(11) Application No. AU 2003244552 B1

(19) AUSTRALIAN PATENT OFFICE

(54) Title
Method and system for blocking unwanted e-mail

(51)6 International Patent Classification(s)
G06F 017/60 H04L 012/58

(21) Application No: 2003244552

(22) Application Date: 2003.09.04

(43) Publication Date : 2004.04.29

(43) Publication Journal Date : 2004.04.29

(71) Applicant(s)
New Millenium Solutions Pty Ltd

(72) Inventor(s)
Corby, Benjamin Victor Siddons7

(74) Agent/Attorney
Chrysiliou Law, 15-19 Parraween Street, CREMORNE, NSW, 2090

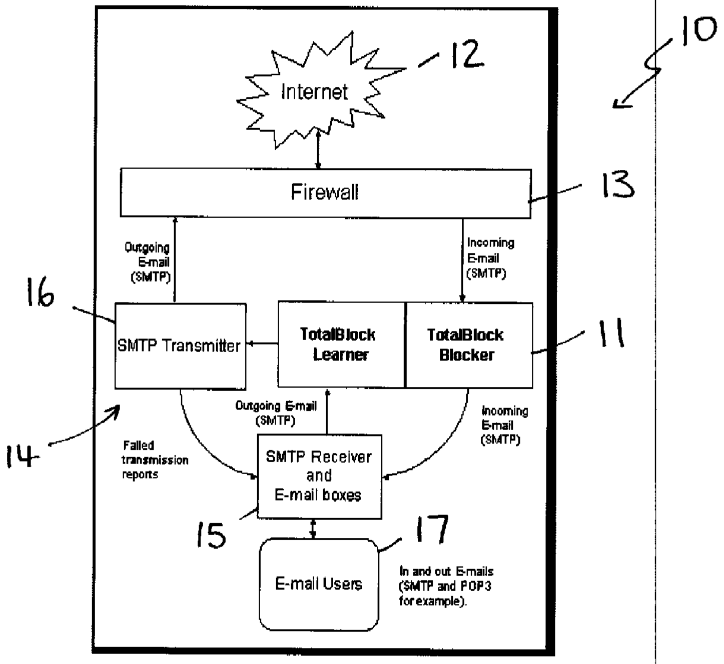
(56) Related Art
US 5956491
WO 1999/10817
US 6112227

ABSTRACT

A method blocking unwanted e-mail, SPAM or the like includes the steps of providing a system (11) for determining an e-mail source address and comparing said e-mail source address with a stored list of known addresses. If the mail is from a known source, the system (11) allows the mail to proceed to addressee, and if mail is from an unknown source, the system returns the mail to sender requesting a reply, and if reply is received, allows the mail to proceed to the addressee. Preferably, the step of returning mail to the sender requesting a reply includes the step of requesting identification of an identifiable item associated with the returned mail.

Fig. 1

1/1



10
12
Internet
Firewall
13
Outgoing E-mail (SMTP)
Incoming E-mail (SMTP)
16
SMTP Transmitter
TotalBlock Learner
TotalBlock Blocker
11
Outgoing E-mail (SMTP)
Incoming E-mail (SMTP)
14
Failed transmission reports
SMTP Receiver and E-mail boxes
15
17
E-mail Users
In and out E-mails ($MTP and POP3 for example).

Fig. 1

METHOD AND SYSTEM FOR BLOCKING UNWANTED E-MAIL

The present invention relates to electronic mail and, in particular, to a method and system for reducing SPAM or unsolicited or junk e-mail sent indiscriminately to multiple mailing lists, individuals or news groups.

BACKGROUND TO THE INVENTION

SPAM has become a major problem as it is generally computer generated and these computers are capable of generating millions of unwanted e-mails a day. As a person's e-mail address can become known through simple use such as sending personal or business e-mails across the internet, accessing internet sites and obtaining products which require e-mail information, etc. The more commonly known a person's e-mail address, the more likely that they will receive unwanted or SPAM e-mail. It is not uncommon for persons to receive up to 100 to 200 SPAM e-mails a day which results in time wasted determining which are wanted e-mails as opposed to SPAM, and then deleting the SPAM from their systems. It is estimated that 90 - 95% of the corporate server system is dedicated to managing SPAM which is a significant and unwanted overhead task.

