MOBILE ACCESS TERMINAL SECURITY FUNCTION

FIG. 1

The system includes a wireless communications system, a security module, and a base station controller. The security module contains security policies and the wireless device transmits data through the wireless communications system to the base station controller. The security module verifies the data transmitted and allows it to be transmitted onto the wireless network. If the data originates from the wireless device, the packet data is prevented from being transmitted onto the wireless network (102).
CLAIMS

1. A method, with a wireless communication device, for managing packet data transmissions, the method comprising:
   - receiving, from a service provider, a set of security policies;
   - receiving a request from an application to originate packet data;
   - analyzing, in response to receiving the request to originate packet data, the set of security policies provided by the service provider;
   - determining, in response to the analyzing, if the set of security policies allows the packet data to be transmitted;
     - if the set of security policies allows the packet data to be transmitted, then allowing the packet data to be transmitted onto a wireless network; and
     - if the set of security policies does not allow the packet data to be transmitted, then preventing the packet data from being transmitted onto a wireless network.

2. The method of claim 1 wherein the packet data are Internet Protocol packet data.

3. The method of claim 1 further comprising:
   - notifying, in response to the packet data being prevented from being transmitted onto the wireless network, a security module residing on the wireless network of the prevented transmission of packet data.

4. The method of claim 1 wherein the set of security policies includes at least a security policy for transmitting packet data and at least one security policy associated with a set of applications.

5. The method of claim 1 wherein the preventing comprises:
   - analyzing a destination of the packet data; and
   - comparing the destination to the set of security policies.
6. The method of claim 1 further comprising:
   receiving a user request to add an application;
   analyzing, in response to receiving the user request, the set of security policies provided by the service provider;
   determining, in response to the analyzing, if the set of security policies allows the application to be added;
   if the set of security policies allows the application to be added, then allowing the application to be added; and
   if the set of security policies does not allow the application to be added, then preventing the application from being added.

7. The method of claim 6 further comprising:
   notifying, in response to the application being prevented from being added, a security module residing on the wireless network of the prevented addition of the application.

8. The method of claim 6 wherein allowing the application to be added comprises:
   generating a unique identification associated with the application; and
   storing the unique identification in a secure memory.
9. A wireless communication device for managing packet data transmissions, the wireless communication device comprising:
   a memory;
   a processor communicatively coupled to the memory;
   a security module communicatively coupled to the memory and to the processor, wherein the security module is adapted to:
   receive, from a service provider, a set of security policies;
   receive a request from an application to originate packet data;
   analyze, in response to receiving the request to originate packet data, the set of security policies provided by the service provider;
   determine, in response to the analyzing, if the set of security policies allows the packet data to be transmitted;
   if the set of security policies allows the packet data to be transmitted, then allowing the packet data to be transmitted onto a wireless network; and
   if the set of security policies does not allow the packet data to be transmitted, then preventing the packet data from being transmitted onto a wireless network.

10. The wireless communication device of claim 9 wherein the security module is further adapted to:
    notify, in response to the packet data being prevented from being transmitted onto the wireless network, a security module residing on the wireless network of the prevented transmission of packet data.

11. The wireless communication device of claim 9 wherein the set of security policies includes at least a security policy for transmitting packet data and at least one security policy associated with a set of applications.

12. The wireless communication device of claim 9 wherein the preventing comprises:
    analyzing a destination of the packet data; and
    comparing the destination to the set of security policies.
13. The wireless communication device of claim 9 wherein the security module is further adapted to:
   receive a user request to add an application;
   analyze, in response to receiving the user request, the set of security policies provided by the service provider;
   determine, in response to the analyzing, if the set of security policies allows the application to be added;
   if the set of security policies allows the application to be added, then allowing the application to be added; and
   if the set of security policies does not allow the application to be added, then preventing the application from being added.

14. The wireless communication device of claim 13 wherein the security module is further adapted to:
   notify, in response to the application being prevented from being added, a security module residing on the wireless network of the prevented addition of the application.