SYSTEM AND METHOD FOR BLOCKING HARMFUL INFORMATION ONLINE, AND COMPUTER READABLE MEDIUM THEREFOR

Technical Field

The present invention relates to computer security systems, and more particularly, to a system and method for diagnosing, remedying and blocking harmful information including computer viruses online over a computer network via which a client is linked to a web server.

Background Art

With the development of computer network based technologies, and particularly, the World Wide Web ("the Web") technology, the number of users on computer networks, and particularly, on the Internet, is rapidly expanding. Now, the Internet is no longer a new technology and service field in virtual space, but is getting into the realities of life. An ever-growing number of businesses, for example, shopping, auction, banking and advertising businesses, have established a presence on the Internet. Computer users now routinely employ the Internet to access various information, and conduct a variety of economical activities.

The Internet provides convenience to computer users in various ways. On the other hand, as computer and Internet related technologies have grown, concerns about highly possible illegal extraction of personal information or damage caused by a variety of computer viruses through computer networks are also quickly increasing. The damage caused by harmful information such as computer viruses can be serious. Reportedly, the amount of worldwide damage by computer viruses in the first half of 1999 marked a three-fold jump at $7.6 billion over 1998's $2.5 billion.

For example, the Chernobyl (CIH) virus, which is a high-risk computer virus, corrupted all of the data on a hard disk, and caused tremendous damage in the world including Korea. Recently, new harmful information such as the Back Orifice virus, or the School Bus virus which implants a "spy" file capable of remote controlling a computer, into

computers along with other computer viruses, to thereby illegally extract personal information from the computers, has been introduced onto the Internet.

An existing counterplan for protection against various harmful information is based on the first damage/post-repair policy. This protection counterplan assumes a passive position by taking measures (for example, follow-up development of appropriate antivirus programs) after computer systems have been suffered from unidentified harmful information. Another disadvantage found in the protection policy lies in that a variety of antivirus programs for protecting against harmful information need to be manually installed on individual personal computers, which is an inefficient process overloading computer users with the installation activity. Furthermore, since various harmful information is created and distributed ever quickly through the Internet, it is not easy to consistently equip computers with the latest releases of antivirus programs.

Thus, if new harmful information, such as new species of computer virus, against which appropriate antivirus programs have not been developed yet, infiltrates a user computer, it is inevitable that the computer system is damged by the new computer virus, or personal information is illegally drawn out of the computer system. In addition, a user must visit harmful information related service providers, or online communications companies to get the latest version of the antivirus program whenever an unidentified computer virus is discovered. Furthermore, downloading the latest version of the antivirus program is followed by manual installation, which is an unnecessary labor-intensive task.

The existing counterplan for protecting user computers from harmful information provides no communication channel for effectively reporting occurrences of harmful information or damage caused by the harmful information to the harmful information related service providers, so that statistical data on distribution of harmful information and damage caused by the harmful information, and the systematic data analysis thereof are not available to the harmful information related service providers.

Disclosure of the Invention

To solve the above problems, it is a first objective of the present invention to provide a system and method for blocking harmful information online, which allows a client system to actively block the harmful information, using a harmful information blocking program which is automatically transmitted and installed in the client system upon accessing to the web server via a computer network, and which inspects in real time file input/output (I/O) or network packet I/O on the client system.

It is a second objective of the present invention to provide a method for providing service of blocking harmful information online by a web server on a computer network.

It is a third objective of the present invention to provide a computer readable medium storing the harmful information blocking program.

An aspect of the first objective of the present invention is achieved by a method for blocking harmful information including computer viruses, the method comprising the steps of: (a) on a computer network through which a web server and a client system are linked to each other, the web server receiving a connection request from the client system over the computer network; (b) the web server transmitting a harmful information blocking code module to the client system; and (c) once the transmission of the harmful information blocking code module is completed, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses.

Step (c) preferably comprises the steps of: (c1) inspecting file input/output (I/O) on the client system; (c2) determining on the client system whether files inspected in step (c1) are harmful or not; and (c3) appropriately treating a file determined to be harmful in step (c2) if it can be treated, and aborting execution of a file determined to be harmful in step (c2) if it cannot be treated. In step (c3), the web server may be provided with information relating to the file determined to be harmful in step (c2).