A known method of managing SPAM is to filter the received e-mail based on its contents and to reject that e-mail that includes unacceptable words, eg viagra, however, a consequence is that sometimes wanted e-mail can be blocked and not received. Another method is to store the e-mail and challenge the sender, only forwarding the e-mail if the sender successfully responds to the challenge, however a consequence of this method is that a significant amount of e-mail is stored and never forwarded since most unsolicited e-mail is SPAM.

OBJECT OF THE INVENTION

It is an object of the present invention to provide a method and system of blocking unwanted e-mail and the like which substantially overcomes or ameliorates the above mentioned disadvantages. At the very least, the object of the invention is to provide an alternative to known systems.

DISCLOSURE OF THE INVENTION

According to one aspect of the present invention there is disclosed a method blocking unwanted e-mail, SPAM or the like, said method including the steps of providing a system for determining an e-mail source address and comparing said e-mail source address with a stored list of known addresses, wherein if e-mail is from a known source, allowing the e-mail to proceed to addressee and if the e-mail is from a known undesirable source, preventing the mail from proceeding to the addressee, and if e-mail is from an unknown source, responding to the sender's mail server in such a way that a personal sender is aware of an action to be taken to be authorized to send e-mail to the addressee and the sender's server cannot determine that the receiving address exists and if the sender correctly takes the steps to be authorized, allowing the e-mail to proceed to the addressee and not storing the original e-mail for this purpose.

Preferably, the step of responding to the sender requesting an action that includes the step of requesting identification of an identifiable item in the e-mail. In the preferred form, this step of returning the mail to the sender requesting a reply includes the step of including an identifiable item in the mail to the sender and requesting the sender to identify the item, whereby if the item is identified correctly, the mail is allowed to proceed to the addressee.

In another preferred form, this step of returning the mail to the sender requesting a reply includes the step of including a link to a web page which contains an identifiable item in the returned mail to the sender and requesting the sender to identify the item, whereby if the item is identified correctly, the mail is allowed to proceed to the addressee.

Preferably, the identifiable item can be a picture or some special text or the like whereby the picture or special text or the like cannot be identified by a computer but requires a personal response of identification.

In a preferred form, before the mail is allowed to proceed to the addressee, the system provides details of the sender to the addressee who has the option of receiving or blocking the mail. In a preferred form, this step can occur prior to returning the mail to sender requesting a reply.

Preferably, the addressee has the option of authorizing senders who are added to the stored list of known addresses. In a preferred form, receivers of outgoing mail are added to the stored list of known addresses, ie they are authorized to send mail to the addressee.

Preferably the method includes the steps of providing a stored list of addresses from which all mail is to be blocked.

Preferably, the system interrogates the incoming mail header and thereby prevents contents of mail from unknown or blocked source even being received by the server. Preferably the system replies to sender that mail is blocked in such a way that only a human will recognise the action required to be authorized.

Preferably, the method includes the steps of blocking mail servers and IP addresses.

In a preferred form the method includes the step of an administrator or user of identifying users, mail servers and IP addresses as being allowed to send mail.

In another preferred form, the method includes the step of providing a reporting facility which enables users of the system to inspect the actions of the system.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be now be described with reference to the accompanying drawing by which:

Fig. 1 is a schematic block diagram of a mail management system of a preferred embodiment.

BEST MODE OF CARRYING OUT THE INVENTION

A system 10 of a preferred embodiment of mail management is shown in Fig. 1. A mail management system 11 is seen connected to the internet 12 by a firewall 13. The mail management system 11 is installed on a server machine behind the firewall 13 on a SMTP gateway 14. The gateway 14 includes a SMTP receiver and e-mail boxes 15 and a SMTP transmitter 16. The SMTP receiver and e-mail boxes 15 portion of the gateway 14 is connected to the e-mail users 17. The SMTP servers can be any software on any platform and the user's e-mail client can be any software on any platform.

