

SECURITY MANAGEMENT SERVICE

Field of the Invention

[0001] The present invention relates to mobile device security. In particular, the invention relates to a system and method for securing a mobile communication device.

Background

[0002] Mobile communication devices, such as a mobile phone, have since become the most widely spread technology and the most common gadget in the world. Along with the technology advancements, one single mobile communication device is now able to provide a wide range of applications that reduces significantly the amount of items to be carried by users. As the mobile communication device becomes more powerful in features, users rely heavily on the mobile communication device for storing and communicating personal data and private and confidential information.

[0003] Therefore, it is important that the information stored on or transmitted through the mobile communication device is properly protected to ensure the confidentiality, integrity, and the availability of personal information.

Summary

[0004] In accordance with one aspect, the present invention provides a secure communication manager for securing a mobile communication device from unauthorized access of applications, data and hardware residing on the mobile communication device. The secure communication manager comprises a plurality of secure services adapted to operationally monitor and control of access and execution of the applications and data; a plurality of drivers operable to interface the hardware with the secure communication manager; a secure core operable to handle and manage the secure services and drivers to detect for any unauthorized access of the applications, data and hardware, the secure core is operable to detect the unauthorized access based on security requirements and restrictions defined by the secure services and drivers.

The secure communication manager resides and operates at a operating system layer of the mobile communication device.

[0005] In one embodiment, the secure communication manager resides and operates at the operating system layer as a service.

[0006] In another embodiment, the plurality of secure services include a secure data service for managing data access and transmission, a secure multimedia service for managing voice communication and a secure access validation service for validating access and execution of applications and data of the mobile communication device. The secure data service may be operable to handle data security, wherein the data includes text data and multimedia data. It is also possible that the secure multimedia service is adapted to operationally encrypt/decrypt and encode/decode the multimedia data. Yet, the secure access validation service may be operable to control accessibilities of the applications and data, of which, the accessibilities include local access and remote access, wherein the secure access validation service denies access when a validation fails. The validation may include PIN code access, biometric verification and face recognitions. The secure access validation service may also be adapted to provide validation for accessing a wireless communication module of the mobile communication device. The mobile communication device may comprise one or more wireless communication module.

[0007] In a further embodiment, the drivers include a secure algorithm driver for driving a secure algorithm operable to facilitate security processing.

[0008] In yet another embodiment, the drivers include an audio/codec driver and a camera driver.

Brief Description of the Drawings

[0009] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0010] **FIG. 1** illustrates a block diagram showing architecture of a secured mobile communication device in accordance with one embodiment of the present invention; and

[0011] **FIG. 2** illustrates a block diagram of a security service of a mobile communication device in accordance with one embodiment of the present invention.

Detailed Description

[0012] In line with the above summary, the following description of a number of specific and alternative embodiments are 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.

[0013] **FIG. 1** illustrates a block diagram showing architecture of a secure mobile communication device **100** in accordance with one embodiment of the present invention. The architecture of the secure mobile communication device **100** can generally be presented in three layers: a low-level layer **110**, an operating system (OS) layer **120** and a high-level layer **130**. The low-level layer **110** includes a camera device **112**, an audio and codec device **114**, a secure algorithm **116**, a secure processor **118** and other device hardware **119**. The device hardware **119** includes a device processor, input/output (I/O) interfaces and transceivers integrated in the mobile communication device **100**. The OS layer **120** includes a device OS **122** and a security service **125**. The device OS **122** is responsible for managing and coordinating activities for the low-level layer **110** and the high-level layer **130**. The secure service **125** is provided in the OS layer **120** to supplement the device OS **122** for handling and managing secure operations on the mobile communication device **100**. The secure service **125** allows the mobile communication device **100** operates in a normal mode and a secure mode, which can be triggered by a rightful user manually. Under the normal mode, while the secure service **125** may still assist the device OS **122** in handling some security operations, it only provides a minimal security service typically as required by the industrial standards and protocols. Under a secure mode, the secure service **125** loads up its secure services and drivers to control and manage operations of the mobile communication device **100**. The secure service **125** may further work in conjunction with additional algorithms and/or cipher to secure the mobile communication device **100**. The high-level layer **130** comprises software applications **132** that include applications bundled with the mobile communication device **100** and any user installed

applications. Generally, these applications are easily accessible by any one using the mobile communication device **100** under the normal mode.

