US 20010005889A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2001/0005889 A1

Albrecht (43) Pub. Date: Jun. 28, 2001

(54) REMOTE COMPUTER VIRUS SCANNING

(75) Inventor: **Mikael Albrecht**, Espoo (FI)

Correspondence Address:
ARENT FOX KINTNER PLOTKIN & KAHN, PLLC
Suite 600
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5339 (US)

(73) Assignee: **F-Secure Oyj**

(21) Appl. No.: **09/741,084**

(22) Filed: **Dec. 21, 2000**

(30) **Foreign Application Priority Data**

Dec. 24, 1999 (GB) 9930613.6

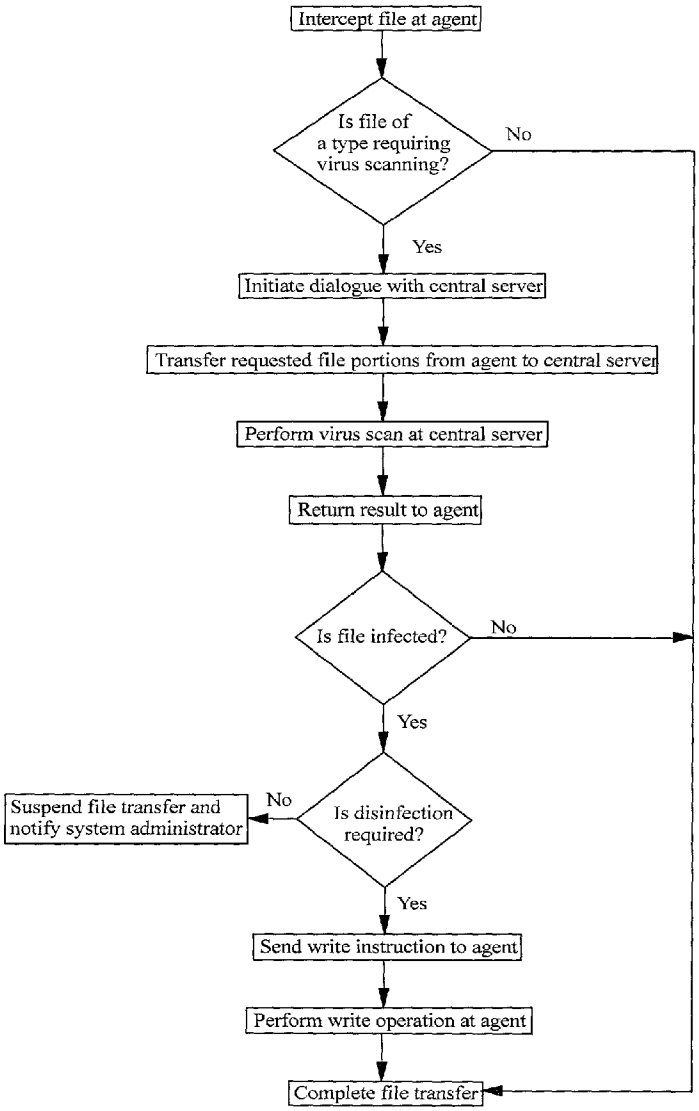
Publication Classification

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

(52) **U.S. Cl.** **713/201**; 713/188

(57) **ABSTRACT**

A method of scanning electronic files for computer viruses comprises identifying at a first node **4** of a computer network **1,** electronic files which require to be scanned for computer viruses. The first node **4** initiates a dialogue with a second node **7** of the network **1,** the second node comprising a virus scanning application. During the dialogue, the second node **7** identifies to the first node **4** one or more portions of the electronic file required by the virus scanning application. The first node **4** transfers the identified portions to the second node **7** which then carries out a virus scanning operation. The result of this operation is then returned to the first node **4.**



