Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2764283 A1 2013/07/16

(21) 2 764 283

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2012/01/16

(41) Mise à la disp. pub./Open to Public Insp.: 2013/07/16

(51) Cl.Int./Int.Cl. *G06F 15/00* (2006.01),
H04W 88/02 (2009.01)

(71) Demandeur/Applicant:
MORELLI, GIOVANNI J., CA

(72) Inventeur/Inventor:
MORELLI, GIOVANNI J., CA

(74) Agent: NA

(54) Titre : APPLICATION DE COMMANDE POUR SECURITE ET DIAGNOSTICS AMELIORES SUR APPAREIL MOBILE
(54) Title: MOBILE DEVICE CONTROL APPLICATION FOR IMPROVED SECURITY AND DIAGNOSTICS

(57) Abrégé/Abstract:
A control application is provided for reading from and writing to hardware and software information in the stack of a mobile device. The mobile operating system is accessed by the control application at layers including the kernel, security layer, and user-interface. The control application provides improved access to and retrieval of records of user hardware access and times based on kernel or other information; software access and times per kernel, user interface or information. There is improved security for and control of the device generally, or per specific desired criteria. Use of the mobile device by multiple users is promoted.

ABSTRACT

A control application is provided for reading from and writing to hardware and software information in the stack of a mobile device.

The mobile operating system is accessed by the control application at layers including the kernel, security layer, and user-interface.

The control application provides improved access to and retrieval of records of user hardware access and times based on kernel or other information; software access and times per kernel, user interface or information.

There is improved security for and control of the device generally, or per specific desired criteria. Use of the mobile device by multiple users is promoted.

MOBILE DEVICE CONTROL APPLICATION FOR IMPROVED SECURITY AND DIAGNOSTICS

TECHNICAL FIELD

The field relates to mobile device hardware and software monitoring and data transfer.

BACKGROUND

Access to the features of mobile devices (e.g., smartphone, tablet, PDA, netbook, mini-notebook) is restricted due to the reduced computing power available when these devices are compared with laptop and desktop computers. This impacts the ability to control access to security and other settings, user profile customization, and diagnostic and analytic information. Limited access to the underlying software stack also impacts use of these features. Improved access is desired.

BRIEF DESCRIPTION

A control application is provided for reading from and writing to hardware and software information in the stack of a mobile device.

The mobile operating system is accessed by the control application at layers including the kernel, security layer, and user-interface.

The control application provides improved access to and retrieval of records of user hardware access and times based on kernel or other information; software access and times per kernel, user interface or information.

There is improved security for and control of the device generally, or per specific desired criteria.

The control application also promotes use of the mobile device for multiple users, including an administrator, through improved use of user profiles at an application, system wide, or restricted system level, as desired.

DETAILED DESCRIPTION

Access by the control application at layers including the kernel, security layer, and user-interface provides improved use of device records. Access can be provided, in one example method, where the device's software component signature check protocol is accessed to modify the interaction with the stack.

The control application can generate a library data report of software or hardware use for desired time periods. These may be stored on the device for upload either manually, at set times, or by continuous real-time transfer.

A permissions table can be generated from retrieved information based on, for example, a list of software, hardware, or both, as accessed by the user within a selected time period.

Permission criteria can be established and assigned for designated software or hardware items, (e.g., applications) to control associated settings such as authorized access, ability to change individual settings, etc., against a permission library generated by the control application or otherwise.

Criteria can be applied more globally across a range of items on the device as well. Internal debugging or other reports or information can be monitored for specific messages that can then be summarized or used to trigger further action.

For example, a permission library can authorize a terminate command created by the control application if the control application's administrator determines that access to a specific application is restricted. In that case, the control application could, for example, respond by closing the application, redirecting the user to the user interface home page, turning off the device, or performing some other action that restricts the user's access. Specific applications may also be hidden by the control application at the user interface level, based on the permission setting.

Some examples follow: A detected touch of the screen can generate a touch dispatch method that can reset the inactive counter. This can be modified to detect screen touch for specific applications.

In another example, where the user tries to click the power button to shut off the screen, the logs are used to detect this. Once the "goToSleepWithReason" message is found, a wake lock can be triggered to force the screen back on.

In an example of improved control of the mobile device intended for a larger user group (e.g., for retail display),

Background services can perform a set of actions per every designated time interval (e.g., every 200 milliseconds). These actions can include, for example, incrementing the inactiveTime variable. If it hits a target such as 300 (1 minute) a broadcast can be sent off to tell the Home screen to display a set message as an inactivity warning. If it hits 600, or 2 minutes the device can be shut down.

In another example, the brightness level can be checked, and where the device brightness is not 255 (100%), the brightness is forced back. This prevents the user from manually setting the device brightness low.

In another example, volume levels are checked (ringer, media, music, notification, etc.) against preset levels and reset accordingly.

In another example, the active activity is monitored. If it matches any of the restrictions, such as Settings, Package Installer, Task Manager, Market Downloader etc, then the home screen activity is started to prevent the user from continuing.

Other improved functionality can be provided to specific applications. For example, passwords may be provided on an individual application basis by the control application, which in this example functions as a password protected administrator.

In this way, one or more *de facto* user profiles can be generated for a mobile device in order to facilitate multiple user use. For example, user #1 could access individual applications according to the username and password or passwords set up in the permissions table for each. A second user could access these based on a different username and password or passwords.

Applications that provide access, customization, and so on based on individual user settings can be provided on one device for multiple users. In the case of mobile applications such as browsers, for example, this will enable different users to each load and maintain their own individual user profiles within the specific application.

The control application can also be used to generate new or modified "launcher" applications for use at the user interface. Each new launcher can be designated with its own respective username and password. When launched the customization applies for the user across all designated settings and applications, similar to a user account profile provided on a laptop or desktop computer that functions with more processing power. This provides a more uniform user profile across designated unrestricted portions of the device.

Where internal debugging or other reports or information are monitored or library data usage reports or other summaries are generated, these can be transferred from this device to a local address, web address, or both. For transfer to a web address, the file can be accessed by URL. The data can be formatted otherwise for access from a web browser. Additional security can be arranged at the web browser to ensure additional passwords, etc.

Transfer to a local address can be provided manually, at set times, or as a continuous transfer in real time.

The transfer can be implemented with a security feature that searches for one or receiving devices with software corresponding at the local address. When the identity is confirmed, the transfer to local device can begin, either by receipt of confirmation from that device, or automatically. For example, the local device can listen for incoming pairing connections from the host device and respond accordingly.

In this way, technical information such as crash reports, etc., can be more easily and completely accessed by the local device recipient for improved response. Information may be provided by web to a software or hardware manufacturer, for example, or to a marketing or retail company for analytics.

In a local scenario, the report can be sent to a repair shop, retailer, etc., when the user provides the mobile host device in close proximity to the local receiver, here the technical support, retailer, etc.

In this example, the ability to provide local data transfer is improved because the receiving technical support machine need not, unless desired, initiate the request, set up individual wired or wireless transfer, etc. The control application can pre-load the option to provide this information automatically or on confirmation, based on established security information or not, when the devices are in a designated proximity.

The improved access to the mobile stack promotes a greater range of function available from the control application. Various functions can be implemented based on the stack information available and the actions and results desired.