[0014] Referring back to the device OS **122**, it comprises drivers and services which are to be executed for general operations of the mobile communication device **100**. The general operations include executing and processing applications **132** resided on the mobile communication device **100**, activating a transmission protocol via communication module or transceivers, coding/decoding transmissions transmitted to/from the multimedia I/O interfaces, accessing and managing the files and folders on the mobile communication device, and etc. In the normal mode, the general operations may be carried out with little or no security protections. For example, a telephone conversation between two mobile communication devices is usually coded/decoded with common codec. Any eavesdroppers may intercept the transmission between the two devices through the air and listens to the conversation. In another example, when the mobile communication device **100** is handed on another person not the rightful owner, that person may easily access the personal data, such as address book, files/folders and etc. Under the secure mode provided by the secure service **125**, the above mentioned problem can be eliminated.

[0015] Still referring to **FIG. 1**, when the mobile communication device **100** is switched under the secure mode, the security service **125** fully administers the security of the mobile communication device **100**. The dedicated security processor **118**, when present, is adapted to handle and process the security operations of the security service **125**. Such dedicated processor not only lighten processing load on the device processor of the mobile communication device **100**, but allowing more complex security features to be implemented to enhance security without compromising performance of the mobile communication device **100**. In conjunctions with the dedicated security processor **118**, the secure algorithm **116** can be adapted to further enhance the security level. The secure algorithm **116** includes ciphers, codec, keys generators and handlers, biometric detector, access controller and etc. catering for different type of operations on the mobile communication device **100**.

[0016] Further, under the secure mode, operations through the camera device 112 and the audio and codec device 114 are also supervised by the security service 125. Any software applications (including the device OS 122) or hardware devices attempt to access said devices 112 and 114, locally or remotely, the access are verified by the security service 125. Similarly, executions of some applications 132 or even some features of the applications 132 on the mobile communication device 100 are restricted.

[0017] In accordance with another embodiment, the secure algorithm 116 is provided as a software module.

[0018] In an alternative embodiment, the security manager 110 is handled by a processor/controller of the mobile communication device.

[0019] FIG. 2 illustrates a block diagram of a security service of the mobile communication device 100 of FIG. 1 in accordance with one embodiment of the present invention. Under a secure mode, the security service 125 provides security surveillance and control for both low-level layer hardware and algorithm, and high-level layer software applications. The hardware and algorithm include a secure processor 260, a secure algorithm 259, an audio/codec device 258 and a camera device 261. The software applications include a phone application 251, multimedia recorder and player application 252, messaging applications 253, Internet applications 254, user data applications 255, wireless module 256, and user applications 257.

[0020] To facilitate the security surveillance and control, the security service 125 comprises a secure core 200, a secure data service 202, a secure multimedia service 204, a secure access validation service 206, a secure algorithm driver 208, a secure codec driver 209 and a secure camera driver 210. These services and drivers are adapted to interact with respective software applications and hardware of the mobile communication device 100 allowing the mobile communication device 100 to operate under a secure environment. The services handle applications and data at the higher-level layer of the mobile communication device. The responsibilities of the services include checking the type of data being accessed and providing/defining security requirements for each type of data that requires protection. The drivers handle the

hardware and algorithms implemented at the low-level layer of the mobile communication device and allow applications at a higher-level layer to interact therewith. The drivers include requirements and conditions of usage of the hardware and algorithm under the secure mode.

[0021] The secure core **200** is a main component of the security service **125** that is responsible for managing and controlling the services and drivers **200**, **202**, **204**, **206**, **208**, **209** and **210**. Under the secure mode, the secure core **200** monitors data signatures and hardware activities that require security attentions via the services and drivers. The secure core **200** manages the data flows and hardware activities based on the instructions provided in the services and drivers. The processing and security operations are generally performed by the relevant hardware or software application as appropriately.

