

SECURITY FOR MOBILE COMMUNICATIONS DEVICE

BACKGROUND OF THE INVENTION

[0001] The present invention relates to mobile communications.

[0002] As a result of their mobility, mobile communications devices are sometimes lost or stolen. Frequently, the loss of the information stored on a missing device is of greater concern than the loss of the device itself. For example, the device may have sensitive and/or confidential information stored on it that could cause harm if acquired by others. Such sensitive information could include, among other things, stored messages of a confidential nature, and stored communications information that would allow a third party to masquerade electronically as the person to whom the mobile device rightfully belongs.

[0003] In some mobile communications networks, once a user discovers that his or her mobile device is missing, he or she can contact the network operator and request that a "kill packet" be sent to the missing mobile device instructing the device to wipe sensitive information from its memory. However, such a system requires that the user realize that the mobile device is missing, and that the mobile device be in communication with the network. If the user relies on the device for communication, they may be unable to report it missing or stolen in a timely manner.

[0004] Thus, security for mobile communications devices is a concern.

SUMMARY OF THE INVENTION

[0005] According to an example embodiment of the invention, there is provided a mobile communications device for communicating with a wireless network. The mobile communications device includes an electronic storage having data stored thereon, a processor connected to the storage for accessing the data, a communications sub-system connected to the processor for exchanging signals with the wireless network and with the processor, a user input interface connected to send user input signals to the processor in response to user action, and a security module associated with the processor for detecting a trigger condition and automatically taking a security action if a user bypass action is not detected after detection of the trigger condition.

[0006] According to another example embodiment of the invention, there is provided a method for providing security for a mobile communication device that is configured to communicate over a wireless communications network, including steps of: (a) monitoring for a trigger condition; (b) subsequent to occurrence of the trigger condition, monitoring for a user bypass action at the mobile communication device; and (b) upon failure to detect the user bypass action after occurrence of the predetermined condition, automatically taking action to protect data stored on the mobile communication device.

[0007] Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Embodiments of the present invention will now be described, by way of example only, with reference to the attached Figures, wherein:

[0009] Figure 1 is a block diagram showing a communications system including a mobile communications device to which the present invention may be applied;

[0010] Figure 2 is a flow diagram of a security process according to embodiments of the invention.

[0011] Like reference numerals are used throughout the Figures to denote similar elements and features.

DETAILED DESCRIPTION

[0012] Referring now to the drawings, Figure 1 is a block diagram of a mobile communication device 10 to which the present invention is applied in an example embodiment. The mobile communication device 10 is a two-way communication device having at least data and preferably also voice communication capabilities. The device preferably has the capability to communicate with other computer systems on the Internet. Depending on the functionality provided by the device, in various embodiments the device may be a data communication device, a multiple-mode communication device

configured for both data and voice communication, a mobile telephone, a PDA (personal digital assistant) enabled for wireless communication, or a computer system with a wireless modem, among other things.

[0013] The device includes a communication subsystem 11, including a receiver 12, a transmitter 14, and associated components such as one or more, preferably embedded or internal, antenna elements 16 and 18, local oscillators (LOs) 13, and a processing module such as a digital signal processor (DSP) 20. As will be apparent to those skilled in the field of communications, the particular design of the communication subsystem 11 will be dependent upon the communication network in which the device is intended to operate.

[0014] Signals received by the antenna 16 through a wireless communication network 50 are input to the receiver 12, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection and the like, and in some embodiments, analog to digital conversion. In a similar manner, signals to be transmitted are processed, including modulation and encoding for example, by the DSP 20 and input to the transmitter 14 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission over the communications network 50 via the antenna 18. In certain device embodiments, the antenna 16 and the antenna 18 may be the same antenna while other embodiments will include two separate antenna systems for a receiver antenna and a transmitter antenna.

[0015] The device 10 includes a microprocessor 38 that controls the overall operation of the device. The microprocessor 38 interacts with communications subsystem 11 and also interacts with further device subsystems such as the display 22, flash memory 24, random access memory (RAM) 26, auxiliary input/output (I/O) subsystems 28, serial port 30, keyboard or keypad 32, speaker 34, microphone 36, a short-range communications subsystem 40, and any other device subsystems generally designated as 42.

[0016] Some of the subsystems shown in Figure 1 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 32 and

display 22 for example, may be used for both communication-related functions, such as entering a text message for transmission over a communication network, and device-resident functions such as a calculator or task list.

[0017] Operating system software 54 and various software applications 58 used by the microprocessor 38 are, in one example embodiment, stored in a persistent store such as flash memory 24 or similar storage element. Those skilled in the art will appreciate that the operating system 54, specific device applications 58, or parts thereof, may be temporarily loaded into a volatile store such as RAM 26. It is contemplated that received communication signals may also be stored to RAM 26.

