Title: SECURITY FOR COMMUNICATION APPARATUS

(57) Abstract: A method of security for a communication apparatus comprises a comprehensive management system for the tagging of contacts, and the hiding of those contacts, and all communication and data related to those contacts from a user of the communications apparatus.

Fig. 3

Incoming communication

Activated

Notify user

Store record of communication

Hide communication

Allow user to reply
Security for Communication Apparatus

The present invention relates to security for communication apparatus such as mobile phones. In particular the invention relates to hiding communication, contact records and files.

In some circumstances, it is desirable to prevent access to communication apparatus so as to hide items or evidence of events, including for example communication, contact records and files. One way of doing this is to prevent access to the communication apparatus altogether. This can be achieved using, for example, user name and password access to a computer, or more simply a PIN (personal identification number) for access to a mobile phone. Another approach is to allow access to the communication apparatus, but to partition different users into different accounts so that one user does not have access to the communication information of another. In that case an administrator may have access to their own communication information as well as that of other users. However, a disadvantage of the above approaches is that when a user comes to access the communication apparatus they are made aware that they have restricted access. Furthermore, a further disadvantage is that they may be prevented from using the communication apparatus altogether.

For example, if the owner of a mobile phone wanted to arrange a surprise birthday party for her husband, she might want to enter contact details of the party venue into her phone so that she can use the phone to make the arrangements for the party. However, if her husband finds the phone, then browses through the contacts then his suspicions would be aroused if he found these contact details in the phone. However, if the owner of the phone changed her PIN number to prevent access altogether by her
husband then this would also arouse his suspicions as he would wonder why the phone was locked and he didn't know the PIN number.

Furthermore, the phone would record a log of communications such as calls made to or received from the party venue, which could be visible to her husband. The mobile phone owner is left in the position that she must either keep her phone hidden from her husband, which could itself arouse suspicions, or she would have the inconvenience of deleting the contact details and records of communication with the party venue in order to keep the party a surprise.

This problem with communication apparatus also affects anyone wanting to keep their communication with another entity and data secret from other users who have access to their communication apparatus. As well as the obvious use for hiding evidence of an affair from your partner, children have problems hiding communication with friends from their parents and people involved in confidential work have problems hiding the details of confidential communication and data from family members who need access to their phone at home.

It is an object of the present invention to hide communication and communication information from a user.

According to a first aspect of the present invention there is provided a security system for use with a communication apparatus, the security system comprising:

- a marking means for marking a contact record; and
- a selectively activatable hiding means for hiding from a user communication associated with a marked contact record and for hiding from the user marked contact records.
Preferably, the marking means is configured for marking a data item and the hiding means is configured for hiding from the user marked data items.

Preferably, the data item comprises a file.

Alternatively, the data item comprises a folder.

Preferably the hiding means is operable to prevent access by the user to the marked data item.

Preferably the hiding means is operable to prevent the presentation to the user of the communication.

Preferably the hiding means is operable to prevent access by the user to the marked contact record.

Preferably the communication comprises an incoming communication to the communication apparatus.

Preferably the communication comprises a record of communication received by the communication apparatus.

Preferably the record of communication received resides remotely from the apparatus.

Preferably the communication comprises a record of communication sent.

Preferably the security system further comprises an activating means for activating the hiding means.
Alternatively, the hiding means is activatable remotely from the security system, for example by SMS.

Preferably, UI elements of a device's operating system are suppressed. For example, a listener module can intercept system events and override the OS level handling routines with a bespoke application such as a call handler.

Preferably, an overlay graphics panel can be generated and assigned a higher priority order than the device OS event handler allowing it to come to the foreground of the display.

Preferably, a listening module can listen to key press events for a voice mail service and intercept the call out function to kill the call and playback a pre-recorded message stating that voicemail is unavailable.

Preferably, the system comprises a kernel that sits between the API stack of an operating system of the communication apparatus and the services/apps layer of the communication apparatus.

Preferably, the kernel comprises management logic for content and physical file object management; an events listener for monitoring activity such as calls, messages, emails, push data; an events handler that handles the events as passed by the events listener, and a content type handler that distinguishes the content mime type and determines the correct API methods to use to action events.

Preferably the management logic comprises a native API wrapper for accessing device features and hardware, a file system manager and a database manager.
Preferably, the system comprises a user interface, that a user sees in order to manage content, contacts, logs, messages as well as set rules for specific content.