[0022] The secure data service **202** is provided for handling data security. The data can be text data and multimedia data, which includes SMSs, emails, video and audio data, user diary and address book data, and etc. Under the secure data service **202**, type of the data is identified and an appropriate application is called to process the data. When necessary, the secure data service **202** further executes relevant applications to perform verifications and authorizations when these data are being created or accessed. The verification includes verifying bio-matrix and passwords to determine if the user is the rightful owner to use the mobile device.

[0023] In addition to the secure data service **202**, the multimedia data requires the secure multimedia service **204** to pre-process of the multimedia data before it is sent to the secure data service **202**. The secure multimedia service **204** manages the encryption/decryption, noise or echo cancellation, and compression/decompression of the multimedia data. The secure multimedia service **204** further secures creation of new multimedia or edits existing multimedia data stored on the mobile communication device.

[0024] Typically, different types of data can be handled by one or more corresponding software applications, for example, multimedia data corresponds to the

phone application **251** and the multimedia recorder and player application **252**, instance messages or emails correspond to messaging applications **253**, Internet contents correspond to Internet applications **254** and user's data corresponds to the user data application **255**. The Internet applications **254** include a web-browser, instant messaging clients, and the like. The user data applications **255** include file explorer/viewer, electronic address/phone book, e-calendar and etc.

[0025] The secure access validation service **206** provides controls on accessibility of features and data/information of the mobile communication device **100**. The accessibility includes local and remote access. For avoidance of doubt, the local access refers to physical usage and access of the mobile communication device by a user, whether or not a rightful user; the remote access refers to access to the mobile communication device through communication means, such as wireless communications. Under the secure mode, the secure access validation service **206** monitors activities' signatures of the Internet applications **254**, the user data applications **255**, the wireless module **256** and the user applications **257**, and acquires verifications when necessary. The activities include Internet transmissions, user input data, wireless module controls, user applications executions, etc. Depending on the type of validations required, the secure access validation service **206** interacts with software applications at software layer, hardware/algorithm at the hardware layer or both through the secure core **200** to handle more complex validations processing as required. When necessary, the secure validation service **206** may initiate multi-level/step verifications to increase the security level. The multi-level verifications can be processed through the means in software and hardware layers. When any one of the validations fail, the secure access validation service **206** ceases/denies accessibility of the pending operations through the secure core **200**. The validations and authentications provides by the secure validation service **206** to protect the mobile communication device from unauthorized access.

[0026] The validations and authorizations provided by the secure access validation service **206** include PIN code access, biometric verification, face recognitions and etc. The validations and authorizations are generally required before the execution of the relevant feature or access of the relevant data. It is also possible

that the secure validation service **206** acquire validations and authorizations while accessing the features or data of the mobile communication device **100**. Where require, the secure validation service **206** may work in conjunction with the secure processor **260** and the secure algorithm **259**, for example, for validations and authorizations processing.

[0027] In addition, data that relates to the Internet application **254** and the user data applications **255** processed under the secure data service **202** after the verification through the secure access/validation service **206**.

[0028] The drivers are provided to allow interactions between the operating system **122** with the respective hardware and algorithms at the low level layer under the secure mode. In particular, the secure algorithm driver **208** is used to drive the secure processor **260** and the secure algorithm **259**; the audio/codec driver **209** is used to drive the audio/codec device **258**; and the camera driver **210** is used to drive the camera device **261**. Some of the drivers, such as the audio/codec driver **209** and the camera driver **261**, are proprietary drivers that are mostly made without or with minimal security features. When these drivers are provided in the secure service **125**, the devices driven by these drivers are protected with the security features provided by the secure service **125**. The secure service **125** is further adapted for receiving new drivers so that drivers' activities are also monitored and protected under the secure service **125**.

[0029] The secure algorithm driver **208** interacts with the secure processor **260** and in conjunction with the secure algorithm **259** to achieve higher level of data security. The secure processor **260** includes a dedicated processor unit integrated in the mobile communication device for handling security related processing. The secure algorithm **259** includes algorithms and processes that are adapted to handle encryption/decryption, validations processing and etc. Generally, the algorithms and processes are proprietary and configurable for better security protection.

