

SYSTEM AND METHOD OF IDENTIFYING THE USER/POSSESSOR OF A MOBILE STATION

Field of the Invention

[0001] The present invention generally relates to authentication of mobile stations, and more particularly to a system and method of identifying the user/possessor of a mobile station.

Background of the Invention

[0002] Telecommunications have been transformed by the advent of portable mobile stations such as mobile phones. The mobile phone provides the users with real time communications without boundaries. It offers efficiency and convenience to mobile phone users. However, a problem with using such devices is that they are sometimes stolen or lost. If the user/possessor of the stolen mobile phone cannot be identified, there may be a black market for the stolen/lost mobile phones. It will inevitably increase the losses of the mobile phone owners.

[0003] There are provided many approaches to deter the theft of mobile phones. For example, some networks authenticate the users of mobile phones by validating the IMEI number, allowing the networks to blacklist or block the usage of the invalidated mobile phones to access the networks. However, it does not identify the user of the invalidated mobile phone.

[0004] U.S. Patent 6,696,941 discloses a system and method for remotely triggering an audible alarm within a mobile phone. The mobile phone comprises a remote trigger detection element that responds to an alarm personal identification number (PIN) entered by a remote user to produce an alarm signal. However, the identity of the user of the mobile phone is not revealed.

[0005] JP 2003199155A discloses a mobile communication apparatus having a function of authenticating a possessor itself. If authentication is failed, the theft can automatically be reported to a service center and the owner. However, the authentication is complicated by using fingerprint, voice print and iris authentication method. Moreover, the identity of the user of the mobile phone is not revealed.

[0006] U.S. Patent Application 2003/0218532 A1 discloses a mobile phone having a transponder to be used for authentication purposes. The transponder is input with user-specific information. When an interrogating reading device stimulates the transponder, the transponder emits the user-specific information. This enables authentication of a user. However, the addition of the transponder and interrogating reading device to a mobile phone increases its cost. Moreover, the operation is not convenient. Furthermore, the identity of the user of the mobile phone is not revealed. Also, RFID tag needs to work in close proximity with Interrogating Apparatus.

[0007] Therefore, there is an imperative need to have a system and method for identifying the user/possessor of a mobile station. The identification process must be simple and convenient. This invention satisfies this need by disclosing a simple method to identify the rightful owner of a mobile station and at the same time reveal the identity of the user/possessor of the mobile station. Other advantages of this invention will be apparent with reference to the detailed description.

Summary of the Invention

[0008] The present invention provides a system and method of identifying the user/possessor of a mobile station. When the mobile station is first purchased, the method for identifying the user/possessor of the mobile station comprises the steps of programming the mobile station with a user interface (UI) password when the mobile station is first powered on without an SIM card; wherein the mobile station has an international mobile subscriber identity (IMSI) number capture program allowing the mobile phone to capture of the IMSI number from an inserted SIM card and store the captured IMSI number into the memory of the mobile station; and authenticating the user/possessor of the mobile station after one SIM card is inserted into the mobile station; wherein the authentication is executed by asking the user/possessor to input the UI password; whereby, if the input UI password is right, the IMSI number capture program captures the IMSI number from the inserted SIM card and stores the captured IMSI number into the memory of the mobile station, and the mobile station goes to normal operation; or whereby, if the input UI password if wrong, the mobile station will send the IMSI number of the newly inserted SIM card to the network; thereby the user/possessor of the mobile station is identified.

[0009] The present invention also provides systems and methods for identifying the user/possessor of a used mobile station. The method comprises authenticating the user/possessor of the mobile station after one SIM card is inserted into the mobile station; whereby, if the IMSI number from the newly inserted SIM card matches any stored IMSI number, the mobile station goes to normal operation; or whereby, if the IMSI number from the newly inserted SIM card fails to match any stored IMSI number, the authentication is executed automatically, wherein the mobile phone expects the user/possessor to input the UI password without prompting; whereby, if the input UI password is right, the IMSI number capture program captures the IMSI number from the inserted SIM card and stores the captured IMSI number into the memory of the mobile station, and the mobile station goes to normal operation; or whereby, if the input UI password is wrong, the mobile station will send the IMSI number of the newly inserted SIM card to the network; thereby the user/possessor of the mobile station is identified.

[0010] Accordingly, one object of the present invention is to discourage the theft of mobile stations and to encourage the return of stolen/lost mobile stations to the rightful owners.

[0011] The objectives and advantages of the invention will become apparent from the following detailed description of preferred embodiments thereof in connection with the accompanying drawings.