According to a second aspect of the present invention, there is provided a computer program product carrying instructions for implementing the system of the first aspect. The computer program product can be downloaded or downloadable onto, or provided with, a communications device such as a mobile telephone, in which case communications devices that comprise the computer program product provide further aspects of the invention.

The computer program product may comprise computer readable code embodied on a computer readable recording medium. The computer readable recording medium may be any device storing or suitable for storing data in a form that can be read by a computer system, such as for example read-only memory (ROM), random-access memory (RAM), CD-ROMs, magnetic tapes, floppy disks, optical data storage devices, and carrier waves (such as data transmission through packet switched networks such as the Internet, or other networks). The computer readable recording medium can also be distributed over network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion. Also, the development of functional programs, codes, and code segments for accomplishing the present invention will be apparent to those skilled in the art to which the present disclosure pertains.

An embodiment of the present invention will be described below by way of example only in relation to the following figures in which:
Figure 1 shows a communication apparatus in accordance with the apparatus of the present invention;

Figure 2 is a flow chart showing the operation of hiding marked contact records according to the present invention;

Figure 3 illustrates a flow chart showing the hiding of incoming communication according to the present invention;

Figure 4 illustrates a further exemplary embodiment of the invention;

Figure 5 illustrates an example architecture for implementing the invention;

Figure 6 shows detail of a kernel architecture that is part of the architecture of Figure 5;

Figure 7 is a UML diagram illustrating a package structure and selected modules of an application according to one embodiment of the invention;

Figure 8 is a diagram illustrating how features of the embodiment illustrated in Figure 7 cascade down into device systems of a mobile device that runs an application embodying the invention; and

Figures 9 to 15 illustrate some exemplary screenshots of an embodiment of the invention.

With reference to Figure 1 a mobile phone 2 is shown in wireless communication with another mobile phone 4 and a voice message server 6.
The mobile phone has a display and a key pad 10. A processor 12 controls the various software modules with the display and key pad to communicate via the transceiver 14. Software modules in the phone include a contact interface 16, which allows users to display and edit contact information such as name, address, telephone number, e-mail address contact, photograph, fax number, web address and any other information related to a contact. This information is stored in contact record storage 22. This information may be input by the keypad 10 or, for example, synchronised with an external computer. The communication interface 18 allows the user to communicate with contacts. This may be done using a microphone and loudspeaker for presenting voice calls or, for example, using a display for presentation of and keypad for input of text messages (e.g. using the Short Messaging Service, SMS protocol). The communication interface also includes a notification module 20 that notifies a user of incoming communication received by the phone, for example by using the speaker to play a ring tone, or by using the display to display the contact name, and/or using a vibration unit (not shown) to notify the user. The notification module 20 can notify a user of text messages or e-mails arriving or voice messages that have been left, as well as incoming telephone calls. The communication interface 18 also presents to the user records of communication received by the phone from the contact 28, including voice messages and the like on a remote server, and records of communications sent from the phone to contacts 30.

The present invention also includes an activation module 32, a marking module 34 and a hiding module 36. Further storage 38 is provided for a table associating contact identifiers 40 with a flag 42 for marking each identifier as hidden. Although in this embodiment the table 38 is stored separately, the marking of contacts could be done in a variety of different
ways including having an additional field in the contact record storage 22 for marking a contact as hidden. This field would not be displayed unless the hiding module is inactive.

The operation of the phone in accordance with various aspects of the present invention is shown with reference to figure 2. The contact interface 16 is used by a user to enter contact details 44. The user then makes and receives calls with the contact and records of the received and sent (incoming and outgoing) communication are stored in the contact information storage 22. The user then invokes the contact marking module 34 and marks contacts 48 that he wishes to keep hidden when the hiding module 36 is activated. The marking module may be invoked by the entry into the phone using the keypad 10 of a special code. The marking module may have its own interface for selecting and marking contacts that are to be hidden. Other ways of marking contacts can be envisaged, such as invoking the marking module which causes the contact interface 16 to allow the marking of contacts that are currently being viewed as hidden.

It is to be appreciated that the steps 44, 48 are optional processes. Contacts will only be entered to the phone once, and need only be marked once. After all necessary contacts have been marked, the process will start at step 50, with the activation or deactivation of the hiding module. Of course, when a new contact is added, that contact can then be marked, and then hidden or shown depending on the activation or deactivation of the hiding module.