Alternatively, step (c) may comprise the steps of: (c1) inspecting network packet input/output (I/O) on the client system; (c2) determining on

the client system whether packets inspected in step (c1) are harmful or not; and (c3) if any packet is determined to be harmful, blocking a communication port assigned for the packet I/O.

The harmful information blocking code module executed in step (c) preferably displays its running status in a separate window, and the execution of the harmful information blocking code module is aborted when the separate window is closed. It is preferable that the harmful information blocking code module executed in step (c) continues to run on the client system even when the client system assesses another web server. It is preferable that the harmful information blocking code module transmitted in step (b) is an ActiveX™ or Java™ program.

In another embodiment, the present invention provides a method for blocking harmful information including computer viruses, the method comprising the steps of: (a) on a computer network through which a first web server, a second web server and a client system are linked to each other, the client system connecting to the second web server over the computer network; (b) the client system connecting to the first web server over the computer network, according to information provided from the second web server to the client system; (c) the first web server transmitting a harmful information blocking code module to the client system; and (d) once the transmission of the harmful information blocking code module is completed, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses.

The second objective of the present invention is achieved by an online service providing method for blocking harmful information including computer viruses, the method comprising the steps of: (a) on a computer network through which a first web server and a client system are linked to each other, constructing a homepage on the first web server for online service; (b) the first web server receiving a connection request from the client system over the computer network; and (c) the first web server transmitting a harmful information blocking code module to the client

system, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses.

It is preferable that the connection request received by the first web server in step (b) is issued by the client system according to information provided from a second web server after the client system is connected to the second web server separated from the first web server.

Another aspect of the first objective of the present invention is achieved by a system for blocking harmful information including computer viruses, comprising: a first web server for providing online services through a computer network; and a client computer linked with the first web server via the computer network, wherein when the client computer is connected to the first web server via the computer network, the first web server transmits a harmful information blocking code module to the client computer, and the harmful information blocking code module is automatically executed on the client computer to block in real time harmful information including computer viruses.

It is preferable that the harmful information blocking system further comprises a second web server linked to the client computer through the computer network to provide online services through the computer network, wherein when the client computer is connected to the second web server through the computer network, the second web server provides the client computer with hyperlink information used to access to the first web server.

The third objective of the present invention is achieved by a computer readable medium having recorded thereon a computer program for blocking harmful information, the computer program transmitted from a web server to a client system through a computer network, and automatically executed on the client system, wherein the blocking of harmful information comprises the step of: (a) inspecting file input/output (I/O) of the client system; (b) determining on the client system whether files inspected in step (a) are harmful or not; (c) appropriately treating a file determined to be harmful in step (b) if it can be treated, and aborting

execution of a file determined to be harmful in step (b) if it cannot be treated; and (d) providing the web server with information relating to the file determined to be harmful in step (b).

Brief Description of the Drawings

FIGS. 1A and 1B are schematic views of systems applied to implement the present invention;

FIGS. 2A and 2B are flowcharts illustrating preferred embodiments of a method for blocking harmful information online according to the present invention;

FIG. 3 is a schematic view showing the configuration of an example of a harmful information blocking code module adopted in the present invention; and

FIG. 4 is a flowchart illustrating the operation of the harmful information blocking code module shown in FIG. 3.

Best mode for carrying out the Invention

As shown in FIG. 1A, which illustrates a system applicable to implement a preferred embodiment of the invention, a harmful information management server 110 , which is a web server, has a homepage, and is linked with a client computer 130 via a computer network, such as the Internet.

The harmful information management server 110 provides an online service for providing a harmful information blocking code module, which is capable of blocking in real time harmful information, to the client computer 130. The term "harmful information" collectively refers to an undesirable object or action that adversely effects computer systems and/or computer networks, including computer viruses, undesirable lascivious web sites on the Internet, and the act of illegally extracting personal information.

The operation of the system shown in FIG. 1A is illustrated in FIG. 2A. A first embodiment of a method for blocking harmful information online according to the present invention will be described with reference to FIG.

2A.

The method begins with a homepage being constructed for online services on the harmful information management server 110 (step 210). A computer user launches a web browser on the client computer (hereinafter, referred to as merely "client") 130 (step 220). When the client 130 is connected to the harmful information management server 110 (step 240), the harmful information management server 110 transmits a harmful information blocking code module to the client 130 (step 250).

