



(19) **United States**

(12) **Patent Application Publication**

Bajikar

(10) **Pub. No.: US 2003/0112182 A1**

(43) **Pub. Date: Jun. 19, 2003**

(54) **METHOD AND APPARATUS FOR CONTROLLING ACCESS TO MOBILE DEVICES**

(22) Filed: Dec. 19, 2001

Publication Classification

(76) Inventor: **Sundee M. Bajikar**, Mountain View, CA (US)

(51) **Int. Cl.⁷** **G01S 3/02**
(52) **U.S. Cl.** **342/457**

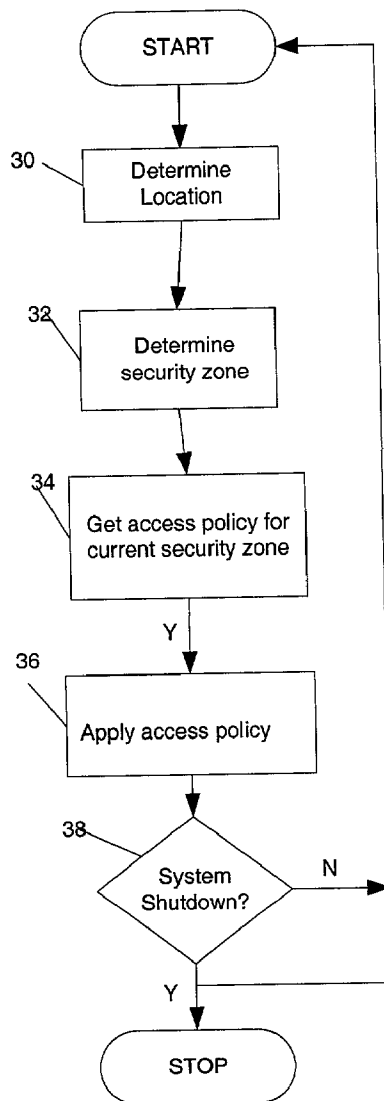
Correspondence Address:

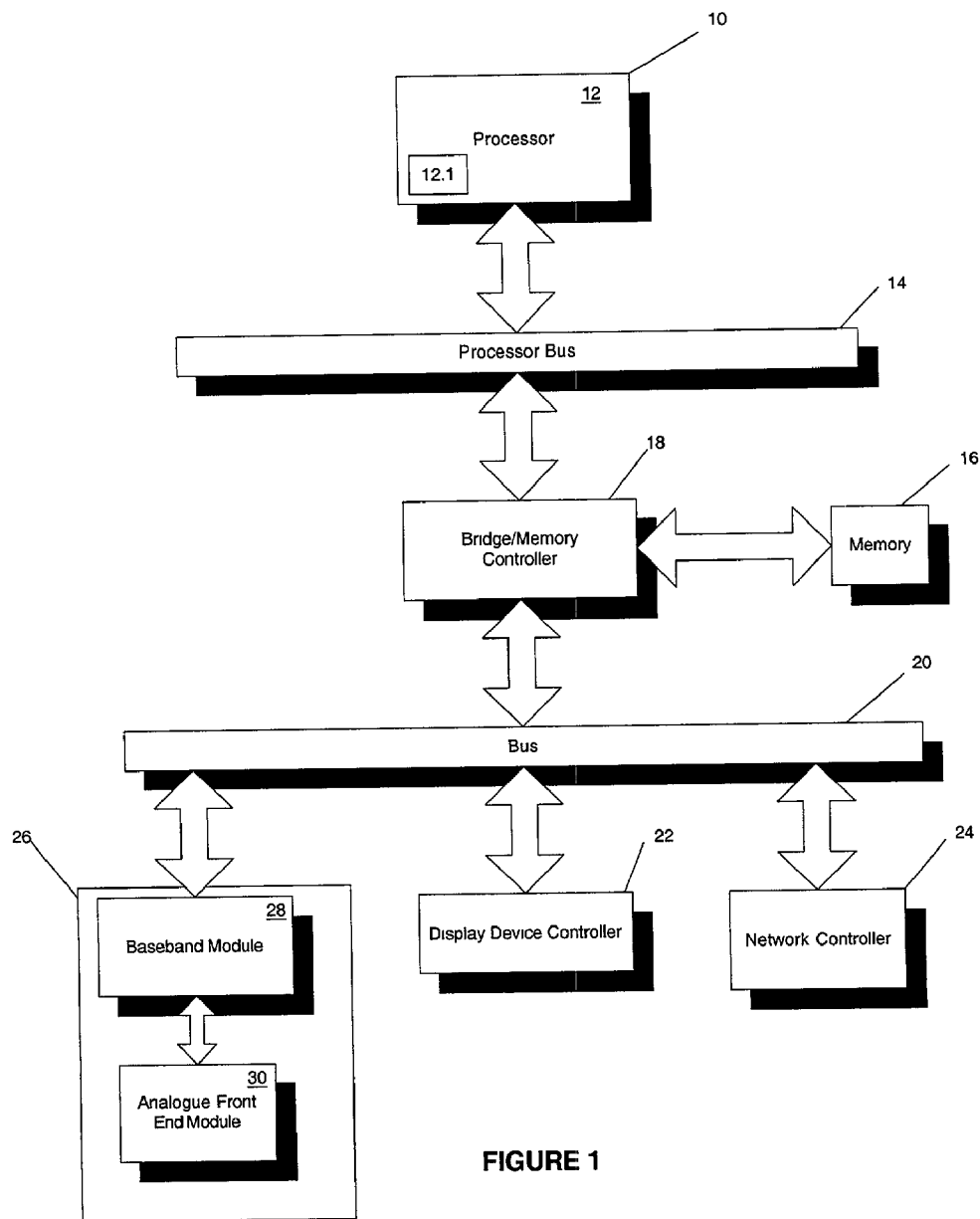
John Patrick Ward
BLACKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026 (US)

(57) **ABSTRACT**

According to one embodiment, the invention discloses a method comprising determining a position of a mobile device; and controlling access to said mobile device based on said position. According to another embodiment of the invention there is provided a mobile device comprising a positioning mechanism to determine a position a mobile device; and a controlling mechanism to control access to said mobile device based on said position.

