(12) UK Patent Application (19) GB (11) 2 382 893 (13) A

(43) Date of A Publication 11.06.2003

(21) Application No 0220180.4

(22) Date of Filing 30.08.2002

(30) Priority Data
(31) 09948825 (32) 07.09.2001 (33) US

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto,
California 94304, United States of America

(72) Inventor(s)
John Leland Boldon
David A Martz

(74) Agent and/or Address for Service
Carpmaels & Ransford
43 Bloomsbury Square, LONDON,
WC1A 2RA, United Kingdom

(51) INT CL[7]
G06F 1/00 3/12

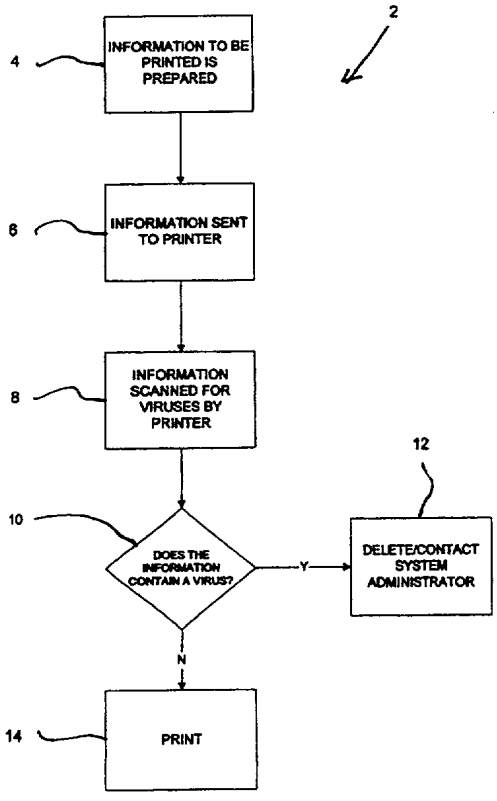
(52) UK CL (Edition V)
G4A AAP AFGDX

(56) Documents Cited
JP 110119927 A US 5623600 A
US 5434562 A

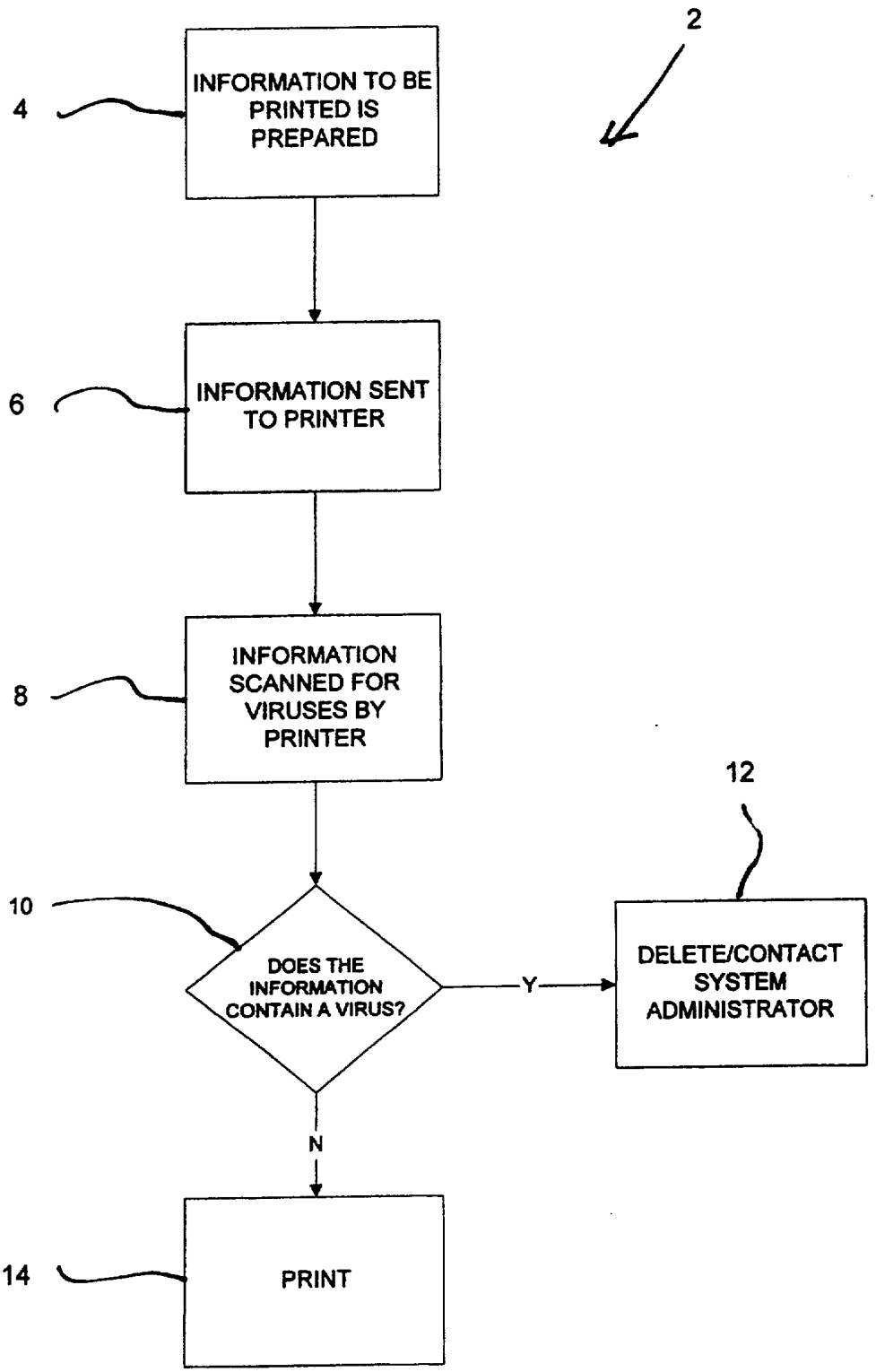
(58) Field of Search
UK CL (Edition V) G4A
INT CL[7] G06F
Other: Online EPODOC, JAPIO, WPI.

