SOFTWARE METHOD TO PREVENT CONNECTED DEVICE SERVICE THEFT

INVENTOR:

SUNDAR R. SRIRAM

Software solution to prevent connected device service theft.

Stolen modems are a common and prevalent problem.

See idea: Methods to prevent connected device service theft. Many solutions were proposed as part of the above invention.

I propose a software and credential-based solution to the above problem.

Solution:

A software-based solution for the above problem is proposed.

This involves a security application program that helps the User and Cable Operator protect the device from theft.

The security application program is pre-loaded into a system partition of the CM so that the security application program will not be erased during factory reset of the device or after reinstallation of new a new firmware/software.

When the CM is being setup as a new device, it will require the user to register the device with an external server using Users Credentials. An example of user credentials could be Google Account or Facebook Account or independent login/password. The User credentials are associated with the permanent device identifiers (MAC address, serial number, any other ID).

The User will can also setup a factory reset protection profile to have full control over the CM. This helps unlock a device if the User credentials are forgotten.

We see 2 use cases:

1. **User owns the CM**: User will setup the credentials on the CM. User is also responsible for setting up the factory reset protection profile.
2. **User rents the CM (from MSO)**: MSO will setup the credentials on the CM and the factory reset protection profile.

Theft Scenarios:

We see rendering the CM useless and unable to provide service as a huge deterrent to theft.

Here are the 2 associated use cases.

Use case1: CM is stolen. A genuine theft.

Any attempt to onboard the CM will require the User credentials of the original owner (either User or MSO). Hence, the device is rendered useless.

Use case2: CM is stolen. Malicious User.

For MSO owned CM, when an attempt is made to setup/onboard the CM in the new MSO, neither the User nor the new MSO have the credentials to onboard the device. Hence, the device is rendered useless.