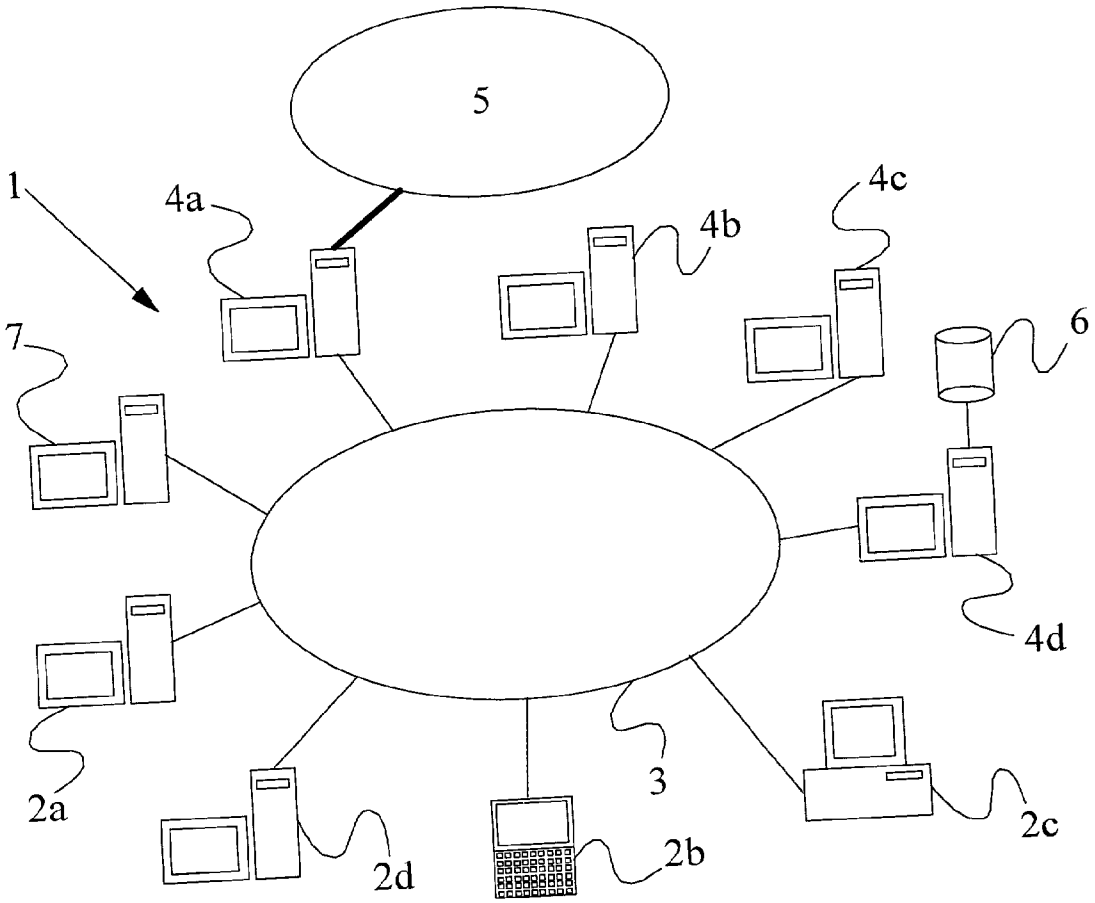


Figure 1

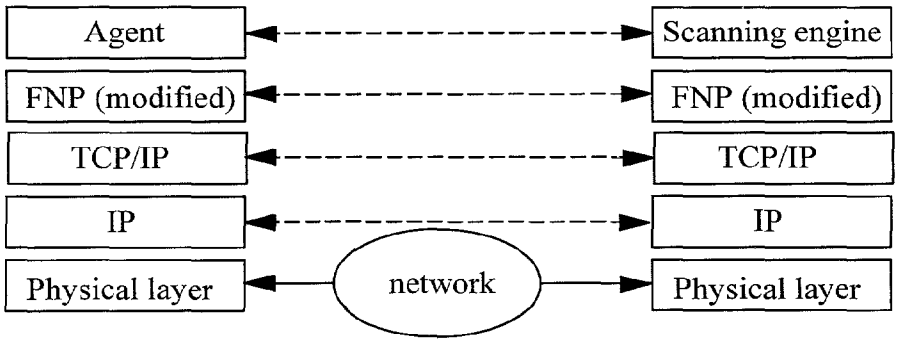


Figure 2

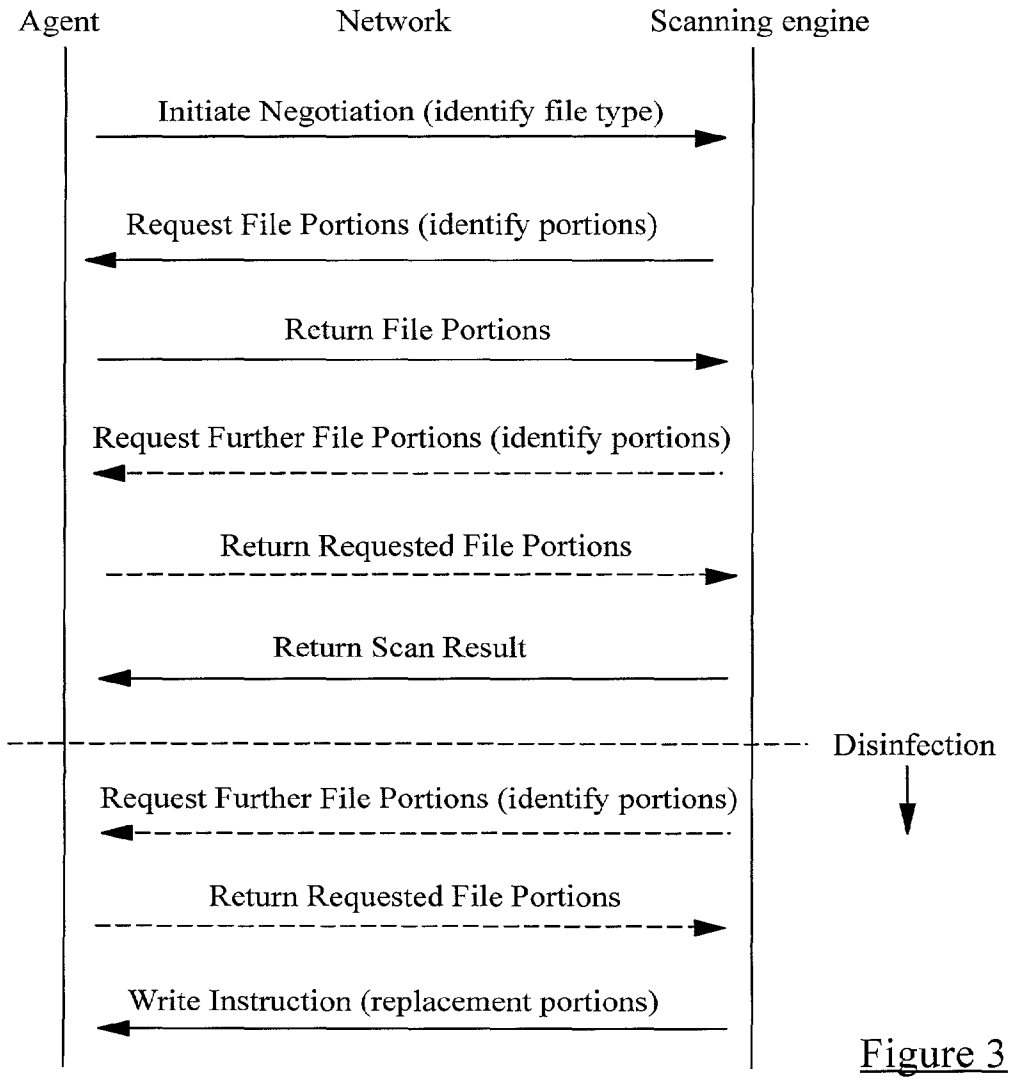


Figure 3

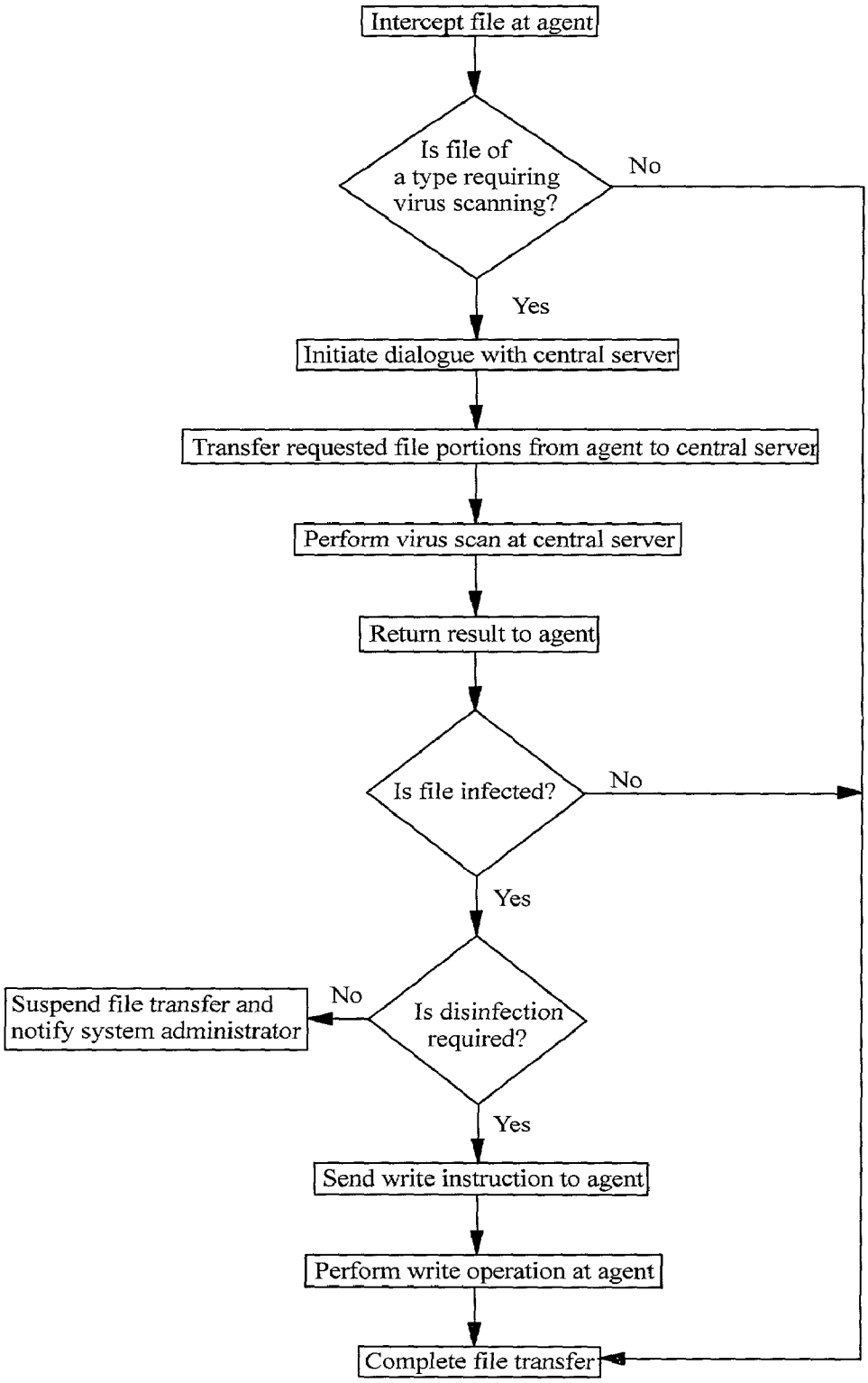


Figure 4

REMOTE COMPUTER VIRUS SCANNING

FIELD OF THE INVENTION

[0001] The present invention relates to remote computer virus scanning and in particular to virus scanning in a system where data to be scanned is transferred from an agent to a scanning engine located on a central server. The invention is applicable in particular, although not necessarily, to a system in which the agent and the server exist at different locations.