(54) Abstract Title
Method of virus filtering for use in peripherals having embedded controller devices.

(57) Disclosed is a method for filtering documents or files sent to peripherals eg printers for processing, in which the peripheral has an embedded controller. The method comprises the steps of preparing the information to be printed, sending the information to the printer, scanning the information by the printer, deciding if there is a virus in or attached to the information and printing the information if no virus is detected. The embedded controller in the printer could be a web server. The information could be deleted or the system administrator/user could be informed if a virus is detected in the information.



GB 2 382 893 A


2
4
INFORMATION TO BE PRINTED IS PREPARED
6
INFORMATION SENT TO PRINTER
8
INFORMATION SCANNED FOR VIRUSES BY PRINTER
10
DOES THE INFORMATION CONTAIN A VIRUS?
Y
12
DELETE/CONTACT SYSTEM ADMINISTRATOR
N
14
PRINT

FIGURE

METHOD OF VIRUS FILTERING FOR USE IN PERIPHERALS HAVING EMBEDDED CONTROLLER DEVICES

FIELD OF THE INVENTION

This invention relates to virus filtering. Such structures of this type, generally, employ a virus filtering for use in peripherals, such as, but not limited to, printers, scanners, facsimile machines or the like. These peripherals also contain embedded controller devices, such as, but not limited to, embedded Web servers that allow the peripheral to interact with information inputting devices, such as, but not limited to, computers, word processing devices or the like.

DESCRIPTION OF THE RELATED ART

A virus is a software program that is downloaded into a user's computer, usually unknowingly, such that the program will infect the user's computer. The effects of the virus may range from the minor to the malicious. Once the computer is infected, the virus may be spread to other computers and/or peripherals and, quite possibly, shut down the entire computing system.

It is known, in computing systems, to employ virus scanners. Exemplary of such prior art are U.S. Patent No. 5,808,751 ('751) to G. Hochman, entitled "Method and Apparatus for Messaging of Binary Files," U.S. Patent No. 6,119,165 ('165) to B. Li et al., entitled "Controlled Distribution of Application Programs in a Computer Network," and U.S. Patent No. 6,195,767 ('767) to P.M. Adams, entitled "Data Corruption Detection Apparatus and Method." While these references discuss the use of virus scanners in general-purpose devices used to do a variety of tasks, such as personal computers, a more advantageous scanning system would be employed if the scanning were done on any external data that would be coming into a peripheral device, such as a printer, scanner, facsimile machine or the like.