[0018] The microprocessor 38, in addition to its operating system functions, preferably enables execution of software applications 58 on the device. A predetermined set of applications 58 which control basic device operations, including at least data and voice communication applications for example, will normally be installed on the device 10 during manufacture. Further applications may also be loaded onto the device 10 through the network 50, an auxiliary I/O subsystem 28, serial port 30, short-range communications subsystem 40 or any other suitable subsystem 42, and installed by a user in the RAM 26 or a non-volatile store for execution by the microprocessor 38. Such flexibility in application installation increases the functionality of the device and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the device 10.

[0019] In a data communication mode, a received signal such as a text message or web page download will be processed by the communication subsystem 11 and input to the microprocessor 38, which will preferably further process the received signal for output to the display 22, or alternatively to an auxiliary I/O device 28. A user of device 10 may also compose data items such as email messages for example, using the keyboard 32 in conjunction with the display 22 and possibly an auxiliary I/O device 28. Such composed

items may then be transmitted over a communication network through the communication subsystem 11.

[0020] The serial port 30 in Figure 1 would normally be implemented in a personal digital assistant (PDA)-type communication device for which synchronization with a user's desktop computer (not shown) may be desirable, but is an optional device component. Such a port 30 would enable a user to set preferences through an external device or software application and would extend the capabilities of the device by providing for information or software downloads to the device 10 other than through a wireless communication network.

[0021] A short-range communications subsystem 40 is a further component which may provide for communication between the device 10 and different systems or devices, which need not necessarily be similar devices. For example, the subsystem 40 may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. The device 10 may be a handheld device.

[0022] In an example embodiment, wireless gateway 62 is adapted to route data packets received from a mobile communication device 10 over wireless mobile network 50 to a destination electronic mail messaging or Internet access server 68 through a wireless connector system 64, and to route data packets received from the server 68 through the wireless connector system 64 over the wireless mobile network 50 to a destination mobile communications device. Wireless mobile network 50 is, in an example embodiment, a wireless packet data network, (e.g. Mobitex™ or DataTAC™), which provides radio coverage to mobile devices 10, although it could be any other types of wireless networks. Depending on the type of wireless network 50, it may be necessary to route data packets between a TCP wireless gateway 62 connection and an X.25 or IP address mobile network connection and vice versa using an intermediary routing mechanism that provides TCP clients access to an X.25 connection. As is conventionally known, such a wireless mechanism could use, among other things, NET ID (DataTAC) or FST MAN (Mobitex) to connect to wireless mobile network 50.

[0023] Wireless gateway 62 forms a connection or bridge between the servers and wireless networks associated with wireless e-mail communication and/or Internet access. Specifically, wireless gateway 62 is coupled between wireless network 50 and the hardwired data network that includes wireless connector system 64 and destination electronic mail server 68. In an example embodiment, the wireless gateway 62 stores system configuration information, system state data, and tables that store mobile device 10 information, and also includes wireless transport modules that interface between mobile devices 10 and wireless gateway 62. The wireless transport module communicates with wireless mobile network 50 using the intermediary routing mechanism discussed above (that provides TCP clients access to an X.25 or UDP connection) and assembles data packets being received from mobile device 10 over wireless mobile network 50. Once data packets are assembled, they are sent to the upper layer of the wireless transport module for processing through wireless gateway 62 to wireless connection system 64 and eventually to destination electronic mail server 68. Wireless connector system 64 is part of the wired, backbone network and is coupled to wireless gateway 62. Wireless connector system 64 communicates with wireless gateway 62 and each electronic message server that connects to wireless gateway as a unique address. Mail server 68 is coupled to wireless connector system 64 and, in one embodiment, is a conventional electronic mail server.

[0024] The mobile device 10 stores service data 60 and other data 64 in an erasable persistent memory, which in one example embodiment is flash memory 24. In various embodiments, the service data 60 includes the information required by the mobile device to establish and maintain communications with the wireless communications network 50 (wireless network service data) and the wireless gateway 62 (gateway service data). Other data 64 may include, among other things, user application data such as email messages, address book and contact information, calendar and schedule information, notepad documents, image files, and other commonly stored user information stored on the device 10 by its user. Other data 64 may also include data required for the communications layers managed by the wireless connector system 64 and servers 68.

[0025] In order to provide security for a lost or stolen mobile device 10, the device 10 includes a security module 56, which in one example embodiment is a software component that is part of the operating system 54. In other embodiments, the security module 56 is, or is part of, a specialized software application 58 separate from the operating system 54. The security module 56 includes instructions for configuring the microprocessor 38 to cause the device 10 to carry out security process 200 that is shown in Figure 2. The security process 200 is in effect a “deadman’s” switch in that it configures the device to, upon the occurrence of one or more predetermined trigger conditions, require a user to take a predetermined user bypass or override action, failing which the mobile device 10 will automatically take active security measures.