Subsequently, although it may not be immediately after marking the contacts, the user activates 50 the hiding module 36 by invoking the activation module 32. The activation module is invoked by the user
entering another special code using the keypad 1 0 . Importantly, the status of the hiding means is not displayed on the communication apparatus, and its presence is not displayed on the phone in the form of icons or options on menus etc. The owner of the communication apparatus needs to know the special code in order to activate or deactivate the hiding means. The codes for invoking the marking and activation modules may be chosen so that they are unlikely to be entered by accident by the user of the phone. The marking module and activation module may themselves be invoked by a separate module that monitors the keypad for entry of these special codes, or for example, the activation module might run in the background and perform that function of monitoring the keypad.

The user may enter another code to deactivate 5 0 the hiding module 3 6. In this way the hiding module may be toggled on or off by the entry of special codes. It is envisaged that the same code could be used for activation and deactivation of the hiding module or even one code could be used to enter a menu system to allow the user to select which feature such as marking, activation or deactivation is desired.

When a user comes to use the phone to access contact information 5 2, using the contact interface 1 6, the hiding module 3 6 determines 5 5 if the activation module 3 2 has activated its hiding functionality. If the hiding module 3 6 is activated, the hiding module 3 6 co-operates with the contact interface 1 6 to hide 5 6 the information of all contacts that have been marked to be hidden by the user using the marking module 3 4. In this way the hiding module 3 6 prevents the contact interface 1 6 from providing access to the marked contact records to the user. If the hiding module 3 6 is not activated, then the hiding module 3 6 allows the contact interface 1 6 to show 5 8 the information of marked contacts.
In either case whether the hiding module is activated or not, the contact interface 16 shows the information of all unmarked contacts, thus providing the user with access to the contact records in the phone.

The process of figure 2 may also apply to hiding of records of communication received from and sent to (incoming and outgoing) a contact, in addition to the hiding of the contacts themselves. In that case, instead of steps 52, 56, 58 and 59 relating to contacts, those steps relate to communication records associated with marked and unmarked contacts respectively; that is, the communication records of marked contacts are hidden. The communication records may include sent and received messages (including SMS and MMS) and e-mails, and records of sent and received calls.

The process of figure 2 may also further apply to hiding of data items such as files and/or folders. In this case, instead of steps 44, 48, 52, 56, 58 and 59 relating to just contacts, those steps also relate to other data items such as files or folders; that is, the files or folders that are associated with marked contacts are hidden.

Just as the marking module allows the marking or tagging of contact records for suppression when the hiding module is active, it also allows the tagging of files and folders. The files may be of the media or image type, but other types are also supported. When the hiding module is activated, the tagged files and folders will not show in the device's normal file browser. Thus they will only show when the application is deactivated. Whether the hiding module is activated or not, the file browser shows the information of all untagged files, thus providing the user with access to the files in the phone.
A settings screen in the marking module displays a device file browser where a user can go through their files and folders and ‘tag’ for suppression individual files or folders of files.

In this case, software modules in the phone include a file browser, which allows users to create, display and edit files, corresponding to the contact interface 16 of figure 1. This information is stored in file storage, corresponding to the contact record storage 22. The further storage 38 is in this case provided for a table associating file identifiers 40 with a flag 42 for marking each identifier as hidden.

With reference to figure 3 the operation of the present invention is described in relation to hiding incoming communication. After the contact details have been set up as per step 44 of figure 2 and contacts have been marked as per step 48 and the activation of the hiding module has been set as per step 50 of figure 2, the mobile phone receives a communication 60 from a contact. The communication may be a message, such as an SMS or MMS, an e-mail, or a voice or video telephone call. If the hiding module is activated 62, then any incoming communication associated with a marked contact is hidden 64 from a user.

If however, the hiding module is not activated then the user is notified 66 of the incoming communication, for example an incoming phone call or text message, and the user is allowed 68 to reply to the received communication by, for example, answering the phone call or sending a return text message.

The association of an incoming communication with a marked contact involves matching metadata or other information associated with the
communication with fields or other information of the contact record. For example, an incoming message will have a mobile phone number associated with it, and that number can be matched with the information in the phone's contacts. Similarly, the "from" address of an incoming e-mail or the phone number of an incoming call can be matched against the contact records.

