mobile communication device **100** can be any portable electronic devices, such as mobile phone, having a plurality of applications and features **102** provided therein. The applications and features **102** can be any hardware or software based applications and features that are easily accessible by owner/user of the mobile communication device **100**. The applications and features **102** include Bluetooth for wireless communications, phone profiling containing profile settings for user selection, and etc. These features **102** are identified as function identities (IDs) **104** in the mobile communication device **100**, wherein the status of the applications and features **102** are represented by associated status values. The mobile communication device **100** comprises a software agent **110** adapted to restrict/limit usage of one or more of the applications and features **104** on a temporary basis, typically when user/owner of the mobile communication device **100** enters a restricted area. Depending on the restriction requirements, the software agent **110** operates to locate the function IDs **104** and to re-configure the associated status values according to the restrictions/limitations to force the working status of the relevant applications and features **102** to the restricted states. In a non-

limiting example, the software agent **110** can be set to re-configure the relevant status values of the function IDs **104** to turn off a Bluetooth transmitter of the mobile communication device **100**. In another example, the software agent **110** can also be set to re-configure the relevant status values of the function IDs **104** for forcing the phone profile of the mobile communication device **100** into a silent mode prior to entering a cinema theater. For the ease of illustrations, the "restriction state" shall herein refer to a period when the one or more applications or features **102** are restricted for usage by the software agent **110**.

[0020] The restriction state is initiated on the mobile communication device **100** by sending a command signal to the software agent **110** via a wireless communication. The command signal re-configures the mobile communication device **100** according to the restriction policies of the restricted area. Depending on the route of communication used, the command signal can be transmitted to the mobile communication device **100** in various forms; for example, the command signal can be sent in a form of a short messaging service (SMS) message via GSM network. The command signal includes commands and parameters for executing the restriction policies on the applications or features **102** of the mobile communication device **100**. The command signal is adapted not to be viewed by the user of the mobile communication device **100**, and after the software agent **110** parses the required commands and parameters the command signal, the command signal is removed/deleted from the mobile communication device **100**. During the restriction state, the software agent **110** proactively accesses the function IDs **104** and changes the relevant status values according to the extracted commands and parameters. The software agent **110** activates a timer to perform recursive checking and updating on the status values to ensure that the applications and features **102** remain at the required restriction state. To terminate the restrictions/limitations, another authenticated command signal is required to restore the status values of the function IDs **104**. The command signal to terminate the restriction state is generally sent when owner/user of the mobile communication device **100** is leaving the restricted area.

[0021] The software agent **110** is adapted to execute automatically at startup of the mobile communication device **100** and it is running on the background of the mobile communication device **100**. When the mobile communication device **100** is rebooted, the software agent **110** detects if the mobile communication device **100** was in the restriction state before rebooting and the soft agent **110** maintains the mobile communication device **100** at the detected previous state.

[0022] The command signal may comprise the restriction policy information, a prescribed time period, password, enabling/disabling instruction, and etc. The command signal can be sent via any of the communication channels available to the mobile communication device **100** and the command signal can be in a form appropriates to the communication channel used. When required, the command signal can be encrypted for transmission.

[0023] In accordance with another embodiment of the present invention, the command signal is inputted to the software agent **110** manually. The software agent **110** may provide a user interface for inputting the relevant restriction policies which in turn convert into commands and parameters for implementing the restriction policies. The software agent **110** may require a password to be entered for initiating the restriction state. To restore working states of the applications and features **102**, the same or a corresponding password is required to be entered to terminate the restriction state.

[0024] **FIG. 2** illustrates a process for controlling the applications and features **102** a mobile communication device **100** in accordance with one embodiment of the preset invention. The process comprises providing a software agent **110** in step **202**; executing the software agent **110** in step **204**; transmitting a command signal in step **206**; reading and parsing commands and parameters in step **208**; and activating/deactivating a restriction state in steps **210**. In the step **202**, the mobile communication device **100** is provided with the software agent **110** that is adapted to change status values of the function IDs **104** on the mobile communication device **100**.

The software agent **110** can be pre-installed or install-on-demand on the mobile communication device **100**. Once it is installed, the software agent **110** is running in the background of the mobile communication device **100** in the step **204**. The software agent **110** is also adapted to be executed automatically at every startup of the mobile communication device **100**. In step **206**, the software agent **110** awaits a command signal to be received. When a command signal is received, the software agent **110** performs verification on the command signal. The command signal can be any transmission signal such as a configuration SMS or the like, that contains appropriate commands and parameters readable by the software agent **110** for enabling/disabling the restriction state. The command signal can be sent through any of the communication channels of the mobile communication device **100**, such as GSM, GPRS, Wi-Fi, Bluetooth etc. In step **208**, the software agent **110** reads the command signal and parses the commands and parameters that include the restriction status values for executing the restriction state. The software agent **110** then activates/deactivates the restriction state accordingly in step **210**.