For this case, the connection between the client 130 and the harmful information management server 110 is accomplished by a HyperText Transfer Protocol formatted request (HTTP request), and the transferring of the harmful information blocking code module from the harmful information management server 110 to the client 130 is performed by a HTTP response. In general, the HTTP request is carried out by typing the Universal Resource Locator (URL) of the harmful information management server 110 or clicking a hyperlink associated with the URL on the web browser.

Preferably, the harmful information blocking code module is an executable application program which runs on the client 130. For example, there are ActiveX™ controls designed for use in the Windows environment developed by the Microsoft Corporation, and Java™ applets and JavaScript™, which can be executed by web browser. Alternatively, an object coded program designed with a high-level language may be linked to a web browser to run.

It is preferable that the harmful information blocking code module is executed in connection with a separate window provided for user interface, and a status report for the harmful information blocking code module is displayed in the separate window. In this manner, upon the linking of the client 130 to the harmful information management server 110, first the harmful information management server 110 provides an HTTP response which enables the creation of a separate window, and then provides the harmful information blocking code module as an HTTP response with

respect to a HTTP request issued from the client 130. When the window is closed, the execution of the harmful information blocking code module is aborted. The separate window provided for user interface is applicable for various purposes, other than for displaying the running status of the harmful information blocking code module. For example, various kinds of news or banner advertisements may appear in the separate window.

When the transfer of the harmful information blocking code module is completed, the harmful information blocking code module is automatically executed on the client 130 (step 260) and blocks in real time harmful information including computer viruses (step 270). Since the harmful information blocking code module runs in real time on the client 130, unless the status displaying window is closed, the harmful information blocking code module continues to run on the client 130 even when the client 130 attempts linking to another web server. Thus, the client 130 can be provided with a harmful information blocking service for security, by a single connection to the harmful information management server 110.

Prior to description of the mechanism of the harmful information blocking code module, a variation (hereinafter, referred to as "second embodiment") of the embodiment described with reference to FIG. 1A will be described. FIG. 1B illustrates the configuration of a system applied for the second embodiment according to the present invention, and FIG. 2B is a flowchart illustrating the second embodiment of the method for blocking harmful information online according to the present invention.

As shown in FIG. 1B, the system further comprises a web server 120 (hereinafter, referred to as "second web server"), other than the harmful information management server 110, for providing online services on a network. The second web server 120 is a common web sever linked with a client system via a computer network such as the Internet.

In the present embodiment, referring to FIG. 2B, step 210 and step 220 are carried out in the same way as in the first embodiment described with reference to FIG. 2A. Next, the client 130 primarily accesse the second web server 120 (step 230).

Since the second web server 120 provide hyperlink information for use in accessing the harmful information management server 110 as well as information relating to online services to the client 130 (step 235). It is preferable that the hyperlink information is not link information for the front homepages of the harmful information management server 110, but link information that directly enables the client 130 to receive the harmful information blocking code module from the harmful information management server 110 through a separate window.

Next, the client 130 performs an HTTP request to the harmful information management server 110, according to the hyperlink information from the second web server 120 (step 245). The harmful information management server 110 transmits the harmful information blocking code module, which is an HTTP response with respect to the HTTP request issued from the client 130 (step 255).

When the transfer of the harmful information blocking code module is completed, the harmful information blocking code module is automatically executed on the client 130 (step 260), and blocks in real time harmful information such as computer viruses (step 270), as in the first embodiment.

The harmful information blocking code module will now be described in greater detail. FIG. 3 shows the configuration of an example of the harmful information blocking code module adopted in the present invention, and FIG. 4 is a flowchart illustrating the operation of the harmful information blocking code module shown in FIG. 3.

As shown in FIG. 3, the harmful information blocking code module includes an input/output management unit 310, a harmful information blocking unit 320, and an information transferring unit 330. The harmful information blocking code module is related to a separate window 340 on which its running status is displayed, and execution of the harmful information blocking code module aborts upon the closing of the separate window 340, as previously described.

The input/output management unit 310 inspects file input/output (I/O) on the client 130. The inspection of the file I/O refers to the action taken to

get file information by hooking up file I/O routines. Preferably, the input/output management unit 310 also inspects network packet I/O on the client 130 so as to block harmful information from the network. A computer virus capable of illegally extracting personal information, such as the Back Orifice virus, may be blocked by checking file I/O, or checking processes, which will be described below. Preferably, the input/output management unit 310 further has a function for monitoring any Internet address that the client 130 attempts accessing, which prevents computer users from accessing undesirable lascivious web sites.