(21) Appl. No.: **10/028,472**





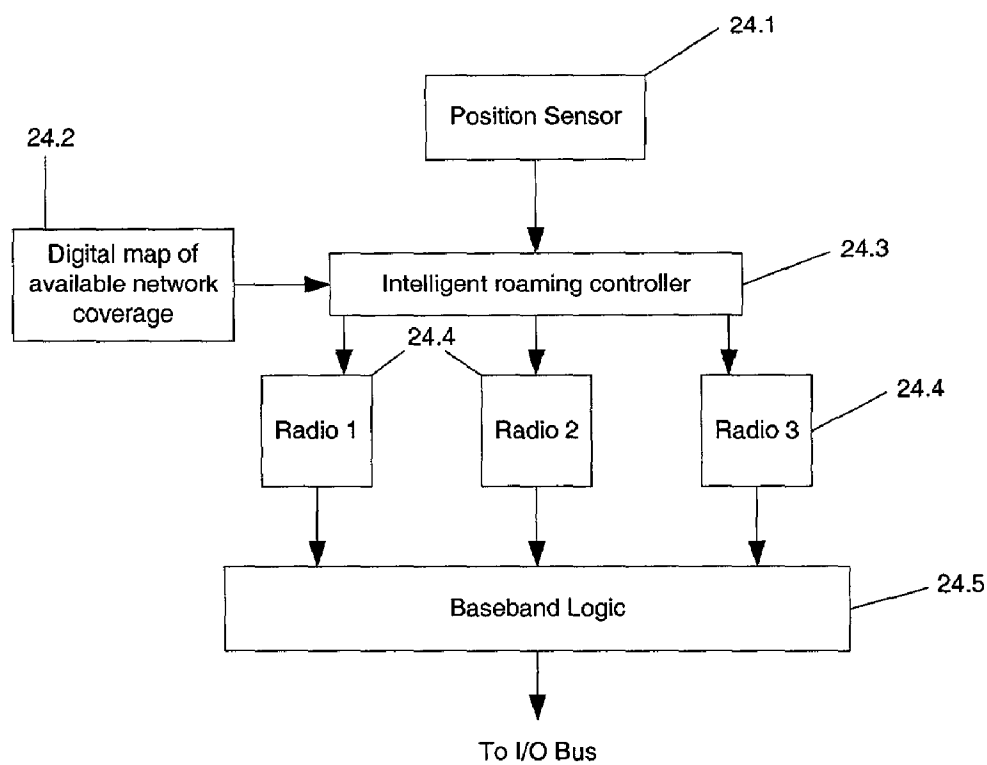


FIGURE 2

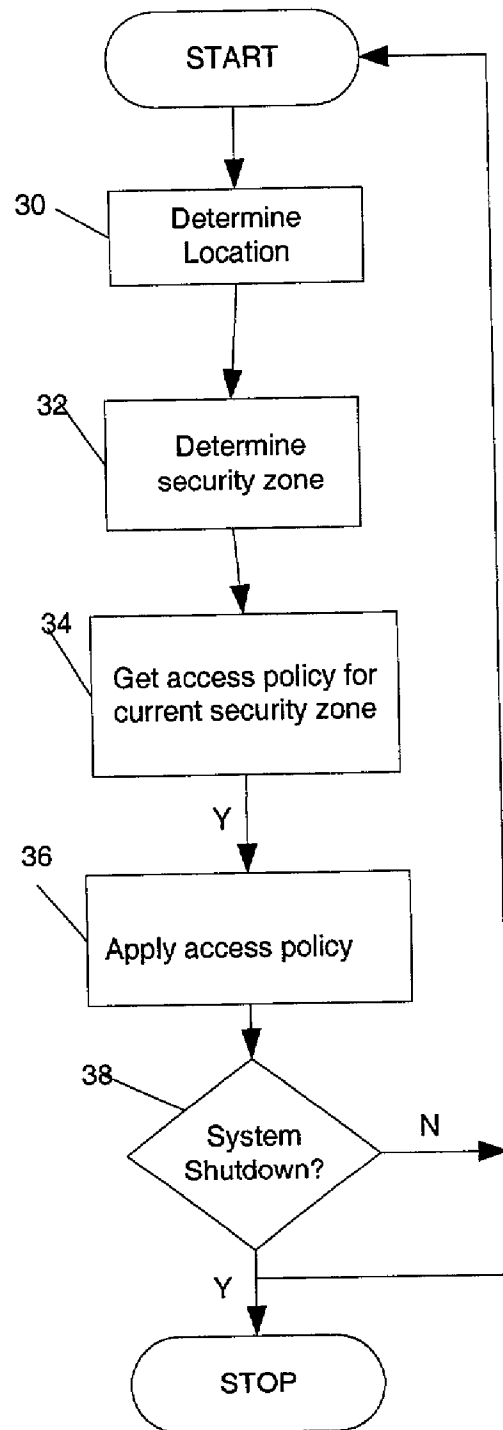


FIGURE 3

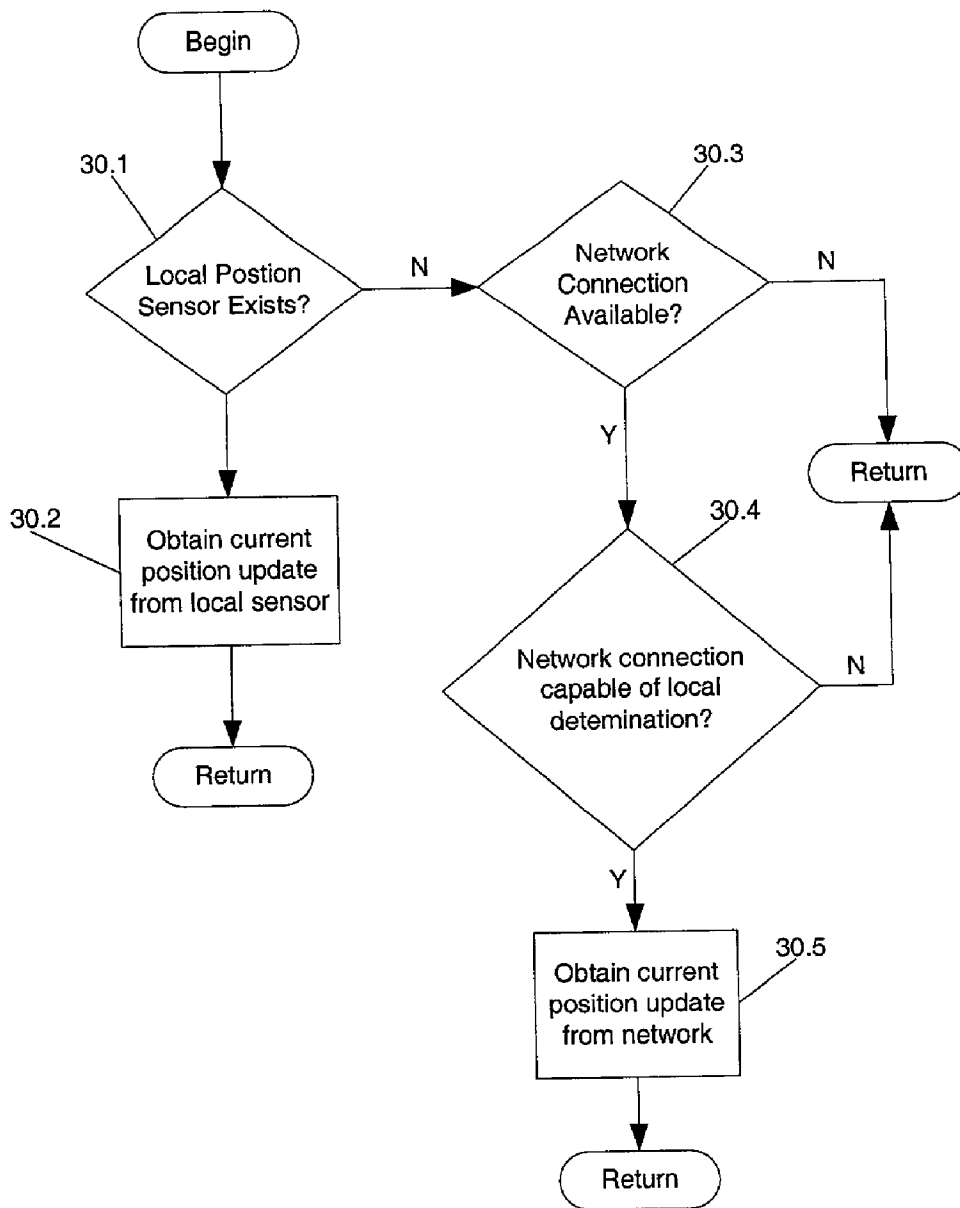


FIGURE 4

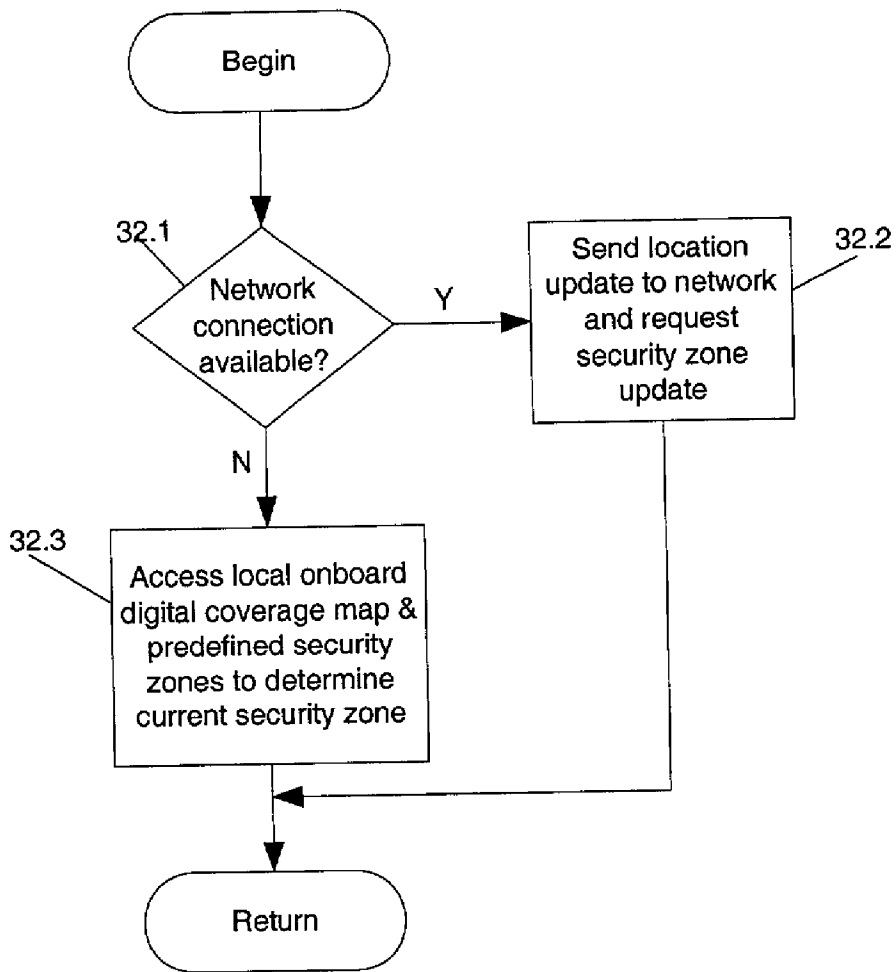


FIGURE 5

METHOD AND APPARATUS FOR CONTROLLING ACCESS TO MOBILE DEVICES

FIELD OF THE INVENTION

[0001] This invention relates to access control. In particular is relates to controlling access to mobile devices.

BACKGROUND

[0002] Mobile devices such as notebook computers, Personal Digital Assistants (PDAs) and cellular telephones are typically used in different locations depending on the movement of a user. Depending on where the mobile device is being used, it must be appropriately configured in order to prevent unauthorized use thereof. For example, when the user is on a corporate campus and is connected to a corporate intranet there is no need for data encryption for communications confined