

MOBILE COMMUNICATION DEVICE PROTECTION SYSTEM AND METHOD

Field of the Invention

5

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

10

Background

[0002] With many communications take place over a distance wirelessly via mobile communication devices, such as a mobile phone, it is increasingly important that the communications over the air are remained private and secure. However, most
15 of the communications exchanged through the air can be eavesdropped. These communications include data, audio and video communications.

[0003] There are various ways that the eavesdropper intercepts a private communication. At the sender's or the receiver's end, as the communication signals
20 are transmitting freely in the air. Any one with an appropriate receiver can obtain a "copy" of the communication signals when equipped with appropriate tools through the air. The communication signal can also be tapped over the circuit switching station or through the infrastructure of voice/data circuits of the communication devices.

25 **[0004]** In order to protect the channels from being tapped off air and/or over the circuit switching station, end-to-end encrypted voice/data channel needs to be established to achieve a more acceptable level of security.

[0005] That is to say, in the absence of environmental awareness and control,
30 even if the communicating devices being used are capable of performing the highest level of cryptography, the entire voice/data security path will not be present in this

scenario. Hence, the control of usage of content is the primary step or requirement towards security and privacy.

[0006] In an example of mobile communication devices such as mobile phones that uses GSM protocol for communication, has designed within its level of security feature that prevent common eavesdroppers with limited resources from breaking through easily SIM card and its encryption. However, with the help of some professional equipment and also at the infrastructure end, it will be difficult to guarantee the integrity and security of the channels in use.

[0007] Thus, it is essential that for secured communications, even over a digital network like GSM which has its built-in level of security, an end to end encrypted voice/data path is required to guarantee a secured path.

Summary

[0008] The present invention provides a mobile communication device having an application processor, and a communication module, wherein a communication with another mobile communication device is executed by the application processor and communicated via the communication module.

[0009] In accordance with one embodiment, the device comprises a security processor adapted to connect to the application processor and the communication module, the security processor being operable to take control of the application processor and the communication module, and to monitor all executable operations on the mobile communication device and to overrule an executed operation when eavesdropping or prohibited activity is detected. When a communication with intended mobile communication device is established, the security processor is also responsible to encrypt and decrypt communication signals of the communication module.

[0010] In accordance with another embodiment, there is provided a method of providing secure communication to the mobile communication devices.

Brief Description of the Drawings

5 **[0011]** This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0012] **FIG. 1** illustrates a block diagram of a mobile communication device in accordance with one embodiment of the present invention;

10

[0013] **FIG. 2** illustrates a block diagram of the security processor in accordance with another embodiment of the present invention;

[0014] **FIG. 3** illustrates a schematic diagram of a mobile communication
15 device in accordance with another embodiment of the present invention;

[0015] **FIG. 4** shows a flow diagram of a crypto mode in accordance with one embodiment of the present invention; and

20 **[0016]** **FIG. 5** illustrates a block diagram of a mobile communication device in accordance with one embodiment of the present invention.

Detailed Description

[0017] In line with the above summary, the following description of a number of specific and alternative embodiments is provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practised 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.

10

[0018] FIG. 1 illustrates a block diagram of a mobile communication device 100 in accordance with one embodiment of the present invention. The mobile communication device 100 comprises an application processor 110, a communication module 120, a codec and audio switch 130, a speaker 132, a microphone 134 and a security processor 150. The application processor 110 is a processor that executes and runs a device operating system and all other applications available on the mobile communication device 100, and provides overall control of peripherals of the mobile communication device 100. The peripherals include display screen, input keys, LED indicators, etc. The application processor 110 is further connected to device memories, such as RAM and ROM. The communication module 120 is adapted to establish communications with networks and other devices. The communications are based on the communication protocols such as Global System for Mobile Communications (GSM), 3G, Code Division Multiple Access (CDMA), General Packet Radio Service (GPRS), Bluetooth (BT) and etc. The codec and audio switch 130 is provided for controlling audio path for a voice enabled device. The speaker 132 and the microphone 134 are connected to the codec and audio switch 130 where the audio to be outputted to the speaker 132 and the audio received from the microphone 134 are encoded and decoded herein via the selected audio path. In normal operation, the application processor 110, the communication module 120 and the codec and audio switch 130 function as other mobile communication known in the art. For example, when a user uses the mobile communication device 100 to make a phone call, the application processor 110 executes the communication module 120 to establish a connection.