The harmful information blocking unit 320 diagnoses whether or not a file or packet is harmful, and takes appropriate remedial action if the file or packet is harmful. The information transferring unit 330 informs the harmful information management server 110 of information on the file or packet determined to be harmful.

In the operation of the harmful information blocking code module, referring to FIG. 4, first the harmful information blocking code module, which is automatically executed on the client 130, inspects whether processes currently running on the client 130 are harmful or not (step 410). This is because all future processes can be influenced by the current processes in memory. Another reason for this is that the Back Orifice virus capable of illegally extracting personal information from a system, operates in the form of processes, and enables an external computer system to remote control a user computer.

A method for checking whether or not processes are harmful involves making a list of the ongoing processes loaded in the memory, and examining whether the files corresponding to each of the processes are harmful or not. If a file is determined to be harmful, the corresponding process is determined to be a harmful process and is then aborted. It is appreciated that an appropriate treatment may also be performed on the corresponding harmful file. Preferably, after the detection of harmful information and before performing appropriate treatment, the harmful information blocking code module informs a user of the presence of the

harmful information, and requests the user's approval to take remedial action.

Next, the harmful information blocking code module inspects every file I/O on the client 140 (step 420). As previously mentioned, the file I/O inspection is performed by hooking up file I/O routines. For example, VxD, which is the I/O routine under the Windows environment, may be hooked up for the inspection.

In step 420, network packet I/O may be inspected along with the file I/O so as to block harmful information infiltrating from a network, which was also previously mentioned. The network packet I/O inspection may be accomplished by hooking up socket I/O routines (such as the so-called "Winsock module" in the Windows environment).

Furthermore, as previously mentioned, in step 420, any Internet address that the client 130 attempts to access, may be further monitored, which prevents the accessing of undesirable lascivious web sites. This monitoring for preventing undesirable accessing can be accomplished by checking the header of a HTTP request message or a Domain Name Service (DNS) lookup message.

In other words, step 420 may involve additional functions for checking for possible occurrences of harmful information on the client 130. Subsequent operations of the harmful information blocking code module will be described with reference to file I/O inspection, however, file I/O inspection is only an example and should not be contrived as limiting the scope of the invention.

Next, it is determined whether files, which are monitored in step 420, are harmful or not (step 430). This determination can be performed by various methods, according to the type of harmful information or the necessities of applications. For example, a pattern comparison with known harmful information, for example, identified computer viruses, may be performed for the purpose of the determination. In general, computer viruses operate in a predetermined pattern, and thus the pattern comparison technique can be a tool for identifying new species of viruses.

In step 430, it is preferable to make a determination as to whether or not a network packet is harmful, or whether the client 130 attempts to access an undesirable lascivious web site.

If it is determined that the monitored information is safe, the harmful information code module performs no specified treatment on the file. Accordingly, a user is allowed to continue his or her task on the client 130 irrespective of the harmful information code blocking module.

If the monitored information is determined to be harmful, it is further determined whether the monitored information is related to file I/O or packet I/O to provide a proper treatment consistent with the harmful file or packet. Although not shown in FIG. 4, as for blocking access to an desirable lascivious web site, a HTTP request message can be reformulated to guide the client 130 to a desirable web site good for users.

In the case where the monitored information is related to file I/O, it is determined whether the harmful file can be properly treated (step 450). If the treatment is possible, the related file is treated (step 454). If the treatment is impossible, execution of the corresponding file is merely aborted (step 452). In step 454, it is preferable to notify a user that harmful information was detected, and to request approval for performing treatment on the harmful information.

Lastly, it is preferable to notify the harmful information management server 110 if information indicative of harmful information is detected from the client 130 online, using the harmful information blocking code module (step 470). If the detected information is a new kind of harmful information and thus cannot be treated, it is preferable to transmit the entire file related to the unidentified harmful information to the harmful information management server 110. Of course, it is preferable to get pre-approval regarding notification of the harmful information detection and/or the transmission of the unidentified harmful information file to the harmful information management server 110.

