US 20020042886A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0042886 A1

Lahti et al. (43) Pub. Date: Apr. 11, 2002

(54) SOFTWARE VIRUS PROTECTION

(76) Inventors: **Pasi Lahti**, Helsinki (FI); **Ismo Bergroth**, Helsinki (FI); **Simo Huopio**, Helsinki (FI)

Correspondence Address:
ARENT FOX KINTNER PLOTKIN & KAHN
1050 CONNECTICUT AVENUE, N.W.
SUITE 600
WASHINGTON, DC 20036 (US)

(21) Appl. No.: **09/939,717**

(22) Filed: **Aug. 28, 2001**

(30) **Foreign Application Priority Data**

Aug. 31, 2000 (GB) 0021281.1

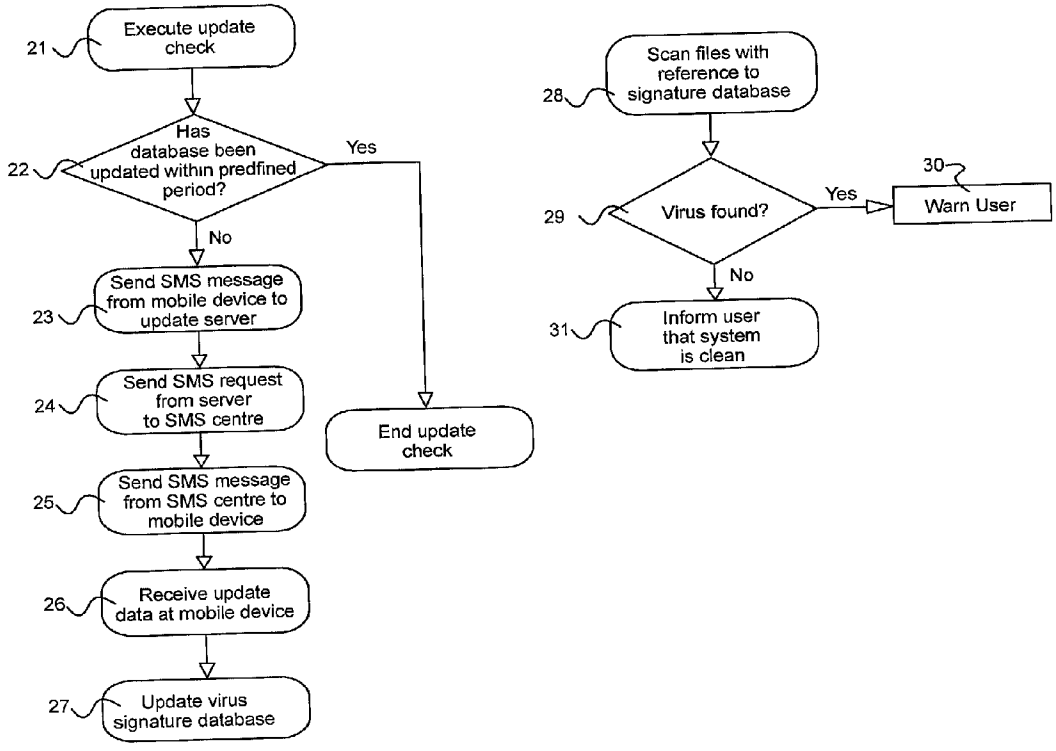
Publication Classification

(51) **Int. Cl.**[7] **G06F 11/30**

(52) **U.S. Cl.** **713/201**

(57) **ABSTRACT**

A method of protecting a wireless device against viruses, comprising maintaining a database of virus signatures on the device, updating the database by downloading virus signatures in a Short Message Service (SMS) Message, and searching for virus signatures in the memory of or files stored on the wireless device by comparison with the database.