[0025] In step **206**, the command signal can be sent in various ways. In one embodiment, the command signal is transmitted to the mobile communication device **100** automatically when the owner/user of the mobile communication device **100** enters the restricted area. Location-based-services and global positioning system, for example, can be used to detect if owner or user of the mobile communication device **100** is within the restricted area. In another embodiment, the command signal is sent manually to the mobile communication device **100** when the owner/user registers to enter the restricted area at the check point.

[0026] To prevent that the restrictions state is disabled/terminated by unauthenticated command signal sent to the software agent **110**, the command signal may include authentication data for verification. The authentication data can be a password or similar indicia. Accordingly, once the restriction state is enabled, it can only be disabled/terminated with an authenticated command signal.

[0027] **FIG. 3** illustrates a process for enabling/disabling the restriction state of a mobile communication device **100** in accordance with one embodiment of the present invention. The process comprises checking the command signal to determine whether the restriction state is to be enabled or disabled in step **302**; starting a timer in step **304**; storing present status values in step **306**; setting restriction status values **308**; reading current status values in step **310**; awaiting another command signal in step **312**; checking if the current status values is the restriction status values in step **314**; stopping the timer in step **316** and restoring the present status values in step **318**. The process occurs when the command signal is verified as being valid, and the restriction policy commands and parameters are extracted from the command signal. In the step **302**, the software agent **110** checks if the command signal is used for enabling or disabling the restriction state. If the command signal is used for enabling the restriction state on the mobile communication device **100**, the software agent **110** starts the timer in the step **304** to perform recursive loops of checking and updating on status values on the mobile communication device **100**. In the step **306**, the software agent **110** stores the present status values that can be used for restoring the applications and features **102** working status. In step **308**, the software agent **110** replaces the present status values with the restriction status values. Accordingly, the relevant applications and features **102** are turned into the working state according to the restriction status values. In the step **310**, the software agent **110** reads the current status values and in the step **312**, the software agent **110** awaits a new command signal. When no new command signal is received, the software agent **314** determines if the current status values remain at the restriction status values. In step **314**, if there is no change in the status values, the software agent **110** loops back to step **310** to read the current status values and the step **312** to listen for a new command signal. When the software agent **110** determines that the status values have been modified or they are different from the restriction status values in step **314**, the software agent **110** loops back to the step **308** to replace the current status values with the restriction status values. When a new command signal is received, the software agent **110** verifies the command signal and parses the restriction policy commands as in the steps **206** and **208** of **FIG. 2**. Similarly, the software agent **110** determines whether the command signal is used to disable/terminate the restriction state

in the step **302**. When a command signal to disable/terminate the restriction state is received, the software agent **110** stops the timer in step **316** and restores the present status values in step **318** to terminate the restriction state.

[0028] Still referring to **FIG. 3**, the status values relates generally to parameters that are used to identify the working state of the applications and features **102** on the mobile communication device **100**. It is understood that the status values representing the working states are not necessary limited to only "ON" or "OFF". For example, they can be values representing levels of the working state, such as volume levels of a ring tone or values that representing the various modes of features. The present status values relate to the status values appear on the mobile communication device **100** immediately before the restriction state starts. The restriction status values relate to the status values used during the restriction states and they are set according to the restriction policies required during the restricted state. The software agent **110** is operable to maintain the restriction status values on the mobile communication device **100** during the restriction state.

[0029] There are various possibilities that can cause changes to the status values during the restriction state. In one example, general usage of the mobile communication device **100** by the owner/user may change the status values when the applications and features **102** of the mobile communication device **100** are executed. The usage can be an user initiated usage or automatic operations on the mobile communication device **100**. In another example, rebooting the mobile communication device **100** may cause status values to be reset to default status values. In any event, when the software agent **110** determines that the status values do not accord with the restriction status values during the restriction state, the software agent **110** replaces the status values by the restriction status values.

[0030] Whenever possible, the software agent **110** is configured to have a high priority level to prevent interruption by other applications during its operations.

[0031] The following non-limiting examples illustrate various methods of transmitting the command signal to enable/disable the restriction state.

[0032] Example 1: Via Bluetooth

[0033] The Bluetooth of the mobile communication device is required to be turned on to receive a command signal to enable/disable the restrictions state. The Bluetooth transceiver at the restricted area is adapted to search for any active Bluetooth device and once detected, the Bluetooth transceiver sends a command signal to enable and disable the restriction state of the mobile communication device.

[0034] Example 2: Via Global Positioning System (GPS)

[0035] A mobile communication device with GPS receiver is able to detect a location of the mobile communication device. The software agent further provides a database of restricted areas and when the software agent detects that the mobile communication device is within the restricted area, the software agent automatically enable the restriction state.