In other words, the present embodiment provides the function of automatically providing the harmful information management server 110

with information on harmful information detected in the client 130. Accordingly, the harmful information management server 110 is allowed to acquire statistical data on harmful information, and can thus instantaneously counteract the occurrence of an unidentified computer virus, for example, by developing an effective antivirus program. In this manner, the harmful information management server 110 analyzes the unidentified harmful information from the client 130 to develop a proper treatment program, and provides an appropriate security service for blocking harmful information from attacking the client 130, with the latest version of the harmful information blocking code module. Therefore, the present invention can prevent user computers operating in an open network environment from damage caused by various harmful information.

In the present embodiment, a communications channel for use by the harmful information blocking code module in automatically transmitting harmful information to the harmful information management server 110 may be implemented with Internet mail transfer protocol such as Simple Mail Transfer Protocol (SMTP), or File Transfer Protocol (FTP). More preferably, a specified communication channel is provided exclusively for the transmission of the harmful information.

Meanwhile, if it is determined in step 440 that harmful information is related with packet I/O, a communication port assigned for the packet I/O is blocked (step 460). If internal processes for supporting the network packet I/O via the communication channel is in progress, it is preferable to abort the processes.

Next, a proper treatment is performed on the harmful information infiltrating through the communications port in a similar way as for the harmful information related with file I/O (step 462). In step 470, the harmful information management server 110 is informed of the detection of the harmful information from the network packet I/O.

The present embodiments may be implemented as a computer readable program code. The invention may be embodied in a general purpose digital computer by running a program from a computer readable

medium, including but not limited to magnetic storage media (e.g., ROM's, floppy disks, hard disks, etc.), optically readable media (e.g., CD-ROMs, DVDs, etc.) and carrier waves (e.g., transmissions over the Internet).

While this invention has been particularly shown and described with reference to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made thereto without departing from the spirit and scope of the invention as defined by the appended claims. The embodiments should be construed as being illustrative and not as limiting the scope of the invention. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description.

Industrial Applicability

As previously described, according to the present invention, the harmful information blocking code module is automatically provided to and installed in the client system by only online connecting to the harmful information management server, so that harmful information detected on the client system can be actively blocked in real time without requiring a manual installation process.

The harmful information blocking code module has a function of informing the harmful information management server of information indicative of an unidentified computer virus detected in the client system. Accordingly, the harmful information management server can acquire useful statistical data relating to harmful information, and keeps up-to-date with the latest releases of the harmful information blocking code module, which ensures latest security service for user computers.

Furthermore, the harmful information blocking code module is able to inspect the network packet I/O, which warrants secured electronic commerce through the Internet. In particular, for private enterprises or government organizations, the present invention can be effective in actively protecting business information, or confidential information relating to national security from various harmful information. The present invention

is effective in terms of both security and efficiency.

What is claimed is:

1. A method for blocking harmful information including computer viruses, the method comprising the steps of:

(a) on a computer network through which a web server and a client system are linked to each other, the web server receiving a connection request from the client system over the computer network;

(b) the web server transmitting a harmful information blocking code module to the client system; and

(c) once the transmission of the harmful information blocking code module is completed, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses.

2. The method of claim 1, wherein step (c) comprises the steps of:

(c1) inspecting file input/output (I/O) on the client system;

(c2) determining on the client system whether files inspected in step (c1) are harmful or not; and

(c3) appropriately treating a file determined to be harmful in step (c2) if it can be treated, and aborting execution of a file determined to be harmful in step (c2) if it cannot be treated.

3. The method of claim 2, wherein in step (c3) the web server is provided with information relating to the file determined to be harmful in step (c2).

4. The method of claim 3, wherein in step (c3), if the file determined to be harmful in step (c2) cannot be treated, the file is transmitted to the web web server.

5. The method of claim 2, wherein step (c3) comprises requesting the client system user's approval for the execution of step (c3).

6. The method of claim 1, wherein step (c) comprises the steps of:

(c1) inspecting network packet input/output (I/O) on the client system;

(c2) determining on the client system whether packets inspected in step (c1) are harmful or not; and

(c3) if any packet is determined to be harmful, blocking a communication port assigned for the packet I/O.

7. The method of claim 1, wherein the harmful information blocking code module executed in step (c) checks whether current processes running on the client system are harmful or not.

8. The method of claim 1, wherein if an Internet address that the client system attempts to access is a predetermined lascivious site, the harmful information blocking code module executed in step (c) blocks access to the predetermined undesirable lascivious site.