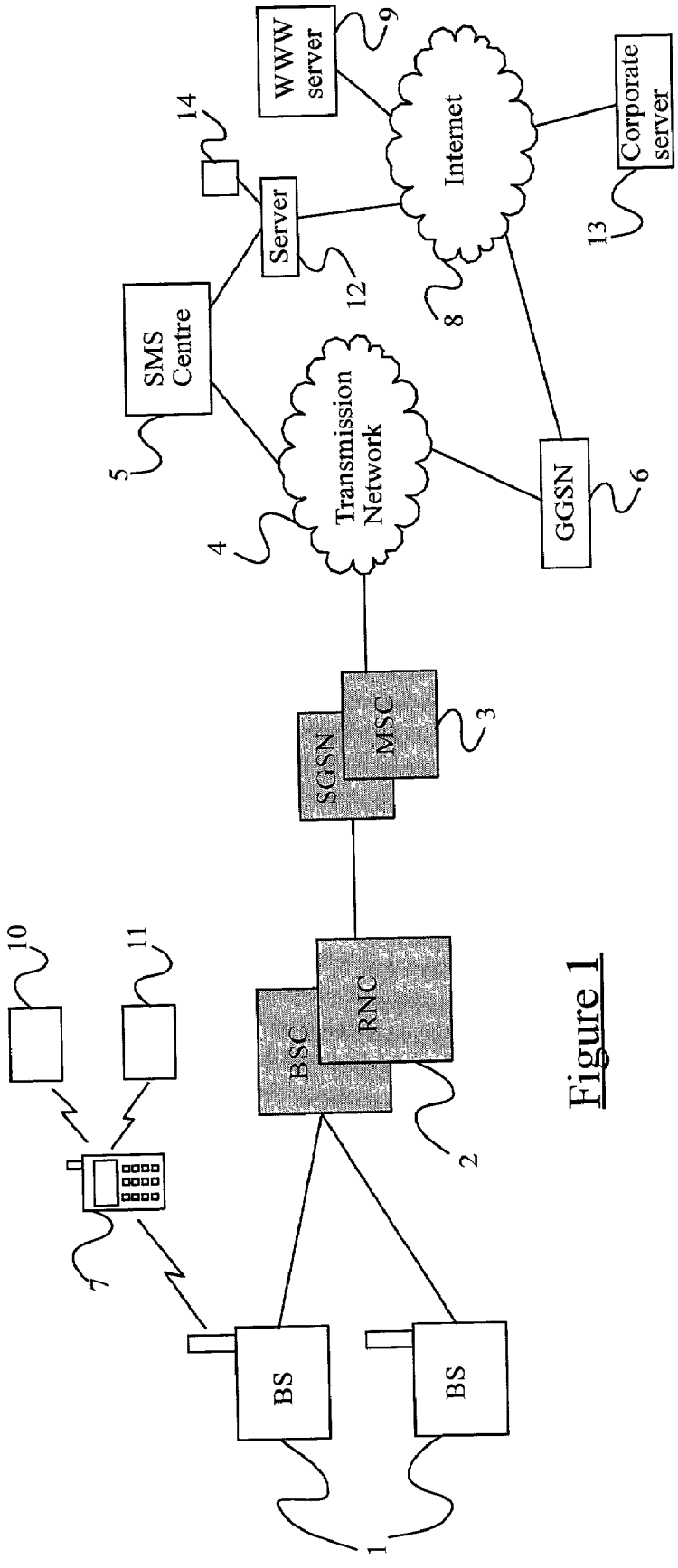

WWW server
9
Internet
Corporate server
13
14
Server
12
8
SMS Centre
5
Transmission Network
4
GGSN
6
SGSN
MSC
3
10
11
BSC
RNG
2
7
BS
BS
1