It can be seen that for some types of communication, for example text messages, then in order to hide the communication from the user, it is only necessary to suppress notification of the received communication. It may not be necessary to actively suppress the user's ability to reply to a received text message. In fact in order to prevent the user becoming suspicious it is not envisaged that a user would be prevented from sending a message to (or phoning) any particular recipient, even a marked contact. However, the user would not be presented with the marked contact details to facilitate the sending of such a message (or making such a call). Therefore, a user could still by chance send a message to the originator of a received hidden communication after the communication is received. In that case, however, the outgoing message would not in fact be a reply to the incoming hidden communication because the user would not have any knowledge or visibility of the incoming communication.

In either case, whether or not the hiding module is activated, the record of the incoming communication is stored. However, this record of the communication will not be visible to the user while the hiding module is activated.

The hiding module may also suppress both the mobile internet browser history and any emails received from a tagged/marked contact.
The present invention may be implemented on mobile phones or home telephones. It may also be implemented in other communication devices such as desktop computers, laptops or servers hosting applications over the internet for example.

A typical implementation will be a software computer program implemented on a mobile phone. This software enhances the functionality of existing software on a mobile phone. The user is able to activate and deactivate the software whenever he chooses. The function of the software enables the user to decide when and which contact's call, text message, voice message, e-mail or any other information to receive.

It can be seen from figure 2 that the user can mark the contact in his or her mobile phone address book. If the software has been activated, the marked contact's information (see figure 2) and incoming communications (see figure 3) will not be accessible and will also not show on the mobile phone. However, if the software has not been activated the marked contact's information and communication will be accessible and will show on the mobile phone.

The hiding module may be activated remotely. For example, if the owner of a mobile phone forgets the phone and leaves it at home and does not have the software activated, he or she can remotely activate the software using a remote activation signal. This can be performed directly from another mobile phone (e.g. phone 4 in figure 1) by the sending of a special text message to the user's mobile phone. Alternatively a website might be used to configure a server to send a special text message to the users phone. In that case a component of the activation module may be running all the time on the mobile phone so that it screens incoming texts and checking each one to see if it is a special activation message. If it is not
then it is passed on to communication interface 18 and treated normally by the phone. However, if it is a special activation message, then the hiding module 36 is activated (step 50 in figure 2).

In order to access voice messages on the voice message service 6 a user typically dials the voice message service provider's number to retrieve all voice messages. The hiding module cannot influence what information is stored on the voice message service 6. However the hiding module when activated can intercept call outs to a voicemail service, either by identifying the number that is being dialled or by detection of other call signatures, and then diverting the call to a service that plays a pre-recorded message saying the voicemail service is currently unavailable.

In use of the present invention, if the user has sent or received any communication with a marked contact, on the activation of the hiding module the history of any communication to or from the marked contact will be hidden while the hiding module 36 has been activated. In addition all details of the marked contact will be hidden while the hiding module is activated.

If anyone takes the mobile phone and looks through it using the contact interface 16, it will not be obvious that the present invention is operating. When the hiding module is activated the marked contact's information is not lost, but stored in a hidden storage area. While the hiding module 36 is activated, if one of the marked contacts attempt to communicate with the mobile phone in any format, then that information or communication will also be stored in the hidden storage area. While the hiding module 36 is activated that mobile phone does not indicate or notify that any such information or communication has been received. However, when the user deactivates the hiding module all communication and information that
he or she has received, as well as any history that has not yet been
deleted will reappear. This includes any communication sent to the user
by one of the marked contacts while the hiding module has been
activated. Therefore any communication sent by a marked contact while
the hiding module is activated is not lost, but is stored and only accessible
when the hiding module has been deactivated.

The invention can also be understood from a different aspect, as shown in
Figure 4. Various operational components of a mobile phone's
architecture are schematically illustrated. The hiding means can be
thought of as being functionally equivalent to a firewall, in that limited
access is granted to files, folders, communication requests, contact
information and phone logs. The "firewall" sits between the
contacts/address book and the mobile phones operating system/software,
and grants limited access to, in this example, the call history, voice
messages, text messages, e-mails, faxes and web browsing information
that are stored on the phone. On the other hand, when the hiding means
is deactivated, full access as normal is granted to all these features. It will
be appreciated that this list of features is not exhaustive and does not limit
the scope of protection.

An architectural view of the invention is shown in Figure 5. The
application comprises a user interface (UI) 500 and kernel 502 which sits
in between the device OS (504) API Stack 506 and Services/Apps Layer
508 comprising in this embodiment SMS 510, Calls 512, Email 514,
Contacts 516).