9. The method of claim 1, wherein the harmful information blocking code module executed in step (c) displays its running status in a separate window, and the execution of the harmful information blocking code module is aborted when the separate window is closed.

10. The method of claim 1, wherein the harmful information blocking code module executed in step (c) continues to run on the client system even when the client system assesses another web server.

11. The method of claim 1, wherein the harmful information blocking code module transmitted in step (b) is an ActiveX™ or Java™ program.

12. The method of claim 1, wherein the harmful information

blocking code module has a function of detecting an unidentified computer virus by pattern comparison with an identified computer virus.

13. A method for blocking harmful information including computer viruses, the method comprising the steps of:

(a) on a computer network through which a first web server, a second web server and a client system are linked to each other, the client system connecting to the second web server over the computer network;

(b) the client system connecting to the first web server over the computer network, according to information provided from the second web server to the client system;

(c) the first web server transmitting a harmful information blocking code module to the client system; and

(d) once the transmission of the harmful information blocking code module is completed, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses.

14. The method of claim 13, wherein step (d) comprises the steps of:

(d1) inspecting file input/output (I/O) on the client system;

(d2) determining on the client system whether files inspected in step (d1) of the client system are harmful or not; and

(d3) appropriately treating a file determined to be harmful in step (d2) if it can be treated, and aborting execution of a file determined to be harmful in step (d2) if it cannot be treated.

15. The method of claim 13, wherein the harmful information blocking code module executed in step (d) continues to run on the client system even when the client system assesses another web server.

16. An online service providing method for blocking harmful

information including computer viruses, the method comprising the steps of:

(a) on a computer network through which a first web server and a client system are linked to each other, constructing a homepage on the first web server for online service;

(b) the first web server receiving a connection request from the client system over the computer network; and

(c) the first web server transmitting a harmful information blocking code module to the client system, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses.

17. The method of claim 16, wherein the connection request received by the first web server in step (b) is issued by the client system according to information provided from a second web server after the client system is connected to the second web server separated from the first web server.

18. The method of claim 16, wherein the harmful information blocking code module transmitted in step (c) determines whether a file is harmful or not by inspecting file input/output (I/O) on the client system, treats a file determined to be harmful if it can be treated; and aborts execution of a file determined to be harmful if it cannot be treated.

19. The method of claim 16, wherein the harmful information blocking code module transmitted in step (c) continues to run on the client system even when the client system assesses another web server.

20. A system for blocking harmful information including computer viruses, comprising:

a first web server for providing online services through a computer network; and

a client computer linked with the first web server via the computer network,

wherein when the client computer is connected to the first web server via the computer network, the first web server transmits a harmful information blocking code module to the client computer, and the harmful information blocking code module is automatically executed on the client computer to block in real time harmful information including computer viruses.

21. The system of claim 20, wherein the harmful information blocking code module determines whether a file is harmful or not by inspecting file input/output (I/O) on the client system, treats a file determined to be harmful if it can be treated; and aborts execution of a file determined to be harmful if it cannot be treated.

22. The method of claim 20, wherein the harmful information blocking code module displays its running status on a separate window, and the execution of the harmful information blocking code module is aborted when the separate window is closed.

23. The system of claim 20, further comprising a second web server linked to the client computer through the computer network to provide online services through the computer network, and

wherein when the client computer is connected to the second web server through the computer network, the second web server provides the client computer with hyperlink information used to access to the first web server.

24. The system of claim 20, wherein the harmful information blocking code module continues to run on the client computer even when the client computer assesses another web server.

25. A computer readable medium having recorded thereon a computer program for blocking harmful information, the computer program transmitted from a web server to a client system through a computer network, and automatically executed on the client system,

wherein the blocking of harmful information comprises the step of:

(a) inspecting file input/output (I/O) of the client system;

(b) determining on the client system whether files inspected in step (a) are harmful or not;

(c) appropriately treating a file determined to be harmful in step (b) if it can be treated, and aborting execution of a file determined to be harmful in step (b) if it cannot be treated; and

(d) providing the web server with information relating to the file determined to be harmful in step (b).

26. The computer readable medium of claim 25, wherein in step (d), if a file determined to be harmful in step (b) cannot be treated, the harmful file is transmitted to the web server.