This is important in the current business environment, due to the fact that many remote peripherals, such as printing devices, scanners, facsimile machines or the like, can be connected to a single computing device. If the computing device becomes infected by a virus, then the virus could possibly spread to the peripherals, unless the data coming into the peripheral is screened/scanned by a virus protection firmware.

It is apparent from the above that there exists a need in the art for a scanning system which can be used with a peripheral device in order to scan any external data coming into a peripheral device and can be employed in conjunction with peripherals having embedded controller devices. It is the purpose of this invention to fulfill this and other needs in the art in a manner more apparent to the skilled artisan once given the following disclosure.

SUMMARY OF THE INVENTION

Generally speaking, this invention fulfills these needs by providing a method for scanning for viruses in print jobs, comprising the steps of: preparing information to be printed; forwarding information to a printing device; scanning the information by the printing device; determining if the information substantially contains a virus; and printing the information if no virus is detected.

In certain preferred embodiments, the printing device can be, but is not limited to, a printer, a scanner, a facsimile machine or the like. Also, the print file of the information to be printed is scanned for viruses. Finally, the method also includes the step of the deleting the information if the information contains a virus and/or contacting the system administrator if a virus is found in the information.

In another further preferred embodiment, the printing device is used to scan the information to be printed in order to substantially eliminate any malicious print jobs.

The preferred virus detection method, according to this invention, offers the following advantages: ease-of-use; excellent virus detection characteristics; use of a printer to detect the virus; good stability; good durability; and excellent economy. In fact, in many of the preferred embodiments, these factors of ease-of-use, virus detection, use of a printer to detect the virus, and economy are optimized to an extent that is considerably higher than heretofore achieved in prior, known virus detection methods.

The above and other features of the present invention, which will become more apparent as the description proceeds, are best understood by considering the following detailed description in conjunction with the accompanying drawing FIGURE and in which:

BRIEF DESCRIPTION OF THE DRAWING

The FIGURE is a flowchart that illustrates a method for detecting viruses in print jobs, according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the past, embedded peripheral devices, such as printing devices, scanners, facsimile machines or the like were similar in that:

1.) The devices performed a single function;

2.) Jobs sent to the peripherals were self-contained (in the sense that all the information needed to process the data was contained within the data stream being processed and how the data was processed was not affected by data from previous "jobs"; and

3.) The devices did not initiate the transmission of data, but rather required an external request (in the form of incoming data or a key press) before any processing activity was performed. Virus protection was not needed for such peripheral devices because the affects of any potential virus would be limited to a single document (or request) and there would be no way for the virus to be transmitted to other devices on the network (which is one of the defining characteristics of a virus).

Modern manifestations of these types of peripheral devices have greatly expanded their functionality. They may contain disk drives allowing them to retain information from one job to the next or to have their operation changed by over-writing programs stored on the disk. They may act as file servers, keeping certain documents and other files internally and then sending them (via a network) to other devices when requested. They may have the ability to receive data in the form of programming language to be interpreted and executed by the device as new functionality, so that data received by the device can actually change the way the device performs its job. Finally, the devices may contain the ability to initiate actions and the sending of data to other devices based on any number of criteria.

Because of this expanded capability, the potential for harm from a malicious or even minor virus is greatly increased. This invention, then describes a method whereby embedded peripheral devices may be able to detect and otherwise render harmless any such virus that is received by the device.

With this background and with reference to the FIGURE, there is illustrated one preferred embodiment for use of the concepts of this invention. Due to the fact that many modern printers contain embedded controller devices, such as embedded Web servers, which allow the printers to become more multifunctional, there is currently a need for a virus detection method that can detect viruses entering into the embedded controller devices. As discussed above, there are many devices/methods for detecting viruses in general-purpose devices, such as personal computers, but there currently are no virus detection methods for use in peripherals having embedded controller devices, such as printers, scanners, facsimile machines or the like.