Brief Description of the Drawings

[0012] Preferred embodiments according to the present invention will now be described with reference to the Figures, in which like reference numerals denote like elements.

[0013] FIG 1 shows a flow chart of the first start when a mobile phone is purchased.

[0014] FIG 2 is a flow chart showing the processes when an SIM card is inserted into a mobile phone that has programmed UI password and at least one stored IMSI number.

[0015] FIG 3 is a flow chart showing the abnormal handling path.

Detailed Description of the Invention

[0016] The present invention may be understood more readily by reference to the following detailed description of certain embodiments of the invention.

[0017] Throughout this application, where publications are referenced, the disclosures of these publications are hereby incorporated by reference, in their entireties, into this application in order to more fully describe the state of art to which this invention pertains.

[0018] The present invention provides a system and method for identifying the user/possessor of a mobile station. As discussed above, the representative device for mobile stations is mobile phone. Thus, the present invention will be illustrated by detailed description of identifying the user/possessor of a mobile phone. It is to be appreciated that the principles of the present invention are applicable to any mobile stations that provide an International Mobile Subscriber Identification (IMSI).

[0019] Usually, a mobile phone will use a subscriber identity module (SIM) card to enable the user/possessor of the mobile phone to make/receive calls. The SIM card is installed with user-specific data including the IMSI number. The user-specific data of the SIM card is accessible to the central processing unit (CPU) of the mobile phone. Thus, the present invention is in principle employing the IMSI number of any SIM card to identify the user/possessor of a mobile station.

[0020] Prior to a detailed description of one embodiment of the present invention, there is provided a brief description of the principles of the present invention. A mobile phone has a user interface (UI) password that allows a valid IMSI number to be stored in the memory of the mobile phone, wherein the last IMSI number stored will be the default IMSI number that is assumed to identify the rightful owner. When the mobile phone is stolen or lost, the owner can contact the network service center to inactivate the SIM card. Thus, the theft or possessor of the stolen/lost mobile phone has to insert a new SIM card in order to use the mobile phone.

[0021] When the theft or possessor of the stolen/lost mobile phone inserts his SIM card into the mobile phone and powers it up, the mobile phone will check the IMSI number of the newly inserted SIM card by comparing it against a database of the IMSI numbers stored previously in the mobile phone. When the mobile phone detects that the IMSI

number of the newly inserted SIM card is not in the IMSI number database, it will expect (without prompting) the user/possessor to enter the UI password. When the user/possessor fails to enter a UI password or enter a wrong one, the mobile phone will automatically send a notification message to the GSM network via USSD. Then default IMSI number and invalid IMSI number will be sent to GSM network via the USSD command by the backend application program of the mobile phone.

[0022] USSD request is passed by the MSC to an appropriate backend application program to process the USSD request. Then the subscription profiles of the owner and the user/possessor will be retrieved and sent to proper authorities for further investigation.

[0023] Now referring to FIGS 1-3, there is provided one embodiment of identification of the user/possessor of a stolen/lost mobile phone in accordance with the principles of the present invention.

[0024] FIG 1 shows a flow chart of the first start when a mobile phone is purchased. In step **100**, the mobile phone is powered on before inserting a SIM card. The mobile phone has an IMSI number capture program allowing the mobile phone to capture the IMSI number from an inserted SIM card and store the number in the mobile phone memory. The IMSI number capture program may be preinstalled in the mobile phone or downloaded from the network. In step **110**, the powered on mobile phone is programmed with a user interface (UI) password. It is noted that the UI password will activate the IMSI capture program so that a new IMSI number will be captured and stored in the mobile phone memory. Thus, the UI password will be strictly private and confidential and stored permanently in the memory. After the UI password is programmed, the mobile phone is turned off. Then a new SIM card is inserted. When the mobile phone is powered on again, a key-in of the UI password is required as shown in step **120**. The step **130** is a decision making one where the mobile phone will check whether the key-in UI password is correct. If the key-in password is correct, the IMSI number capture program will capture the IMSI number from the inserted SIM and store the IMSI number in the mobile phone memory as shown in step **150**. Then the mobile phone will go to normal operation as in step **160**. Back to step **130**, if the key-in password is wrong, the mobile phone will ask a second try as in step **140** which is also a decision making step. If the key-in UI password is right in the second try, the mobile phone will go to step **150** as described above. If the key-in US password is wrong again, the mobile phone will proceed to the abnormal handling path as

shown in FIG 3 detailed hereinafter. The whole process shown in FIG 1 can be summarized in the following pseudocode.

```
[0025]      Enter User Interface (UI) password
            {
                If UI password OK
                    MS resident program extract installed SIM IMSI and store in
                    MS memory
                    Normal Operation
                Else if
                    Counter decrement by 1
                    If counter reaches 0
                Go to abnormal handling path
                    Else if
                go back to Enter UI password
                    Endif
                Endif
            }
```