The device OS can for example be any mobile device OS, including for
example and without limitation, Symbian, Maemo, Android, Windows
Mobile, Blackberry OS, iPhone OS, Palm Web OS, and any other Linux or Unix based systems.

The UI 500 is the front end application that users see in order to manage content, contacts, logs, messages as well as set rules for specific content, while the kernel 502 is the primary controller that takes over the system events and message handler and uses management logic to control the environment and flow of data in and out of the device. The application UI 500 and kernel 502 together provide a unified events manager that can override the device’s normal manner of operation and allow custom rules to be defined for handling content and services on the device for incoming and outgoing activity.

The arrows shown between SMS, call and e-mail modules 510, 512, 514 and the kernel 502 represent services data flow, being the flow of data between services and kernel 502. If the kernel 502 is inactive then the services flow will bypass the kernel 502 and travel directly to the native API layer 506.

Similarly, the arrow between contacts module 516 and the kernel 502 represent contacts data flow, being the flow of data between address book and kernel 502 when the kernel 502 is active. The bidirectional flow of data represents communication between the kernel 502 and the contacts app and is used primarily to filter content and services for tagged contacts.

The arrows between the kernel 502 and the native API layer 506 represent kernel instruction data flow, being instruction/commands directed from kernel 502 to the Native API layer 506 to perform action based on the event handler (602 in figure 6) response deduced by the kernel 502.
The kernel 502 is designed to register itself and override the underlying Event listener and handler of the OS with the one that is implemented in it. A diagram of the kernel 502 is provided in Figure 6. It includes several layers. The bottom layer comprises management logic for content and physical file object management. The management modules in this layer comprise a native API wrapper 606 that is the interface of the kernel 502 to the underlying native API layer (506 in Figure 5) for accessing device features and hardware, including data and resources. Other management modules comprise a file system manager 608 and database manager 610. Each management module includes logic for housekeeping and organisation of data in a normalised and relational manner to keep performance fast and efficient.

The other layers comprise an events listener 600 which is constantly monitoring activity such as calls, messages, emails, push data; an events handler 602 that handles the events as passed by the events listener 600, and a content type handler 604 that distinguishes the content mime type and determines the correct API methods to use to action the event/task.

The kernel 502 provides a universal management system that allows a single action to translate into a series of check, block and administration of content and services on the device. As an example, the tagging of a contact leads to a cascade of management actions like listening to calls, SMS, email, Voice mail so that it is no longer a concern of the native management system but becomes the priority of the kernel 502.

The present invention is a universal management system providing a new combination of capabilities. Through the simple marking of a contact, a cascade of management actions occurs so that all the information relating
to that contact can then be hidden - including all forms of communication and all files and folders.

In a preferred embodiment, the architecture of the application is modular in design using strict design patterns and object oriented structure to allow features and functionality to be plugged in or removed as required. The UML diagram in Figure 5 illustrates the main classes and methods that can form the structure for the application. These are labelled with names that reflect the various functions of each class.

An example embodiment will now be described. The application can be targeted to run on various operating systems, including for example the Symbian Series 60 OS as seen in most Nokia phones. The open nature of that OS allows such an application to be developed by third parties but issues like suppressing the UI elements triggered by incoming events like phone call, SMS, etc required technical workaround. A part of the technical overview is the feature cascade aspect of the application logic. Figure 6 describes how the features of the present invention cascade down into the device systems. In the diagram, the “CallJuggler DB” refers to the database of data relating to hidden contacts.

Series 60 mobile operating system has low level API for handling calls, messages, emails etc. The application uses a listener to intercept such system events and override the OS level handling routines with a bespoke code handler.

In the event of a call or an SMS the OS displays a dialog notifying the phone owner of a new call or SMS along with an audible ringer or beep. The ringer or beep can be suppressed using device level API however the visual display of the SMS or the caller cannot be suppressed or hidden
using the base API. This can be overcome by using an overlay graphics panel that is assigned a priority order higher than the OS event handler allowing it to come to the foreground masking any OS dialogs. This allows the caller number or contact detail and body of the message to be hidden from view.

Voice mail is a network specific feature and provided as a means by which a caller can leave a voice message in case the person on the other end is non reachable. The solution uses a redirect to a voice box number service where recorded messages can be played back, for example stating that the voicemail service is currently unavailable. Thus, voice mail messages are not accessible to the listener when the application is in active mode.