Figure 1

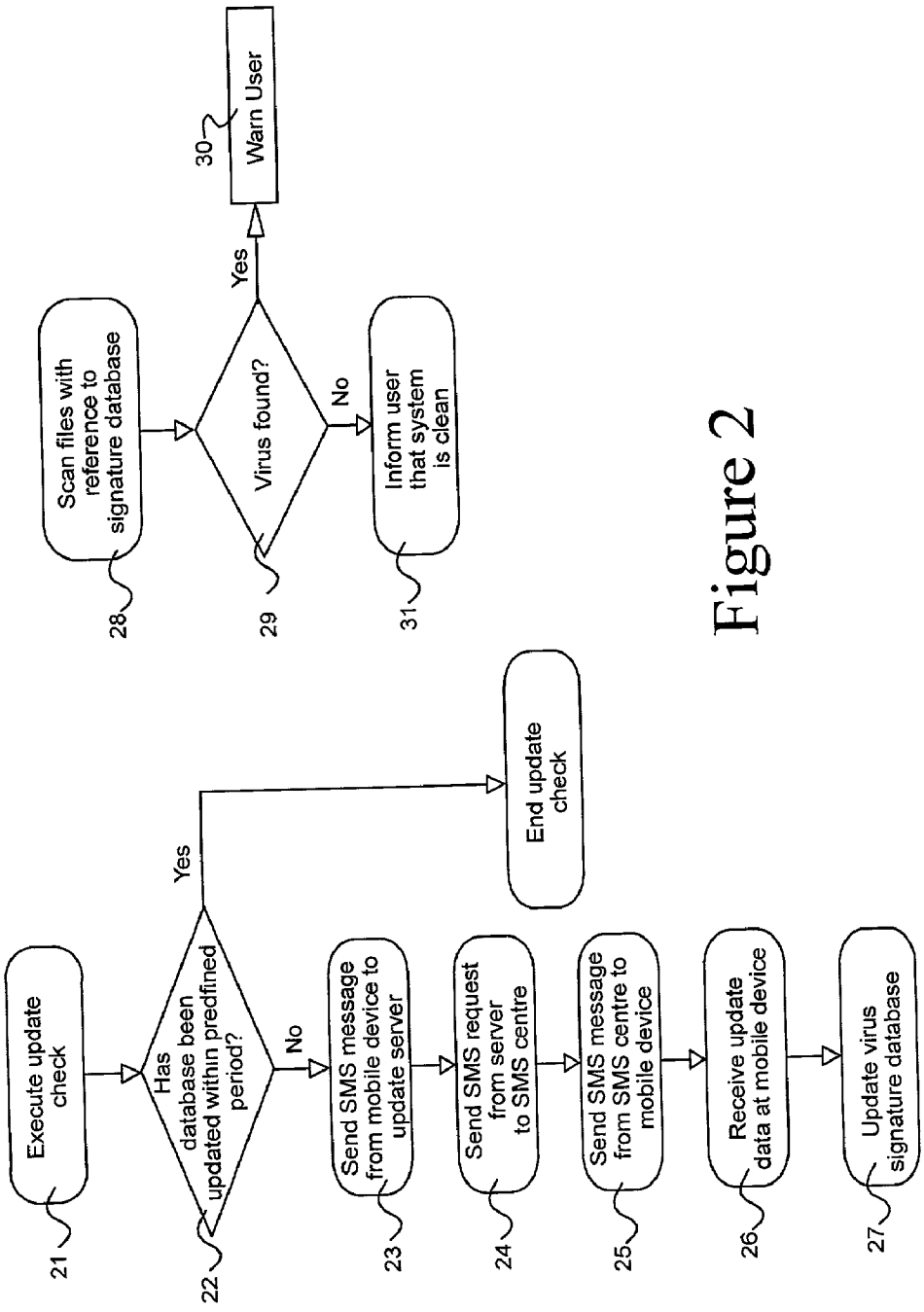

Execute update check
21
Has database been updated within predfined period?
22
Yes
End update check
No
Send SMS message from mobile device to update server
23
Send SMS request from server to SMS centre
24
Send SMS message from SMS centre to mobile device
25
Receive update data at mobile device
26
Update virus signature database
27
Scan files with reference to signature database
28
Virus found?
29
Yes
Warn User
30
No
Inform user that system is clean
31

Figure 2

SOFTWARE VIRUS PROTECTION

[0001] The present invention relates to software virus protection, and in particular to virus protection for wireless devices.

[0002] Viruses are a serious problem to users of computers. In order to combat the problem, there are a variety of anti-virus software products available which are able to identify viruses resident in the files or memory of a computer. Modem anti-virus software, such as for example F-Secure Anti-Virus for Windows NT, uses a virus signature comparison in order to identify viruses. Each virus contains code which can be analysed and recorded on a database. The database need not record all of the code contained in a virus if a unique "digital fingerprint" or signature can be recorded instead. This may be for example the overall pattern of the code, or two or three particular lines. When a signature comparison is made, the anti-virus program searches for viruses by scanning a file for the presence of a virus signature such as are present in the database.

[0003] Clearly, if effective protection is to be maintained, the database used by the anti-virus software must contain signatures for all known viruses. Unfortunately, new viruses are detected all the time, currently at the rate of one per day. Once a newly detected virus has been analysed by the anti-virus software provider and a signature created, the database must be updated on all of the computers which are using the anti-virus software. There have been various methods up until now for carrying out this update.

[0004] The earliest method used by virus software providers was to send a diskette through the mail to registered users of the anti-virus software, this diskette containing the required updates to the database. Another method has been to make the virus updates available on-line, so that they can be obtained by connecting to a remote server maintained by the anti-virus software provider. Updates have also been provided in the form of attachments to e-mail.

[0005] Increasingly, mobile phones are being used to connect to the Internet. Mobile Internet access is being facilitated by new networks (incorporating HSCSD and GPRS) as well as other protocols such as WAP. As mobile "platforms" with wireless modems and internet connections become more powerful, Internet connections will be as easy to obtain as for a desktop PC. This increase in the usage and capacity of mobile platforms renders them susceptible to attack by viruses. The methods outlined above for updating anti-virus software can also be used for mobile platforms. However, in general they will not be permanently connected to the Internet, and indeed may only connect to the Internet occasionally. This can lead to the signature database used by anti-virus software becoming out of date, rendering protection incomplete. Out of date protection can be worse than no protection at all, as it can engender a false sense of security in a user.