As shown in the FIGURE, method 2 for detecting viruses in print jobs is illustrated. Method 2, preferably, includes the steps of: preparing information to be printed (step 4); conventionally forwarding the information to the printing device (step 6); scanning the information for viruses by the printing device (step 8); determining if the information contains a virus (step 10); deleting the information and/or contacting the system administrator if a virus is found (step 12); and printing the print job if no virus is found (step 14).

With respect to step 4, the information to be printed can be conventionally prepared by any known technique, such as word processing, data entry or the like.

With respect to step 6, the information, preferably, is forwarded to a conventional embedded controller device (not shown) located in the printing device and then subsequently printed, according to conventional techniques. It is also to be understood that the information to be printed can be conventionally forwarded to the print engine (not shown) located in the printing device without having to go through the embedded controller device.

With respect to step 8, the information is scanned by scanning the print file of the information to be printed with a virus protection firmware. For example, the printing device may scan an e-mail that is to be printed. In this manner, the printing device may look at the e-mail to determine if the e-mail will print a document and not attempt to write a file to a disk in the printing device and/or general-purpose device. In short, the printing device will attempt to scan any external information coming into the printing device.

If the printing device has determined that the information to be printed contains a virus, the information can be conventionally deleted and/or the system

administrator for the printing device can be conventionally contacted, as shown in step 12. In this manner, it is desired that the virus will be eliminated and/or the virus will not be introduced into other printing devices and/or general-purpose devices once a system administrator has been contacted and proper virus removal steps are taken.

If the printing device has determined that the information to be printed does not contain a virus, then the information is conventionally printed, as shown in step 14.

Once given the above disclosure, many other features, modifications or improvements will become apparent to the skilled artisan. Such features, modifications or improvements are, therefore, considered to be a part of this invention, the scope of which is to be determined by the following claims.

CLAIMS

What is Claimed is:

1. A method (2) for scanning for viruses in print jobs, comprising the steps of:

preparing information to be printed (4);

forwarding the information to a printing device (6);

scanning the information by the printing device (8);

determining if the information substantially contains a virus (10); and

printing the information if no virus is detected (14).

2. The method, as in Claim 1, wherein the forwarding step is further comprised of the step of:

forwarding the information to an embedded controller device located substantially within the printing device.

3. The method, as in Claim 2, wherein the embedded controller device is further comprised of:

an embedded Web server.

4. The method, as in Claim 1, wherein the scanning step is further comprised of the step of:

scanning a print file of the information to be printed.

5. The method, as in Claim 1, wherein the method is further comprised of the step of:

deleting the information to be printed if a virus is detected in the information (12).

6. The method, as in Claim 1, wherein the method is further comprised of the step of:

contacting a system administrator if the information to be printed contains a virus (12).

7. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for scanning for viruses in print jobs (2), comprising the steps of:

preparing information to be printed (4);

forwarding the information to a printing device (6);

scanning the information by the printing device (8);

determining if the information substantially contains a virus (10); and

printing the information if no virus is detected (14).

8. The method, as in Claim 7, wherein the forwarding step is further comprised of the step of:

forwarding the information to an embedded controller device located substantially within the printing device.

9. The method, as in Claim 8, wherein the embedded controller device is further comprised of:

an embedded Web server.

10. The method, as in Claim 7, wherein the scanning step is further comprised of the step of:

scanning a print file of the information to be printed.

Application No: GB 0220180.4
Claims searched: 1 - 10

Examiner: David P Maskery
Date of search: 1 April 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X, Y	X 1 - 5, 7 - 10, Y 2 -6 and 8 -10	JP 11119927	(MITSUBISHI ELECTRIC) See abstract and paras 8, 11 - 15.
Y	3 - 5, 9 and 10	US 5623600	(TREND MIRCO) See fig 6 and col 2 line 39 to col 3 line 16.
Y	2, 6 and 8	US 5434562	(REARDON) See col 3 lines 8 - 18 and col 5 lines 15 - 65.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

G4A

Worldwide search of patent documents classified in the following areas of the IPC[7]:

G06F

The following online and other databases have been used in the preparation of this search report:

EPODOC, JAPIO, WPI.