to the corporate intranet. Likewise, when the user is at home, security concerns related to unauthorized use of a mobile device would be reduced, whereas these concerns would be higher when the user is in a public place such as an airport or a hotel.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] FIG. 1 shows a block diagram of a mobile device in accordance with the invention;

[0004] FIG. 2 shows a block diagram of the wireless communications module of the mobile device of FIG. 1 in greater detail;

[0005] FIG. 3 shows a flowchart of operations performed in order to select an appropriate access policy in accordance with one embodiment of the invention; and

[0006] FIGS. 4 and 5 show aspects of operations in FIG. 3 in greater detail.

DETAILED DESCRIPTION

[0007] According to embodiments of the present invention access control parameters which control access to a mobile device are changed automatically based on the location of the mobile device. In some embodiments of the invention, a user of the mobile device pre-configures a set of security policies with predetermined values for the access control parameters based on knowledge of anticipated usage scenarios. The mobile device then uses an appropriate security policy based on the physical location of the device. Each security policy is associated with a zone which may be user defined. Examples of user defined zones may include a home zone, a work zone, an airport, a hotel zone, etc. Each zone defines the physical region within which the mobile device must be located before the security policy associated with the zone becomes operative. As a user moves around with the mobile device, the position of the mobile device is constantly updated and when the device crosses from one security zone to another, the security policy for that device is appropriately updated without any user intervention.