During the connection, the audio is encoded and decoded in the codec and audio switch **130**. The application processor **110**, the communication module **120** and the codec and audio switch **130** may already provide with standard security features, such as password/pin code protections, data encryptions and the like.

5

[0019] Still referring to **FIG. 1**, the security processor **150** is an additional processor or secondary processor provided for performing all ciphering and deciphering of the audio/video/data contents and providing secured communications.

10 When the security processor **150** is activated, all operations of the mobile communication device **100** are interrupted or overruled by the security processor **150** for security purpose. Depending on security settings by the security processor **150**, most of the operations, if not all, of the mobile communication device **100** required appropriate authentications before they can be executed by the application processor **110**, the communication module **120** and the codec and audio switch **130**.

15

[0020] The security processor **150** is adapted to take over the encryption and decryption operations, and thus the processing load of the application processor **110** is lightened substantially.

20

[0021] With the security processor **150** activated, a communication between two mobile communication devices **100** is an end-to-end secured communication transmission. All transmissions are encrypted before sending and they are only decryptable by the security processor **150** of the mobile communication device **100** on the other end. The signals obtained in the air or at the infrastructure switching circuit or anywhere between the two communication devices **100**, without a proper decryption, are fully unusable signals to all third parties. The proper decryption requires ciphering keys before the data could be decrypted. The ciphering keys are only known between the security processor **150** of the connecting mobile communication devices **100**.

25

30

[0022] In case of communications between the two mobile communication devices **100** through a GSM network for example, the secure transmissions may use GPRS channel or transparent data mode in accordance with one embodiment. A

communication under the GPRS channel is a packets oriented communications. GPRS service supports a high data transfer rate for communications. GPRS channel may be preferred when a complexity of encryption and compression does not demand a high level of ciphering mechanism. In Transparent data mode, on the other hand, it can be
5 used for audio/video, fax transmissions. This type of transmissions generally allows signal loss without the need for re-transmission to reduce any possible delay, and thus achieving a more fluent audio/video communication channel. These are possible communications that are suitable for the present invention. They are provided by way of example, not limitations to the scope of the present invention. It is understood to the
10 skilled person that other communication channels or modes can be desired.

[0023] In the above embodiment, the codec and audio switch **130** is illustrated by way of example only. It is not intended to be a limitation to the scope of the present invention. In accordance with another embodiment, the codec and audio switch **130**
15 can be a codec and switch for video as well provided for video conference communication or the like, of which, video-capturing means (not shown) is required in addition to the speaker and microphone.

[0024] **FIG. 2** illustrates a block diagram of the security processor **150** in accordance with another embodiment of the present invention. The security processor **150** comprises an encryption and decryption module **210**, a compression and decompression module **220**, an echo (audio) canceling module **230**, a configuration and settings module **240** and an interface adaptation module **250**.
20

[0025] The encryption and decryption module **210** is the core of the security processor **150** where the entire ciphering/deciphering algorithms and methods to secure data are implemented. The signals to be transmitted and received are encrypted/decrypted herein. The complexity of this module is determined by the level of security required and the algorithms used to ensure that it could not be hacked.
25

30

[0026] The compression and decompression module **220** compresses/decompresses the data for transmission. It allows data transfer to be more

efficient by reducing the overall effective data required to be transferred. This is especially important as the data size is increased after an encryption process.

[0027] The echo canceling module **230** provides echo canceling algorithm for
5 canceling the echo noise generated in the mobile communication device **100**.

[0028] The configuration and settings module **240** is adapted to manage security parameters provided by the security processor **150**. It works in conjunction with a graphical user interface (GUI) allowing users to customize the security settings
10 according to needs.