[0006] It is, therefore, an object of the present invention to provide a means for updating anti-virus signature databases on mobile platforms.

[0007] According to a first aspect, the present invention provides a method of updating a virus signature database used by anti-virus software operating on a mobile wireless platform, the method comprising sending update data via a signalling channel of a mobile telecommunications network to the mobile wireless platform.

[0008] The update data sent to the mobile wireless platform may be a virus signature database update, or may be a software update such as a software patch.

[0009] Preferably, the network is a GSM based network or an evolved GSM network such as GSM phase 2 (including GPRS) or UMTS (3GPP).

[0010] Preferably, the update data is obtained in one or more Short Message Service (SMS) messages. The SMS protocol, as set out for example in the ETSI GSM 03.40 specification, is a protocol which is well known and widely used for data transfer between mobile devices. For example, programs executing on top of the EPOC operating system have access to SMS communications.

[0011] Alternatively, the update data may be carried by one or more Unstructured Supplementary Services Data (USSD) messages.

[0012] In order to prevent the update information from attack, the payload of the message carrying the update data is preferably cryptographically signed.

[0013] The mobile platform may be a mobile telephone, communicator, PDA, palmtop or laptop computer, or any other suitable platform.

[0014] The mobile platform may send a report to a management centre following the successful receipt and installation of the update data. More preferably, this is returned to a management centre using an SMS message.

[0015] In a preferred embodiment, the present invention provides a method of protecting a wireless device against viruses, comprising maintaining a database of virus signatures on the device, updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages, and searching for viruses contained in the database.

[0016] Some preferred embodiments of the invention will now be described by way of example only and with reference to the accompanying drawings, in which:

[0017] **FIG. 1** is a schematic diagram showing a system according to a preferred embodiment of the invention; and

[0018] **FIG. 2** is a flow diagram of a method of protecting a mobile device from attack by viruses according to a preferred embodiment of the present invention.

[0019] **FIG. 1** illustrates a UMTS Mobile Network comprising a UMTS Terrestrial Radio Access Network (UTRAN) consisting of Base Stations (BS) **1** and Radio Network Controllers (RNCs) **2**, and a core network consisting of MSCs (and SGSNs) **3** and a transmission network **4** (RNCs of the UTRAN may be supplemented with BSCs to facilitate interworking with the GSM standard). Also present in the core network are a Short Message Service (SMS) centre **5** and a GPRS Gateway Support Node (GGSN) **6**. For the sake of simplicity, **FIG. 1** shows only a single RNC **2** and MSC (SGSN) **3**. It will be appreciated that further nodes will be present in a UMTS network in practice. A mobile wireless device **7** can connect to other telecommunication devices (e.g. mobile telephones, fixed line telephones, etc)

via the UTRAN and the core network (of course other networks including "foreign" mobile networks and PSTN networks may be involved in such connections). Using the GGSN **6**, the device **7** is able to connect to the Internet **8**. A user of the mobile wireless device **1** may thus contact for example a remote web server **9** by entering the URL of the web server into his device's Internet browser. The mobile device **1** may also communicate with a bluetooth device **10** and a Local Area Network (LAN) **11**. By way of example, the mobile device **1** may use the EPOC™ operating system.

[**0020**] In view of the risk that viruses could be downloaded from another mobile device, from the remote server **9** via the Internet **8**, from the bluetooth device **10**, or from another node of the LAN **11**, the device **1** is provided with an anti-virus software application which may check any files downloaded from an external source, together with files already resident on the device's system. As explained above, this software searches files for virus "signatures" so that, in order to be fully effective, it requires its database of virus signatures to be updated regularly.

[**0021**] There are various known methods for obtaining updates to a database of virus signatures. One method is to periodically receive media (e.g. floppy disks, compact discs) with the updates recorded thereon. However, this is a cumbersome and expensive method and will result in fewer updates being made, with the database never being fully up to date. A better method is for the user of the mobile device to contact a remote web server operated by the provider of the anti-virus software. The necessary data to update the anti-virus database can then be downloaded from that server. As explained above however, very few mobile devices are permanently connected to the Internet, and in may cases users will only connect to the Internet infrequently. This method also relies on the user remembering to connect to the remote anti-virus server periodically in order to obtain the update data. Thus there will again be periods of time during which the database is not fully up to date.