[0030] The audio/codec driver **209** processes inputs/outputs from/to the audio device **258** of the mobile communication device. The audio device includes microphones and speakers. Under the secure mode, the coding/decoding and

compression/decompression of the audio signals are protected for transmission. The secure service **125** protects the audio signals via encryption/decryption of the audio signal prior to the signal transmissions. When necessary, the audio/codec driver **209** can be disabled/terminated by the secure core **200**, thereby disable/terminate the audio/codec device **258**, when a security threat is detected.

[0031] Similarly, the camera driver **209** processes inputs/outputs from/to the camera device **261**. The inputs/outputs include still images or videos. Under the secure mode, the coding/decoding and compression decompression of the inputs/outputs are protected for transmission. The secure service **125** protects the camera inputs/outputs via encryption/decryption of the camera inputs/outputs. When necessary, the camera driver **261** can be disabled/terminated by the secure core **200**, thereby disable/terminate the audio/codec device **258**, when a security threat is detected.

[0032] The drivers are provided therewith for illustrations only. It is understood that there may be other devices or secure algorithms that require dedicated drivers in the security service **120** for secure operation under the secure mode.

[0033] It is understood that the software applications and hardware of the mobile communication device are illustrated in **FIG. 2** by way of example only, not limitations. It is understood that along with the technology advancement, it is foreseeable that the mobile communication device will integrate with more features, which can be software-based or hardware-based, or both. The security service **125** may be expended accordingly to include other services and devices in accordance with another embodiment of the present invention.

[0034] It is understood that different transceivers may require different wireless module **256**. In accordance with another embodiment, a mobile communication device may consist of more than one wireless module **256** for different wireless transceivers.

[0035] The security features provided in accordance with the present invention not only protects transmission from being stolen off the air, but also prevents wrongful user from using a stolen or missing mobile communication device.

[0036] The configurable security service **125** defined above facilitates a secure solution and its scalabilities allow for further expansion. The security service **125** provides additional secure services to enable and manage common applications and operations under a secured platform.

[0037] 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 secure communication manager for securing a mobile communication device from unauthorized access of applications, data and hardware resided on the mobile communication device, the secure communication manager comprising:

a plurality of secure services adapted to operationally monitor and control of access and execution of the applications and data;

a plurality of drivers operable to interface the hardware with the secure communication manager;

a secure core operable to handle and manage the secure services and drivers to detect for any unauthorized access of the applications, data and hardware, the secure core is operable to detect the unauthorized access based on security requirements and restrictions defined by the secure services and drivers,

wherein the secure communication manager resides and operates at an operating system layer of the mobile communication device.

2. The secure communication manager according to claim 1, wherein the secure communication manager resides and operates at the operating system layer as a service.

3. The secure communication manager according to claim 1, wherein the plurality of secure services include a secure data service for managing data access and transmission, a secure multimedia service for managing voice communication and a secure access validation service for validating access and execution of applications and data of the mobile communication device.

4. The secure communication manager according to claim 3, wherein the secure data service is operable to handle data security, wherein the data includes text data and multimedia data.

5. The secure communication manager according to claim 3, wherein the secure multimedia service is adapted to operationally encrypt/decrypt and encode/decode the multimedia data.

6. The secure communication manager according to claim 3, wherein the secure access validation service operable to control accessibilities of the applications and data, of which, the accessibilities include local access and remote access, wherein the secure access validation service denies access when a validation fails.
7. The secure communication manager according to claim 6, wherein the validation includes PIN code access, biometric verification and face recognitions.
8. The secure communication manager according to claim 6, wherein the secure access validation service is adapted to provide validation for accessing a wireless communication module of the mobile communication device.
9. The secure communication manager according to claim 8, wherein the mobile communication device comprises one or more wireless communication module.
10. The secure communication manager according to claim 1, wherein the drivers include a secure algorithm driver for driving a secure algorithm operable to facilitate security processing.
11. The secure communication manager according to claim 1, wherein the drivers include an audio/codec driver and a camera driver.