[0029] The interface adaptation layer module **250** marks the protocols of both command and data between the the security processor and the application processor. It also manages and controls all communications packets and its timing requirement to
15 ensure communications meet the defined specifications. In addition, its other main role is responsible for communicating with application processor so that information could be transferred correctly. In this case, a corresponding interface adaptation layer module or the like is required on the application processor **110** in order to communicate with the security processor **150** for the application processor **110** be working smoothly and
20 interfaced effectively with the security processor **150**.

[0030] When a call is received, the mobile communication device **100** on the recipient end determines if the mobile communication device **100** on the calling end is making a crypto transmission that requires to activate the security processor. If the
25 receiving call is not the crypto transmission, the call can be made in accordance with the usual GSM communication protocols. If a secured transmission is required, the security processor **150** of the mobile communication device on the recipient end is activated automatically to establish the connection in the crypto mode. An authentication and verification may be required to determine the rightful user of the
30 mobile communication device. Accordingly, the signal transmitting between the two mobile communication devices **100** are secured.

[0031] FIG. 3 illustrates a schematic diagram of a mobile communication device 300 in accordance with another embodiment of the present invention. The mobile communication device 300 comprises an application processor 310, a wireless module 320, an audio switch 330, an audio I/O means 340, a security processor 350 and an access button 355. Similar to the above embodiments, the application processor 310, and the wireless module 320, the audio switch 330 and the audio I/O means 340 are provided in the mobile communication device 300 for normal operation. The audio switch 330 may provided with a codec. The access button 355 is a dedicated button for activating the security processor 350 to function. When the security processor 350 is activated in a crypto mode, the security processor 350 monitors all transmissions and takes over all encryptions and decryptions of the transmissions by the mobile communication device 300. Further, all operations by the application processor 310, the wireless module 320, the audio switch 330, the audio I/O means 340 are also monitored and controlled by the security processor 350 based on the security settings. When a prohibited activity is detected, the security processor 350 takes over the control and denial the prohibited activity accordingly. Similarly, when the security processor 350 detects any unauthorized executions of the wireless modules 320 and the audio switch 330, the security processor performs execution of an overruled mechanism to deny all the unauthorized executions and operations. For example, when the mobile communication device 300 is intruded by a privacy-invasive software, the personal information stored in the mobile communication device 300 may be collected and sent or broadcasted to a third party without the user's consent. In this case, when the security processor 350 is activated, the execution of the privacy-invasive software would be denied. Even if the privacy-invasive software is able to be executed, unauthorized communications initiated by the privacy-invasive software via the wireless module 320 is also blocked by the security processor 350, as the security processor 350 would overrule any unauthorized activities.

[0032] FIG. 4 shows a flow diagram of a crypto mode in accordance with one embodiment of the present invention. The steps comprise activating crypto mode at step 410; taking controls of the mobile communication device at step 420; overruling invalid operations at step 430; validating user and data at step 440 and encrypting and

decrypting transmission at step 450. At the step 410, the crypto mode is activated by activating a security processor of the mobile communication device. The activation of the crypto mode can be achieved by a dedicated button, through a menu selection or automatically as and when the mobile communication device is alerted by a secured call and secured data accessed. At the step 420, the security processor takes controls of the mobile communication device. At the step 430, the security processor overrules the operations by other modules of the mobile communication device. Any unauthorized operations, including communications, on the mobile communication device are denied/rejected/blocked by the security processor. At step 440, the security processor validates user and data to ensure that the communications are established between the intended end users. This is achieved with the authentication and validation combination of user authentication key and other biometric entry like fingerprint scan on the mobile communication device. At step 450, the security processor takes over the encryptions and decryptions of the all transmissions with the algorithms provided therein. During the transmissions between two mobile communication devices, encrypted signals from the security processor of one mobile communication device is only decryptable by the security processor of the coupled mobile communication device.