[0036] Example 3: Via SMS

[0037] For mobile communication devices can receive the control signal in a form of SMS message, typically via GSM network. The SMS message contains simple message/commands and parameters recognized by the software agent to enable/disable the restriction state. The transmission can be done manually or automatically. For manual SMS transmission, the SMS message can be sent by the security officer before owner/user of the mobile communication device enters the restricted area. And when owner/user of the mobile communication device leaves the restricted area, another SMS message is required to terminate the restriction state. For automatic SMS transmission, the SMS message is sent automatically to activate the restriction state when owner or user of the mobile communication device enters the restricted area. A location-based

service may be used to automatically detect if the owner/user of the mobile communication device enters the restricted area.

[0038] For manual SMS transmission, the SMS can be sent by the security officer before the mobile communication device enters the restricted area. And when the mobile communication device leaves the restricted area, another SMS is required to restore the functionality of the applications and features. As for automatic SMS transmission, the location-based service may be used to detect if the mobile communication device has entered the restricted area, when the mobile communication devices entered the restricted area, an SMS is sent automatically to enable/disable the restriction state.

[0039] It is also understood that it need not necessary be a mobile communication device **100** as illustrated above. It can be any portable electronic device, such as personal data assistant (PDA) and the like.

[0040] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

Claims

1. A method for enabling/disabling a restriction state of a mobile device having applications and features, wherein working states of the applications and features are identified by status values on the mobile device and usage on one or more of the applications and features is restricted during the restriction state, the method comprising:

executing a software agent on the mobile device;

receiving a first command signal to enable the restriction state, wherein the first command signal comprises restriction status values;

replacing the status values with the restriction status values, thereby forcing the applications and features in the working states defined by the restriction status values;

maintaining the restriction status values in the mobile device during the restriction state by repeatedly replacing the status values with the restriction status values; and

receiving a second command signal to disable the restriction state.

2. The method according to claim 1, further comprising verifying an authenticity of the second command signal against the first command signal.

3. The method according to claim 2, wherein the authenticity includes a password.

4. The method according claim 1, wherein the software agent is executed at startup of the mobile device.

5. The method according to any one of the preceding claims, wherein maintaining the restrictions status values in the mobile device comprising:

checking recursively if the status values are the restrictions status values; and

replacing the status values with the restriction status values if the status values are not the same as the restriction status values.

6. The method according to claim 1, further comprising storing present status values prior to the step of replacing the status values with the restrictions status values.

7. The method according to claim 6, further comprising restoring the status values to the present status values.

8. The method according to any one of the preceding claims, wherein the first command signal includes a prescribed time period, and the restriction state is disabled after expiration of the prescribed time period.

9. The method according to any one of the preceding claims, wherein the first signal and/or second signal is received via a wireless link.

10. The method according to claim 9, wherein the first and second command signal are in a form of short messaging service message.

11. The method according to any one of the preceding claims, wherein the first command signal and/or the second command signal is created via entering commands through the software agent manually.

12. A system for disabling/enabling a restriction state of a mobile device having applications and features, wherein working states of the applications and features are identified by status values on the mobile device and usage on one or more of the applications and features is restricted during the restriction state, the system comprises:

a software agent executable on the mobile device for receiving a first command signal comprises restrictions status values to enable the restriction state, said software agent is operable to replace the status values to the restriction status values and to maintain the restriction status values in the mobile device during the restrictions states by repeatedly replacing the status values with the restriction status values, thereby forcing the applications and features in the working stats defined by the restrictions status values,

wherein the software agent is operable to disable the restriction state when a second command signal is received.

13. The system according to claim 12, wherein the software agent operable to verify an authenticity of the second command signal against the first command signal.

14. The system according to claim 13, wherein the authenticity includes a password.

15. The system according to any one of the claims 12 to 14, wherein the software agent is executed at startup of the mobile device.

16. The system according to any one of the claims 12 to 15, wherein the software module is operable to check recursively if the status values are the restrictions status values, and to replace the status values with the restriction status values if the status values are not the same as the restriction status values, thereby maintaining the restriction status values in the mobile device.

17. The system according to claim 12, wherein the software agent further operable to store present status values before replacing the status values with the restrictions status values.

18. The system according to claim 17, wherein the software agent operable to restore the status values to the present status values.

19. The system according to any one of the claims 12 to 18, wherein the first command signal include a prescribed time period, and the software agent disables the restriction state after expiration of the prescribed time period.

20. The system according any one of the claims 12 to 19, wherein the first signal and/or second signal is received via a wireless link.

21. The system according to claim 20, wherein the first and second command signals are in a form of short messaging service message.

22. The system according to any one of the claims 12 to 21, wherein the first command signal and/or the second command signal is created via entering commands through the software module manually.