The technique used to achieve this feature utilises code to listen to key press events for the voice mail service and intercept the call out function on the make call key event to kill the call and playback pre-recorded message stating that voice mail service is not available.

Figures 9 to 15 illustrate some exemplary screenshots of an embodiment of the invention, where the application is referred to as "CallJuggler". Figure 9 shows a main settings screen, which can be presented once the application is launched, for example by entry of the special code via the keypad of the mobile device. The main settings screen acts as the main control panel of the application, and also enables the viewing of logs of messages, calls and emails sent by tagged contacts when the application is in active state. Selecting Exit asks user to let application run in background. In the screen shown, the "CallJuggler" option lets the application be switched on or off. When switched on, all tagged contacts, and all previous logs and messages related to those tagged contacts, are removed and stored in a separate storage area of the device. These logs,
messages and contacts are restored when the application is switched back off.

By selecting the "messages" option, the application takes a user to a screen where he can view the text messages received by tagged contacts. By selecting the "Call Details" option, the application takes a user to the screen where he can view missed calls, received calls and also dialled calls related to tagged contacts. By selecting the "Emails" option, the application takes a user to a screen where he can see all emails sent by tagged contacts. By selecting the "Tag/UnTag Media Files" option, the application takes the user to a File Browser where he can select media files including images, audio and video files to hide them or restore them.

Pressing the menu button on the screen of Figure 9 opens a menu on the screen, as illustrated in Figure 10. This menu gives access to options for Tag/UnTag contacts, set voicemail number, change the special code for accessing the application, setting an autostart function for remote activation of the application, entering a help menu, and displaying information about the application.

Figure 11 shows a screen that is displayed when the "call details" option of the screen of Figure 9 is selected. Call logs are opened, which contain history of missed, dialled, and received calls related to your tagged contacts.

Figure 12 shows a screen that is displayed when the "Tag/UnTag Contacts" option of the screen of Figure 10 is selected, in the case where no contact is yet tagged. The screen shows a label instructing the user to "please tag contacts". By selecting the Options command on this screen, a menu can be opened showing options for adding or for restoring
contacts. Selecting the "Add Contacts" command opens address book of the application, as for example shown in Figure 13. The user can then select one or more contacts to add them to tagged contacts list. Selecting the OK command adds selected contacts to the tagged contacts list and takes user to the tagged contact screen. Pressing cancel on Address Book screen takes user back to tagged contacts screen.

Figure 14 shows a screen that is displayed when the "E-mails" option is selected from the screen of Figure 9. This screen shows list of emails received from or sent to tagged contacts. The menu on this screen comprises two options: "View Email" and "Restore Email". Selecting "View Email" command opens the selected email and shows its contents. Selecting "Restore Email" restores email to the respective email folder.

The e-mail viewing screen is shown in Figure 15. There are two commands available. Selecting the "Attachments" command opens list of attachments associated with the email. Selecting the "Back" command takes user to email list view screen.

When the Tag/Untag Media Files option is selected from the main screen shown in Figure 9, if there is no file selected then a label saying "Please tag files" is shown on the next screen. Options to add or restore files can be displayed in an options menu. By selecting "Add Files", the application can open a file browser so that a user can select one or more files and tag them.

As mentioned above, the invention is applicable to any operating system, and in particular can be embodied in any mobile device operating system. However, from an outside developer's perspective, some operating systems are open and some are closed, that is, access to the low level
APIs required to modify message and call handling are in some operating systems not able to be modified by anyone outside of the organisation that owns the operating system. Examples of operating systems that are closed for the purposes of this invention are the iPhone OS and the Blackberry OS. There are however ways in which the invention can be realised by an outside developer even for a closed OS. In particular, when an SMS API is closed, the application can provide a full messaging service that sits on top of the native messaging service.

Improvements and modifications may be incorporated herein without deviating from the scope of the invention.
CLAIMS

1. A security system for use with a communication apparatus, the security system comprising:
   - a marking means for marking a contact record; and
   - a selectively activatable hiding means for hiding from a user communication associated with a marked contact record and for hiding from the user marked contact records.

2. The system of claim 1, wherein the marking means is configured for marking a data item and the hiding means is configured for hiding from the user marked data items.