[0033] FIG. 5 illustrates a block diagram of a mobile communication device 500 in accordance with a further embodiment of the present invention. The mobile communication device 500 comprises an application processor 510, a WiFi and Bluetooth module 521 and a GSM module 522, an audio/video switch 530, audio I/O means 540, a security processor 550 and a crypto overruled control circuitry 552. Similarly, the application processor 510, the WiFi and Bluetooth module 521, GSM module 522, the audio/video switch 530 and the audio I/O means 540 are provided for normal operations of the mobile communication device 500 as others known communication devices. The security processor 550 is further connected to a crypto overruled control circuitry 552 which is hardwired to the WiFi and Bluetooth module 521, the GSM module 522 and the audio/video switch 530 to take over the a full control of these modules from the application processor 510 when it is activated in the crypto mode.

[0034] Privacy and security is always the main concern to personal information, which is private and confidential. Further, as more and more features are integrated in one mobile communication device, often than not, most of the personal information are
 5 stored therein for easy access. That on the other hand makes it easier for an intruder to obtain the users' personal information and intrude the users' privacy by hacking one communication device. Common standard network protocols are built-in with certain level of securities and encryptions, however, these securities feature provide only little protection only. Serious intruders, such as eavesdroppers, are still able to intrude the
 10 mobile communication device under the limited security setup. Accordingly, the dedicated security processor in accordance with the above embodiments is able improved the protection against intruders by restricting functionalities and connectabilities of the mobile communication device and providing higher-level encrypted signals.

15

[0035] In one non-limiting example, when an intruder have sent an invasive command to activate the GSM module and the microphone of the mobile communication device remotely without the user's knowledge. When the GSM module and the microphone are activated, all conversations by the user are transmitted
 20 out through the mobile communication device. With the security processor running, the overruled mechanism, unauthorized activation of the GSM module and the microphone will be rejected.

[0036] Yet another non-limiting example, an intruder could implant viruses to
 25 the application processor in a form of software drivers, middleware or applications. When the viruses are executed, they take controls of the wireless modules including GSM module, WiFi module or the Bluetooth module. These viruses are able to send out the personal information and data resided on the mobile communication devices through any of the wireless channels. With the crypto overruled mechanism, all the
 30 wireless modules are forced to be turned off or shutdown, and therefore, nothing will be transmitted out from the mobile communication device.

[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 mobile communication device having an application processor, and a communication module, wherein a communication with another mobile communication device is executed by the application processor and communicated via the communication module, the device comprising:
- 5 a security processor adapted to connect to the application processor and the communication module, the security processor being operable to take control of the application processor and the communication module, and to monitor all executable operations on the mobile communication device and to overrule an executed operation when prohibited activities is detected,
- 10 wherein when a communication with other mobile communication device is established, the security processor encrypted and decrypted communication signals of the communication channel.
- 15
2. The mobile communication device according to claim 1, further comprising a dedicated button for activating the security processor.
3. The mobile communication device according to claim 1, wherein the security processor comprising:
- 20 an encryption and decryption module;
a compression and decompression module;
an echo canceling module;
a configurations and settings module; and
25 a interface adaptation layer module.
4. The mobile communication device according to claim 1, further comprising a overruled control circuitry adapted to interrupt operations of the communication module to denial unauthorized transmissions.
- 30
5. The mobile communication device according to claim 1, wherein the communication module comprises a Bluetooth transmitter and receiver.

6. The mobile communication device according to claim 1, wherein the communication module is Wi-Fi enabled.
- 5 7. The mobile communication device according to claim 1, wherein the communication module comprises a GSM module.
8. A method of providing secure communication to a mobile communication device having an application processor, a communication module and a codec module,
10 wherein a communication with another mobile communication device is executed by the application processor and communicated via the communication module, the method comprising:
activating a security processor adapted to connected to the application processor;
15 taking control of the application processor and communication module;
monitoring all executable operations of the mobile communication device;
overruling an executed operation when it is detected unauthorized;
encrypting and decrypting communication signals of the communication with another mobile communication device.
20
9. The method of claim 8, wherein the security processor is activated by a dedicated button of the mobile communication device.
10. The method of claim 8, wherein the executed operation include unauthorized
25 transmission.
11. The method of claim 8, wherein the communication include a communication via a Bluetooth service.
- 30 12. The method of claim 8, wherein the communication include a communication via a Wi-Fi service.

13. The method of claim 8, wherein the communication include a communication via a GSM service.