[0026] In an example embodiment, the security process 200 is active whenever the mobile device 10 is on. As indicated in step 204, the process 200 includes a step 204 of checking to see if one or more predetermined trigger conditions have occurred. Such checking step is periodically carried out until a triggering event occurs. In one example embodiment, a trigger event occurs when the mobile device 10 has been out of communication with wireless network 50 for a predetermined time duration. As indicated in step 206, upon occurrence of a trigger event, the device 10 prompts the user to take bypass action (step 206) – for example, in one example embodiment, the device 10 prompts the user to enter a password or other shared secret through keyboard 32 or, in a device 10 having voice recognition abilities, through microphone 36. In various embodiments, the device 10 prompts the user to take other actions or combinations of actions in addition to or in place of inputting a password or other shared secret, such as, by way of non limiting examples, prompting a user to swipe a card carrying identifying information through a card reader attached to the device 10; and/or prompting the user to move the device so that it re-establishes communications with wireless network 50. In some embodiments, the device 10 skips step 206 and does not actively prompt the user to take a required action, but rather just expects the required action to be taken after the trigger event has occurred.

[0027] As indicated in step 208, subsequent to occurrence of a trigger event and after prompting the user to act (in embodiments where a prompt is issued), the device 10 then determines if the required action is taken. In various example embodiments, the required bypass action must be successfully completed within a predetermined time duration (eg. within a "fuse" time) subsequent to the occurrence of the trigger event, and/or within a predetermined number of attempts at the action (for example, within three attempts to enter a password), otherwise the device 10 will proceed to take precautionary security measures. In one embodiment, the security module 56 causes the device 10 to temporarily suspend all or selected communications functions and become effectively non-operational during the fuse time, refusing all attempted user actions other than the bypass action. Thus, during the fuse time the user has no option other than to take the required bypass action, and cannot access data stored on the device or make telephone calls (in phone enabled devices) or send e-mails (in e-mail enabled devices), for example. In some telephone enabled embodiments, 911 calls may be permitted during the fuse time. In alternative embodiments, normal functionality may be fully maintained during the fuse time. If the required bypass action is successfully taken within the fuse time, device functionality is restored, and the security process returns to monitoring for the next trigger event (step 204).

[0028] Turning now to step 210, in the event that the required bypass action is not successfully taken by the user in step 208 within the predetermined fuse time or attempt limit, the device 10 automatically undertakes information protection measures. In one embodiment, the device 10, in order to protect the data stored on device 10 from falling into the wrong hands or being used without authorization, the security module 56 erases or wipes all or selected parts of the service data 60 that is stored in the device's 10 persistent and volatile storage. In one example embodiment, service data 60 required to establish and maintain communication between the device 10 and wireless network 50 is permanently erased, effectively disabling the communications ability of the mobile device 10. In some embodiments where the device includes a wireless phone, 911 emergency service may be exclusively

maintained. The service data required to establish and maintain communications through the wireless gateway 62 is, in various embodiments, also or alternatively deleted. In various embodiments, in addition to or instead of service data 60, selected portions of all of the other data 64 on the mobile device 10, including the user data such as e-mail messages, contact and address book lists, calendar and scheduling information, notepad documents, image and text files and/or other user information is permanently erased from the storage of mobile device 10. Thus, in step 210, in various embodiments, information required by the device 10 to function as a communications device is deleted, and any text or other information that may be confidential to the user is deleted, thereby removing, among other things, information from the device 10 that could be used by others to electronically impersonate the authorised user of the device 10. In various embodiments, the data protection security action taken in step 210 includes encrypting all or selected portions of the service data and/or other data, rendering such data temporarily unusable, instead of deleting it. In such embodiments, the device 10 has a locally installed encryption engine, and an encryption key stored in the persistent memory of the device is used for the encryption. During or after the encryption process, the encryption key is either deleted or encrypted to protect it. Once encrypted, a decryption key must be obtained from a secure third party source (for example, the operator of the wireless network 50 and/or the wireless gateway 62) to decrypt the data.

[0029] In various embodiments, other predetermined trigger conditions are trigger events in step 204. For example, in one embodiment, variation in user input from a predetermined threshold, such as lack of keyboard activity for a predetermined duration, is used to trigger the requirement for user action, failing which information protection measures are taken. In some embodiments, trigger conditions can be based on changes in communications, messaging or usage characteristics or patterns of the device 10. For example a trigger condition could result when volume of data packets sent or received by the device over the wireless network traffic exceeded a predetermined threshold, or when the pattern of base stations used in communications varied from predetermined thresholds. A trigger condition

could result if the device went outside of a predetermined coverage area. In some embodiments, the thresholds for determining trigger conditions could be adaptively configured by the security module based on normal operating characteristics of the device 10.