The mail management system 11 allows each e-mail user to manage their own mail management in the preferred embodiment even though a central administrator can override the individual user's management if desired.

Configuration of the system 11 is such that a list of stored addresses, whether specific (eg fred@mail.com) or group addresses (eg mail.com) or TCP/IP address or any combination of the three, are used by the system 11 to block unwanted mail. This filtering of addresses preferably works on a hierarchical basis whereby if the group address (mail.com) is blocked, but a specific address (fred@mail.com) within the group is not blocked, only the specific address in the group domain (mail.com) will be allowed.

The system 10 works in a away such that all mail is received at the server and if allowed will pass through to the user. If the mail is not identified by the list of allowable addresses, it is rejected and if the address is on the list of blocked addresses, the mail is also blocked.

The rejection of the mail occurs before the content of the mail is sent to the server and as such is not received. A SMTP reply is sent to the sender of the e-mail indicating that they must be authorized to send mail to the addressee. And contains instructions of how to be authorized. The sender can apply to be authorized to send e-mails by sending a mail to a specific authorizing address. This address is preferably dynamic and changes for each blocked e-mail. The instructions can also include an identifiable item in the returned mail to the sender and request the sender to identify the item, whereby if the item is identified correctly, the mail is allowed to proceed to the addressee. The identifiable item can be a picture or some special text or the like whereby the picture or special text or the like cannot be identified by a computer but requires a personal response of identification. In another embodiment, the returned mail contains a link to a web page which contains the identifiable item.

Following the receipt of an application for authorisation, the system 11 forwards a message to the user stating that there is a request for e-mail authorisation. The user can approve the sender responding to the e-mail or configure the system 11 to automatically authorise anyone who requests authorisation. This option is based on the assumption that computer generated SPAM mail will not have the ability to request authorisation. Once a sender has been authorised, their address is included in the authorised list. An address which has been authorised can be unauthorised or blocked at a later date.

The system 10 also allows for an address to be authorised if the user sends mail to that address without the need for user intervention.

The advantages of the systems of the preferred embodiments of the present invention ensures that all SPAM is blocked from being received. A further advantage is that the SPAM mail server cannot be aware that the mail has been rejected, but in most instances, the personal sender will understand what they must do to be authorised. If the system is installed on a network of an organisation, this benefit frees up network capacity, reduces data costs and the number of mails that must be scanned by virus protection systems. There is also a reduced amount of wasted time in handling unwanted SPAM in any way , eg no inspection, no filtering, no content checking etc.

As the system is installed on an organisation's SMTP gateway, and not a a desktop computer, it is easy to implement and administer both centrally and by users.

The system also ensures that only personally sent e-mails can be received as machine sent e-mails are blocked.

Throughout the specification and claims, the word "comprise" and its derivatives are intended to have an inclusive rather than exclusive meaning unless the context requires otherwise.

The foregoing describes only some embodiments of the present invention, and modifications obvious to those skilled in the art can be made thereto without departing from the scope of the present invention.

The claims defining the invention are as follows:

1. A method blocking unwanted e-mail, SPAM or the like, said method including the steps of providing a system for determining an e-mail source address and comparing said e-mail source address with a stored list of known addresses, wherein if mail is from a known source, allowing the mail to proceed to addressee, and if mail is from a known undesirable source, preventing the mail from proceeding to the addressee, and further including the step that if mail is from an unknown source, responding to the sender's mail server in such a way that a personal sender sender is aware of an action to be taken to be authorized to send e-mail to the addressee and the sender's server cannot determine that the receiving address exists and if the sender correctly takes the steps to be authorized, allowing the e-mail to proceed to the addressee and not storing the original e-mail for this purpose.

2. The method according to claim 1, wherein the step of responding to the sender requesting an action that includes the step of requesting identification of an identifiable item associated with the mail whereby if the item is identified correctly, further mail from the sender is allowed to proceed to the addressee.