[0026] FIG 2 is a flow chart showing the processes when an SIM card is inserted into a mobile phone that has a programmed UI password and at least one stored IMSI number. It is understood that an SIM card is inserted before the mobile phone is started at step 200. When the mobile phone is powered on in step 210, the programs in the mobile phone memory will run. Then in step 220, the mobile phone will compare the IMSI number of the newly inserted SIM card with the IMSI number database residing in the mobile phone memory. The step 230 is a decision making one where the mobile phone decides whether the IMSI number of the newly inserted SIM card matches any stored IMSI number. If the IMSI number of the newly inserted SIM card is found in the database, the mobile phone will proceed to normal operation as in step 260. If the IMSI number of the newly inserted SIM card is not found in the database, the mobile phone will proceed to step 240 to see whether a UI password has been entered without prompting. If no password is entered, the mobile phone will give some time for the user to enter the UI password as shown in step 250. If the given time is not expired, the user will have the chance to enter the UI password as shown in step 240. If the given time is expired without any entered UI password, the mobile phone will proceed to the abnormal handling path as shown in FIG 3 detailed hereinafter. Back to the step 240, if the user enters a UI password, the mobile phone will proceed to check whether the entered UI password is correct as shown in step 270. If the entered UI password is right, the IMSI number capture program

will capture the IMSI number from the inserted SIM and store the IMSI number in the mobile phone memory as shown in step 280. Then the mobile phone will go to normal operation as in step 290. Back to the step 270, if the entered password is wrong, the mobile phone will proceed to the abnormal handling path as shown in FIG 3 detailed hereinafter. The whole process shown in FIG 2 can be summarized in the following pseudocode.

```
[0027]   Power On MS
         Check IMSI of installed SIM against IMSI stored in MS memory
         {
         If IMSI found is the same as the IMSI stored in the MS memory
             Normal Operation
         Else if
             If User enter UI password without prompting
                 If password is correct
                     Installed SIM IMSI is stored in MS memory
                     Normal Operation
                 Else if
                     Go to abnormal handling path
                 Endif
             Else if
                 If timer has expired
                     Go to abnormal handling path
                 Else if
                     Go to enter UI password
                 Endif
             Endif
         Endif
         }
```

[0028] FIG 3 is a flow chart showing the abnormal handling path to which a mobile phone will proceed when the user/possessor of the mobile phone fails to enter a UI password or enters a wrong UI password as shown in FIGS 1 and 2 discussed above. In step 300, the mobile phone will send to the GSM network the IMSI number of the newly inserted SIM card and the last valid IMSI number stored in the database of the mobile phone memory if it is available. In certain embodiments, the IMSI numbers can be sent by using the USSD command string. When the GSM network receives the USSD command string, it will send the command string to the backend application program. The backend application program is co-located with the switching network center and will retrieve the subscriber profile of the newly inserted SIM IMSI number as shown in step 310. Then in step 320, the backend application program will retrieve from the GSM network the profiles

of the subscriber for the last valid IMSI number and the subscriber for the IMSI number of the newly inserted SIM card. Finally, the backend application program will print out a report that can be filed with proper authorities as shown in step 330. The processes of the abnormal handling path can be summarized in the following pseudocode.

[0029] Abnormal Handling Path

{

 Send IMSI number in SIM card and MS memory to GSM network

 Backend GSM network application program will retrieve the profiles of the new user and the old valid user

}

[0030] The present invention provides a system and method that can identify the user/possessor of a mobile phone in a simple and convenient manner as long as the user/possessor of the mobile phone changes an SIM card. If no new SIM card is inserted, the local check in the mobile phone will detect and verify that the SIM card inside the mobile phone is one that has been authenticated. Thus, no authentication/verification process is required on the user part, and no authentication command will be sent to the network. Only when a new SIM card is inserted will the mobile phone require that a UI password be entered correctly and promptly. When the user/possessor of a mobile phone fails to enter the UI password or enters a wrong UI password, his identity will be revealed by the GSM network. One apparent advantage of the present invention is that the theft of a mobile phone will be discouraged and that the stolen/lost mobile phones will be more likely to be returned to their proper owners.