[0008] FIG. 1 of the drawings shows one embodiment of a mobile device 10 in accordance with the invention. The device 10 includes a processor 12 that processes data signals. Processor 12 may be a Complex Instruction Set Computer (CISC) microprocessor, a Reduced Instruction Set Computing (RISC) microprocessor, a Very Long Instruc-

tion Word (VLIW) microprocessor, a processor implementing a combination of instructions sets, or other processor device.

[0009] In one embodiment, processor 12 is a processor in the Pentium® family of processors including the Pentium® 4 family and mobile Pentium® processors available from Intel Corporation of Santa Clara, Calif. Alternatively, other processors may be used. FIG. 1 shows an example of a mobile device 10 employing a single processor. However, one of ordinary skill in the art will appreciate that mobile device 10 may be implemented using multiple processors.

[0010] Processor 12 is coupled to a processor bus 14. Processor bus 14 transmits data signals between processor 12 and other components in mobile device 10. Device 10 also includes a memory 16. In one embodiment, memory 16 is a Dynamic Random Access Memory (DRAM) device. However, in other embodiments, memory 16 may be a Static Random Access Memory (SRAM) device, or other memory device.

[0011] Memory 16 may store instructions or code represented by data signals that may be executed by processor 12. According to one embodiment of the invention, a cache memory 12.1 resides within processor 12 and stores data signals that are also stored in memory 16. Cache 12.1 speeds up memory accesses by processor 12 by taking advantage of its proximity to processor 12. In another embodiment, cache 12.1 resides external to processor 12.

[0012] Mobile device 10 further includes a bridge memory controller 18 coupled to processor bus 14 and memory 16. Bridge/memory controller 18 directs data signals between processor 12, memory 16, and other components in device 10 and bridges the data signals between processor bus 14, memory 16, and a first input/output (I/O) bus 20. In one embodiment, I/O bus 20 may be a single bus or a combination of multiple buses.

[0013] In a further embodiment, I/O bus 20 may be a Peripheral Component Interconnect adhering to a Specification Revision 2.1 bus developed by PCI Special Interest Group of Portland, Oreg. In another embodiment, I/O bus 20 may be a Personal Computer Memory Card International Association (PCMCIA) bus developed by PCMCIA of San Jose, Calif. Alternatively, other buses may be used to implement I/O bus 20. I/O bus 20 provides communication links between components in device 10. A display device controller 22 is coupled to I/O bus 20. Display device controller 22 allows coupling of a displayed device to device 10 and acts as an interface between the display device and device 10. In one embodiment, display device controller 22 is a Monochrome Display Adapter (MDA) card. In other embodiments, display device controller 22 may be a Color Graphics Adapter (CGA) card, and Enhanced Graphics Adapter (EGA) card, and Extended Graphics Array (XGA) card or other display device controller. The display device receives data signals from processor 12 through display device controller 22 and displays information and data signals to a user of device 10.

[0014] Mobile device 10 further includes a wireless communications module 24 which is coupled to I/O bus 20. Components of the wireless communications module 24 is shown in greater detail in FIG. 2 of the drawings. Referring to FIG. 2, it will be seen that the wireless communications

module **24** includes a position sensor **24.1**. The position sensor **24.1** may be any commercially available position sensor and in one embodiment it may be a GPS sensor. The module **24** further includes a digital map **24.2** which is an area coverage map indicating which communications networks are operative at a global position of mobile device **10**. The module **24** further includes an intelligent roaming controller **24.3** which provides the functionality of selecting one of radio interfaces **24.4** to connect mobile device **10** to a selected operative communications network as will be described in greater detail below. Finally, the module **24** includes a baseband logic module **24.5**. The detailed components within the baseband logic module **24.5** have not been shown. However, one skilled in the art will understand that it will necessarily include components such as a digital signal processor, embedded controller support blocks such as volatile and nonvolatile memory, clocks, interface logic and any miscellaneous hardware acceleration blocks required by the radio interfaces **24.4**. The baseband logic module **24.5** is coupled to the I/O bus **20**.