BACKGROUND TO THE INVENTION

[0002] Computer viruses are a well recognised problem in the computer and software industry and amongst computer users in general. Whilst early approaches to virus detection relied upon providing an anti-virus software application, capable of detecting previously identified viruses or suspect files, in each individual computer, the recent growth in network computing has led to the introduction of gateway based solutions. This approach involves supplementing, or in some cases replacing, the anti-virus applications running on individual computers connected to a network with anti-virus applications running on the gateway (or gateways) which connects the network to the outside world. Such a gateway based anti-virus application is typically provided at a firewall, although it may also be provided at an Internet server, mail server, etc. An anti-virus application may also be provided at a database server of the network to screen data transfers to and from a central storage location.

[0003] One network approach embodied in the F-Secure Anti-Virus Agent and Server™ product (Data Fellows Oyj, Espoo, Finland) offers an improved solution in which "agents" are located at various transit nodes of a network and identify data which is capable of containing a computer virus (by for example examining file name extensions). The intercepted suspect data is then transferred by the agent, over the network, to a central server comprising an anti-virus scanning application which performs a virus scan on the data. The result of the virus scan is returned from the central server to the agent which initiated the scan. The advantage of this approach as compared to conventional gateway scanning is that it is only necessary to provide one or a small number of scanning applications in a network. This reduces the maintenance overheads for the anti-virus application (e.g. by reducing the number of virus updates required) and also reduces the processing overheads at the machines where the agents are located. It follows that the anti-virus application is more likely to be kept up to date, and hence the security of the network is improved. A further advantage of the agent and server solution is that the scanning engine can be designed to run on one or only a small number of platforms, whilst the agent may be designed to run on a larger number of platforms—it is relatively easy to "port" the agent to different platforms as compared to the scanning engine.

[0004] A disadvantage of the approach described in the preceding paragraph is that it may require the transfer of relatively large volumes of data over a computer network. This can slow down the virus scanning operation and may also result in network traffic congestion, having a knock-on effect on non-virus scanning related traffic. The transfer of unsecure information over a network may also introduce security risks.

SUMMARY OF THE PRESENT INVENTION

[0005] The inventor of the present invention has realised that in many cases, although large volumes of data may be transferred between an agent and a central virus scanning server, the scanning application actually only looks at or examines a relatively small proportion of this data. For example, the scanning application may in some cases be able to tell that a document is not infected with a virus merely by looking at the template-bit in the header of a Microsoft Word™ document.

[0006] It is an object of the present invention to overcome or at least mitigate the above noted disadvantages. In particular, it is an object of the present invention to reduce the volume of data which must be transferred between an agent and a server for the purpose of virus scanning.

[0007] These and other objects are achieved at least in part by transferring from an agent to a virus scanning server substantially only those portions of a file which are actually required by the scanning engine.

[0008] According to a first aspect of the present invention there is provided a method of scanning electronic files for computer viruses, the method comprising:

[0009] identifying at a first node of a computer network, electronic files which require to be scanned for computer viruses;

[0010] initiating a dialogue between said first node and a second node of the network, the second node comprising a virus scanning application, during which dialogue the second node identifies to the first node one or more portions of the electronic file required by the virus scanning application; and

[0011] transferring the identified portion(s) from the first node to the second node over the network.

[0012] Embodiments of the present invention do not necessarily require the transfer of entire electronic files from the agent to the server. Rather, the embodiments only require those parts which are of direct interest to the scanning application to be transferred. For example, the scanning application may require the transfer of only a header portion of an electronic file or of a block of data pointed to by a jump instruction located in the header. In addition to reducing the volume of network traffic, embodiments of the present invention increase network security by avoiding the need to transfer entire files on a possibly insecure network.

[0013] Preferably, the method of the present invention involves identifying electronic files which require virus scanning, at a plurality of first nodes of the computer network. A dialogue is then initiated between the first nodes and the said second node when appropriate. That is to say that a set of first nodes may be served by a single scanning application existing at a second node.

[0014] It will be appreciated that the first node(s) and the second node may be located at respective different locations in the computer network. These nodes may be personal computers workstations, etc.

[0015] The first node may be, for example, one of a database server, electronic mail server, an Internet server, a proxy server, or a firewall server.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.