3. The system of claim 1 or claim 2, wherein the data item comprises a file.

4. The system of claim 1 or claim 2, wherein the data item comprises a folder.

5. The system of any of claims 2 to 4, wherein the hiding means is operable to prevent access by the user to the marked data item.

6. The system of any preceding claim, wherein the hiding means is operable to prevent the presentation to the user of the communication.

7. The system of any preceding claim, wherein the hiding means is operable to prevent access by the user to the marked contact record.

8. The system of any preceding claim, wherein the communication comprises an incoming communication to the communication apparatus.
9. The system of any preceding claim, wherein the communication comprises a record of communication received by the communication apparatus.

10. The system of claim 9, wherein the record of communication received resides remotely from the apparatus.

11. The system of any preceding claim, wherein the communication comprises a record of communication sent.

12. The system of any preceding claim, wherein the security system further comprises an activating means for activating the hiding means.

13. The system of any of claims 1 to 11, wherein, the hiding means is activatable remotely from the security system, for example by SMS.

14. The system of any preceding claim, wherein, UI elements of a devices operating system are suppressed.

15. The system of claim 14, wherein a listener module can intercept system events and override the OS level handling routines with a bespoke application such as a call handler.

16. The system of any preceding claim, wherein an overlay graphics panel is generated and assigned a higher priority order than the device OS event handler allowing it to come to the foreground of the display.

17. The system of any preceding claim, wherein a listening module can listen to key press events for a voice mail service and intercept the call out
function to kill the call and playback a pre-recorded message stating that voicemail is unavailable.

18. The system of any preceding claim, comprising a kernel that sits between the API stack of an operating system of the communication apparatus and the services/apps layer of the communication apparatus.

19. The system of claim 18, wherein the kernel comprises management logic for content and physical file object management; an events listener for monitoring activity such as calls, messages, emails, push data; an events handler that handles the events as passed by the events listener, and a content type handler that distinguishes the content mime type and determines the correct API methods to use to action events.

20. The system of claim 19, wherein the management logic comprises a native API wrapper for accessing device features and hardware, a file system manager and a database manager.

21. The system of any of claims 18 to 20, comprising a user interface, that a user sees in order to manage content, contacts, logs, messages as well as set rules for specific content

22. A computer program product carrying instructions for implementing the system of any of claims 1 to 21.

23. A communications apparatus comprising the computer program product of claim 22.
Enter contact details

Mark contact

Activate / Deactivate

Access contact information

Activated?

Y

Show marked contacts

N

Hide marked contacts

Show unmarked contacts
Incoming communication

Activated?

Y

Notify user

N

Hide communication

Allow user to reply

Store record of communication

Fig. 3
Fig. 4
Please tag Contacts

Options  Back

Fig. 12

Address Book

- Calljuggler Contact 1
- Calljuggler Contact 2
- Zohid Mohammad
- Zohid Mohammad

Ok  Cancel

Fig. 13
**Fig. 14**

From: jeozahidi@localhost.com  
Subject: This is a test email from Calljuggler  
Date: Mon Mar 08 12:03:30 GMT 2010  

hi

**Fig. 15**
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

INV.

H04M1/66  
G06F21/00  
H04M1/2745

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC.

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

H04M  
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched.

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 2008/022758 A1 (NOKIA CORP [FI]; KRAFT CHRISTIAN [DK]; NIELSEN PETER DAM [DK]; OLESEN) 28 February 2008 (2008-02-28) page 2, line 7 - line 11 page 10, line 29 - page 15, line 26 claim 26 figures 1-9</td>
<td>1-23</td>
</tr>
</tbody>
</table>

**D**

Further documents are listed in the continuation of Box C

**X** See patent family annex

**Special categories of cited documents**

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on the novelty claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"A" document member of the same patent family

Date of the actual completion of the international search

5 August 2010

Date of mailing of the international search report

12/08/2010

Name and mailing address of the ISA/

European Patent Office, P B 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Fax (+31-70) 340-3016

Authorized officer

Pini Ila-Ari za, D
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WO 2008022758 A1</td>
<td>28-02-2008</td>
<td>CN 101507246 A</td>
<td>12-08-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2064860 A1</td>
<td>03-06-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2008051072 A1</td>
<td>28-02-2008</td>
</tr>
<tr>
<td>US 2006104445 A1</td>
<td>18-05-2006</td>
<td>NONE</td>
<td></td>
</tr>
</tbody>
</table>