[0015] According to embodiments of the invention, the mobile device **10** may be a mobile device such as a notebook computer, Portable Digital Assistant (PDA), a mobile telephone, etc. The mobile device **10** may be used to perform operations shown in **FIG. 3** of the drawings. Referring to **FIG. 3**, at block **30** the mobile device **10** determines its location relative to a locally defined coordinate system or a global coordinate system. The particular operations performed in order to determine the location of mobile device **10** at block **30** is shown in **FIG. 4** of the drawings. Referring to **FIG. 4**, at block **30.1** a determination is made as to whether a local position sensor exists. If such a position sensor exists then at block **30.2** a current global of mobile device **10** is obtained from said local sensor. Alternatively, if no local sensor exists then at block **30.3**, a determination is made as to whether a network connection is available. If a network connection is available then at block **30.4** a check is made to determine if the network connection is capable of determining the current position of mobile device **10**. According to one embodiment of the invention, this may be achieved by accessing a database of services provided by a network operator, for which services a current user of mobile device **10** is subscribed. If the network connection is capable of determining a current position of mobile device **10** then at block **30.5** said current position is obtained from the network. Obtaining the current position involves sending a triangulation signal to the network operator, who would then triangulate a signal, and receiving said triangulated signal.

[0016] Referring now to **FIG. 3** of the drawings, after the position/location of mobile device **10** has been determined at block **30**, at block **32** the security zone in which mobile device **10** is operating is determined. The particular operations involved in determining the security zone at block **32** are shown in greater detail in **FIG. 5** of the drawings. Referring to **FIG. 5**, at block **32.1** a determination is made as to whether a network connection is available. If a network connection is available then at block **32.2** location information is sent to the network and based on this information a request is made for an update to the current security zone within which the mobile device **10** is operating. If no network coverage is available then at block **32.3** a digital network coverage map including security zones is accessed in order to determine the current security zone. Each security zone is determined in accordance with the current location

or position of mobile device **10**. Typically, security zones are user-defined for locations such as a home location, a work location, an airport location, hotel location, etc. Associated with each security zone is an access protocol which configures access control parameters to mobile device **10** which will determine, for example, whether a screen saver locks, and hence requires passwords to re-authenticate, a lead idle time before the screen saver locks, when to power down the apparatus, when to reset the apparatus and require re-authentication, when to use automatic roaming, when to make electronic payments and the type of external access request that may be accepted.

[0017] Referring again to **FIG. 3** of the drawings, at block **34** the appropriate access policy for the current security zone is obtained and applied at block **36**. At block **38** a determination is made as to whether a system shut down request has been received. If a system shut down request has been received then the system shuts down, failing which operations starting at block **30** are repeated.

[0018] One advantage of the present invention is that it provides a security system that is capable of modifying the access policy of a mobile device based on the location of the device.

[0019] For the purposes of this specification, a machine-readable medium includes any mechanism that provides (i.e. stores and/or transmits) information in a form readable by a machine (e.g. computer) for example, a machine-readable medium includes read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory device s; electrical, optical, acoustical or other form of propagated signals (e.g. carrier waves, infra red signals, digital signals, etc.); etc.

[0020] It will be apparent from this description the aspects of the present invention may be embodied, at least partly, in software. In other embodiments, hardware circuitry may be used in combination with software instructions to implement the present invention. Thus, the techniques are not limited to any specific combination of hardware circuitry and software.

[0021] Although the present invention has been described with reference to specific exemplary embodiments, it will be evident that the various modification and changes can be made to these embodiments without departing from the broader spirit of the invention as set forth in the claims. Accordingly, the specification and drawings are to be regarded in an illustrative sense rather than in a restrictive sense.

What is claimed is:

1. A method comprising:

determining a position of a mobile device; and

controlling access to said mobile device based on said position.