[0031] While the present invention has been described with reference to particular embodiments, it will be understood that the embodiments are illustrative and that the invention scope is not so limited. Alternative embodiments of the present invention will become apparent to those having ordinary skill in the art to which the present invention pertains. Such alternate embodiments are considered to be encompassed within the spirit and scope of the present invention. Accordingly, the scope of the present invention is described by the appended claims and is supported by the foregoing description.

CLAIMS

What is claimed is:

1. A method for identifying the user/possessor of a mobile station, comprising the steps of:

programming the mobile station with a user interface (UI) password when the mobile station is first powered on without an SIM card; wherein the mobile station has an international mobile subscriber identity (IMSI) number capture program allowing the mobile phone to capture of the IMSI number from an inserted SIM card and store the captured IMSI number into the memory of the mobile station; and

authenticating the user/possessor of the mobile station after one SIM card is inserted into the mobile station; wherein the authentication is executed by asking the user/possessor to input the UI password;

whereby, if the input UI password is right, the IMSI number capture program captures the IMSI number from the inserted SIM card and stores the captured IMSI number into the memory of the mobile station, and the mobile station goes to normal operation; or

whereby, if the input UI password if wrong, the mobile station will send the IMSI number of the newly inserted SIM card to the network; thereby the user/possessor of the mobile station is identified.

2. The method of claim 1, wherein the IMSI number capture program is preinstalled in the mobile station.
3. The method of claim 1, wherein the IMSI number capture program is downloaded from the network.
4. The method of claim 1, wherein the step of authenticating may ask the user/possessor to input the UI password more than once in case the user/possessor inputs wrong UI password.

5. The method of claim 1, wherein the IMSI numbers are sent by using the USSD command string.
6. The method of claim 1, further comprising steps of retrieving from the network the profiles of the subscriber of the newly inserted SIM card and sending the identity of the user/possessor of the mobile station to authority.
7. A method for identifying the user/possessor of a mobile station, wherein the mobile station has a user interface (UI) password, an international mobile subscriber identity (IMSI) number capture program allowing the mobile phone to capture of the IMSI number from an inserted SIM card and store the captured IMSI number into the memory of the mobile station, and at least one stored IMSI number, said method comprising the steps of:
 - authenticating the user/possessor of the mobile station after one SIM card is inserted into the mobile station;
 - whereby, if the IMSI number from the newly inserted SIM card matches any stored IMSI number, the mobile station goes to normal operation; or
 - whereby, if the IMSI number from the newly inserted SIM card fails to match any stored IMSI number, the authentication is executed automatically, wherein the mobile phone expects the user/possessor to input the UI password without prompting;
 - whereby, if the input UI password is right, the IMSI number capture program captures the IMSI number from the inserted SIM card and stores the captured IMSI number into the memory of the mobile station, and the mobile station goes to normal operation; or
 - whereby, if the input UI password is wrong, the mobile station will send the IMSI number of the newly inserted SIM card to the network; thereby the user/possessor of the mobile station is identified.
8. The method of claim 7, wherein the IMSI number capture program is preinstalled in the mobile station.

9. The method of claim 7, wherein the IMSI number capture program is downloaded from the network.

10. The method of claim 7, wherein the step of authenticating may ask the user/possessor to input the UI password more than once in case the user/possessor inputs wrong UI password.

11. The method of claim 7, wherein the IMSI numbers are sent by using the USSD command string.

12. The method of claim 7, further comprising steps of retrieving from the network the profiles of the subscriber of the newly inserted SIM card and sending the identity of the user/possessor of the mobile station to authority.

13. An algorithm for identifying the user/possessor of a mobile station, comprising:

```

Enter User Interface (UI) password
{
    If UI password OK
        MS resident program extract installed SIM IMSI and store in
        MS memory
        Normal Operation
    Else if
        Counter decrement by 1
        If counter reaches 0
            Go to abnormal handling path
        Else if
            go back to Enter UI password
        Endif
    Endif
}
Check IMSI of installed SIM against IMSI stored in MS memory
{
    If IMSI found is the same as the IMSI stored in the MS memory
        Normal Operation
    Else if
        If User enter UI password without prompting
            If password is correct
                Installed SIM IMSI is stored in MS memory
                Normal Operation
            Else if

```

```

        Go to abnormal handling path
    Endif
Else if
    If timer has expired
        Go to abnormal handling path
    Else if
        Go to enter UI password
    Endif
Endif
Endif
}
Abnormal Handling Path
{

    Send IMSI number in SIM card and MS memory to GSM network

    Backend GSM network application program will retrieve the profiles of the
    new user and the old valid user
}

```

14. A mobile station having the algorithm of claim 13.
15. The mobile station of claim 14, wherein the mobile station is a mobile phone.