[**0022**] In order to overcome these problems use may be made of the SMS centre **5** within the UMTS core network. SMS is a service provided by current GSM networks for sending short messages over a signalling channel, and is expected to be provided also by UMTS networks.

[**0023**] The SMS centre **5** is located in the core network part of the UMTS network and is coupled to the Internet **8** via an anti-virus server **12** which is operated and controlled by the UMTS network operator. The anti-virus server **12** receives regular updates (e.g. every morning) from an update server **13** maintained by the anti-virus software provider. The SMS server **12** maintains a record of all subscribers to the anti-virus service in a database **13**, and initiates virus signature database updates by sending a Short Message Service (SMS) request for each of the registered subscribers (including the user of the mobile device **1**) to the SMS centre **5**. Upon receipt of a request, the SMS centre **5** generates a corresponding SMS message and send this to the destination mobile device via the Mobile Switching Centre **3** of the core network and the UTRAN. The SMS message contains virus signature data enabling the mobile device **1** to update the anti-virus database to include signatures for those viruses discovered since the last update was made.

[**0024**] As SMS messages can carry only relatively small quantities of information, it may be necessary for the SMS centre **5** to send a "concatenated message", (i.e. several SMS messages) to convey all the necessary information to perform a database update. For the same reason it is desirable to be able to reduce the volume of information sent as part of a virus signature database upgrade. Thus, whilst SMS updates may be sent automatically to all subscribers from the network, it is preferable to send an SMS message to the server **12** from a device **1** (via the SMS centre **5**), containing details of which virus signatures are currently stored in the device's signature database. On receipt of such an SMS request, the anti-virus server **12** needs only to issue an SMS request to the SMS centre **5** containing virus signatures not currently on the signature database of the mobile device **1**.

[**0025**] As noted in the preceding paragraph, SMS updates may be sent automatically from the network to subscribers, or may be triggered by requests from subscribers. **FIG. 2** is a flow diagram illustrating the sequence of steps involved in a subscriber initiated updating process. The mobile device executes the anti-virus software **21**. This is usually done when the device is switched on. The anti-virus software, which uses a database of virus signatures, checks to determine when the database was last updated **22**. If the last update took place more than a pre-defined period ago, e.g. one week, the software causes the device to send an SMS message **23** to the server anti-virus **12** via the SMS centre **5**. This message contains data regarding the current status of the database.

[**0026**] In reply to this SMS message, the anti-virus server **12** returns an SMS request **24** (or several SMS messages forming a "concatenated message") to the SMS centre **5**, the request containing signatures for viruses discovered and analysed since the previous update. The SMS centre **5** generates a corresponding SMS message **25** and sends this to the mobile device **1**, which receives the message **26** and causes the new signature(s) to be incorporated into the anti-virus signature database for future use **27**.

[**0027**] When next requested, or otherwise triggered (e.g. by a scanning scheduler), the anti-virus software scans the files and memory of the mobile device in order to determine the presence of any of the virus signatures in its database **28**. If an infected file is discovered **29**, the user is warned **30** and given an opportunity to delete or clean that file. Otherwise, once all files have been scanned, the software informs the user that his system is "clean"**31**.

[**0028**] It will be appreciated that there are other embodiments which fall within the scope of the invention. For example, the method of the present invention may be used to update the anti-virus software itself, e.g. by sending software patches.

1. A method of updating a virus signature database used by anti-virus software operating on a mobile wireless platform, comprising sending update data via a signalling channel of a mobile telecommunications network to the mobile wireless platform.

2. A method according to claim 1, wherein the update data sent to the mobile wireless platform is a virus signature database update.

3. A method as claimed in claim 1 or **2**, wherein the network is GSM or enhanced GSM network.

4. A method as claimed in claim 3, wherein the update data is carried by one or more Short Message Service (SMS) messages.

5. A method as claimed in claim 1, **2** or **3**, wherein the update data is carried by one or more Unstructured Supplementary Services Data (USSD) message.

6. A method as claimed in any preceding claim, wherein the message carrying the update data is cryptographically signed.

7. A method as claimed in any preceding claim, wherein the mobile platform comprises a mobile telephone, communicator, PDA, palmtop or laptop computer.

8. A method as claimed in any preceding claim, and comprising sending the update data in response to a request from the mobile platform.

9. A method as claimed in claim 8, wherein said request identifies the current status of a virus signature database.

10. A method of protecting a wireless device against viruses, comprising:

maintaining a database of virus signatures on the device;

updating the database by receiving data containing virus signatures in one or more Short Message Service (SMS) or Unstructured Supplementary Services Data (USSD) messages; and

searching for virus signatures contained in the database.

* * * * *