2. The method of claim 1, wherein said position is a global position defined relative to a global coordinate system.

3. The method of claim 1, wherein said position is a local position defined relative to a local coordinate system

4. The method of claim 1, wherein controlling access to said mobile device comprises selecting a security zone associated with said position; and

applying an access protocol defined for said security zone to said mobile device, said access protocol configures access control parameters for said mobile device.

5. The method of claim 4, further comprising first defining a plurality of security zones for particular geographic areas and defining an access protocol for each security zone.

6. The method of claim 1, wherein said position is determined by transmitting a triangulation signal from said mobile device, which signal is triangulated by a network operator; and receiving a result of said triangulation.

7. The method of claim 1, wherein determining said position is achieved using a position sensor which forms part of said mobile device.

8. The method of claim 4, wherein said security zone is selected from a group comprising a work zone, a home zone, a hotel zone and an airport zone.

9. A computer-readable storage medium having stored thereon a sequence of instructions which when executed by a processor cause said processor to perform operations comprising:

determining a position of a mobile device; and

controlling access to said mobile device based on a position.

10. The computer-readable storage medium of claim 9, wherein said position is a global position defined relative to a global coordinate system.

11. The computer-readable storage medium of claim 9, wherein said position is a local position defined relative to a local coordinate system.

12. The computer-readable storage medium of claim 9, wherein controlling access to said mobile device comprises selecting a security zone associated with said position; and applying an access protocol defined for said security zone to said mobile device, which access protocol configures access control parameters for said mobile device.

13. The computer-readable storage medium of claim 12, wherein said operations further comprise first defining a plurality of security zones, each defining a geographic area; and defining an access protocol for each security zone.

14. The computer-readable storage medium of claim 9, wherein said position is determined by transmitting a triangulation signal from said mobile device, which signal is triangulated by a network operator; and receiving a result of said triangulation.

15. The computer-readable storage medium of claim 9, wherein determining said position is achieved using a position sensor which forms part of said mobile device.

16. The computer-readable storage medium of claim 12, wherein said security zone is selected from a group comprising a work zone, a home zone, a hotel zone, and an airport zone.

17. A mobile device comprising:

positioning mechanism to determine a position of said mobile device; and

a controlling mechanism to control access to said mobile device based on said position.

18. The mobile device of claim 17, wherein said position is a global position defined relative to a global coordinate system.

19. The mobile device of claim 17, wherein said position is a local position defined relative to a local coordinate system.

20. The mobile device of claim 17, wherein the controlling mechanism comprises a selection mechanism to select a security zone associated with said position; and a configuration mechanism to apply an access policy defined for said security zone to said mobile device, which access protocol configures access control parameters for said mobile device.

21. The mobile device of claim 20 further comprising an input mechanism to receive input defining a plurality of security zones for particular geographic areas; and for defining an access protocol for each security zone.

22. The mobile device of claim 17, wherein the positioning mechanism operates to transmit a triangulation signal which is triangulated by a network operator, the device then operating to receive a result of said triangulation.

23. The mobile device of claim 17, wherein the positioning mechanism comprises a position determining sensor.

24. The mobile device of claim 23, wherein the position determining sensor comprises a Global Positioning Satellite (GPS) sensor.

25. The mobile device of claim 19, wherein said security zone is selected from a group comprising a work zone, a home zone, a hotel zone, and an airport zone.

26. A mobile device comprising:

means for determining a position of said mobile device; and

means for controlling access to said mobile device based on said position.

27. The mobile device of claim 26, wherein said position is a global position defined relative to a global coordinate system.

28. The mobile device of claim 26, wherein said position is a local position defined relative to a local coordinate system.

29. The mobile device of claim 26, wherein the means for controlling access to said mobile device comprises a selection means for selecting a security zone associated with said position; and a configuration means for applying an access protocol defined for said security zone to said mobile device, which access protocol configures access control parameters for said mobile device.

* * * * *