3. The method according to claim 2, wherein the identifiable item is included in the mail to the sender and the sender is requested to identify the item.

4. The method according to claim 2, wherein the identifiable item associated with the returned mail includes the step of including a link to a web page in the mail, the web page containing an identifiable item, to the sender and requests the sender to identify the item.

5. The method according to any one of claims 2, 3 or 4, wherein the identifiable item can be a picture or some special text or the like whereby the picture or special text or the like cannot be identified by a computer but requires a personal response of identification.

6. The method according to any one of the preceding claims, wherein before the mail is allowed to proceed to the addressee, the system provides details of the sender to the addressee who has the option of receiving or blocking mail.

7. The method according to claim 6, wherein addressee has the option to receive or block the mail prior to responding to the sender.

8. The method according to claim 7, wherein the addressee has the option of authorizing senders who are added to the stored list of known addresses.

9. The method according to claim 8, wherein receivers of outgoing mail are added to the stored list of known addresses.

10 The method according to any one of the preceding claims, wherein the method includes the steps of providing a stored list of addresses from which all mail is to be blocked.

11. The method according to any one of the preceding claims, wherein the system interrogates the incoming mail header and thereby prevents contents of mail from unknown or blocked source being received by server.

12. The method according to claim 11, wherein the system replies to sender that mail is blocked in such a way that the sender is unaware that the mail was ever received.

13. The method according to any one of the preceding claims, wherein the method includes the steps of blocking mail servers and IP addresses.

14. The method according to any one of the preceding claims, wherein the method includes the step of an administrator or user of identifying users, mail servers and IP addresses as being allowed to send mail.

15. The method according to any one of the preceding claims, wherein the method includes the step of providing a reporting facility which enables users of the system to inspect the actions of the system.

16. A method blocking unwanted e-mail, SPAM or the like, said method being substantially as described with reference to the accompanying drawing.

DATED this TWENTY-NINTH day of JANUARY 2004
NEW MILLENNIUM SOLUTIONS PTY LTD
Patent Attorneys for the Applicant
CHRYSILIOU LAW

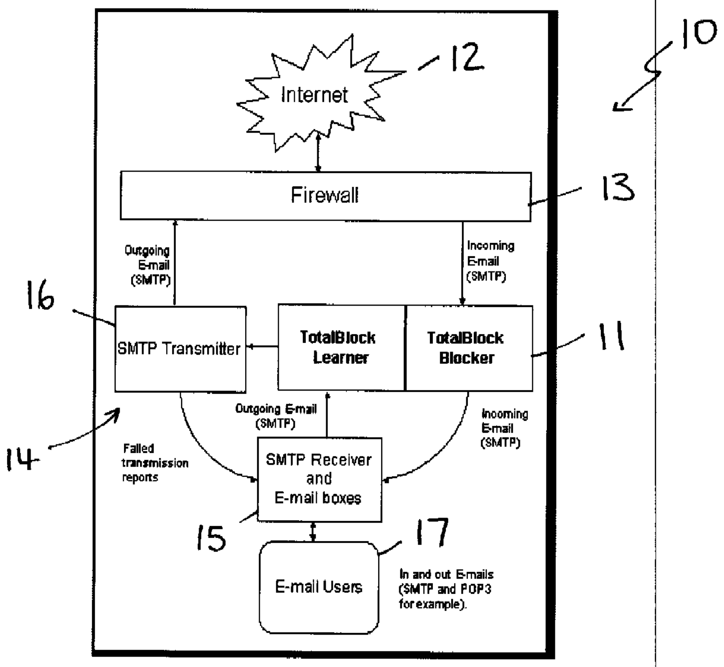

Internet
12
10
Firewall
13
Outgoing E-mail (SMTP)
Incoming E-mail (SMTP)
16
SMTP Transmitter
TotalBlock Learner
TotalBlock Blocker
11
14
Outgoing E-mail (SMTP)
Incoming E-mail (SMTP)
Failed transmission reports
SMTP Receiver and E-mail boxes
15
17
E-mail Users
In and out E-mails ($MTP and POP3 for example).

Fig. 1