[0030] The above-described embodiments of the present invention are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those skilled in the art without departing from the scope of the invention, which is defined by the claims appended hereto.

WHAT IS CLAIMED IS:

1. A mobile communications device for communicating with a wireless network, comprising:
 - an electronic storage having data stored thereon;
 - a processor connected to the storage for accessing the data;
 - a communications sub-system connected to the processor for exchanging signals with the wireless network and with the processor;
 - a user input interface connected to send user input signals to the processor in response to user action; and
 - a security module associated with the processor for detecting a trigger condition, monitoring, after the trigger condition has been detected, to detect if a secret shared by the user and the mobile communications device is entered through the user input interface within a predetermined duration after detection of the trigger condition, and if entry of the shared secret is not detected within the predetermined duration, automatically taking a security action to encrypt or erase at least some of the data stored on the electronic storage.
2. The mobile communications device of claim 1 wherein the security action includes erasing all or selected data from the storage to protect the data.
3. The mobile communications device of claim 1 wherein the security action includes encrypting all or selected data from the storage to protect the data.
4. The mobile communications device of claim 1 wherein the data includes service data required by the mobile device to successfully communicate over the wireless network and the security action includes erasing the service data from the storage.
5. The mobile communications device of claim 1 wherein the security action includes disabling an ability of the device to communicate with the wireless network.

6. The mobile device of claim 1 wherein the trigger condition includes a variance from a predetermined threshold in a communications characteristic between the device and the wireless network.
7. The mobile device of claim 6 wherein the communications characteristic includes a messaging traffic pattern between the device and the wireless network.
8. The mobile communications device of claim 1 wherein the trigger condition includes a lack of communication by the device with the wireless network for a predetermined time duration.
9. The mobile communications device of claim 1 wherein the trigger condition includes a variance in the use of the user input interface from a predetermined threshold.
10. The mobile communications device of claim 9 wherein the user input interface includes a keyboard or keypad and the trigger condition includes inactivity of the user input interface for a predetermined duration.
11. The mobile communications device of claim 1 wherein after detecting the trigger condition and while monitoring for entry of the shared secret, the security module is operative to encrypt or erase the at least some of the data if entry of the shared secret is not detected within a predetermined number of attempts by the user to enter the shared secret.
12. The mobile communications device of claim 1 wherein the device includes a user output device for issuing a prompt for action to the user, the security module causing the prompt to be issued upon detection of the trigger condition.
13. A method of providing security for a mobile communication device that is configured to communicate over a wireless communications network, including steps of:
 - (a) monitoring for a trigger condition;
 - (b) subsequent to occurrence of the trigger condition, monitoring to

detect if a secret shared by the mobile communications device and the user is entered through a user input interface of the mobile communications device within a predetermined duration after the occurrence of the trigger condition; and

(c) if user entry of the shared secret is not detected within a the predetermined time duration after occurrence of the trigger condition, automatically taking security action to erase or encrypt data stored on the mobile communication device.

14. The method of claim 13 wherein the data stored on the mobile communication device includes service data required by the mobile communication device to communicate over the wireless communications network, the security action including permanently erasing the service data stored on the mobile communication device.

15. The method of claim 13 wherein the security action includes encrypting at least some of the data stored on the mobile communication device.

16. The method of claim 13 wherein the trigger condition includes a lack of communications between the communication device and the wireless communications network for a predetermined time duration.

17. The method of claim 13 including a step of prompting the user to take action upon occurrence of the trigger condition.

18. The method of claim 13 including monitoring a number of user attempts to enter the shared secret in step (c) and taking the security action if the shared secret is not successfully entered within a predetermined number of attempts.

19. The method of claim 13 wherein at least some communications functions of the device are suspended during the predetermined time duration.

20. A computer program product including a computer readable medium carrying computer program code means for providing security for a mobile communication device that is configured to communicate over a wireless

communications network, the computer program code means including means for:

- (a) monitoring for a trigger condition;
- (b) subsequent to occurrence of the trigger condition, monitoring to detect if a secret shared by the mobile communications device and the user is entered through a user input interface of the mobile communications device within a predetermined duration after the occurrence of the trigger condition; and
- (c) if user entry of the shared secret is not detected within the predetermined time duration after occurrence of the trigger condition, automatically taking security action to erase or encrypt data stored on the mobile communication device.

21. The product of claim 20 wherein the computer readable medium is selected from a physical medium and a transmitted signal.