(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 August 2003 (21.08.2003)

PCT

(10) International Publication Number
WO 03/069482 A2

(51) International Patent Classification⁷: G06F 12/00, H04L 9/00, 12/22, H04K 1/00

(21) International Application Number: PCT/NZ03/00030

(22) International Filing Date: 18 February 2003 (18.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
517257 18 February 2002 (18.02.2002) NZ
60/409,614 9 September 2002 (09.09.2002) US

(71) Applicant (*for all designated States except US*): **RIPPLE EFFECTS HOLDINGS LIMITED** [NZ/NZ]; 26 Penton Road, Stanmore Bay, Whangaparaoa, 1463 Auckland (NZ).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): **WATERSON, David, Lynch** [NZ/NZ]; 26 Penton Road, Stanmore Bay, WHANGAPARAOA, 1463 AUCKLAND (NZ).

(74) Agents: **ADAMS, Matthew, D** et al.; A J Park, 6th Floor Huddart Parker Building, PO Box 949, 6015 Wellington (NZ).

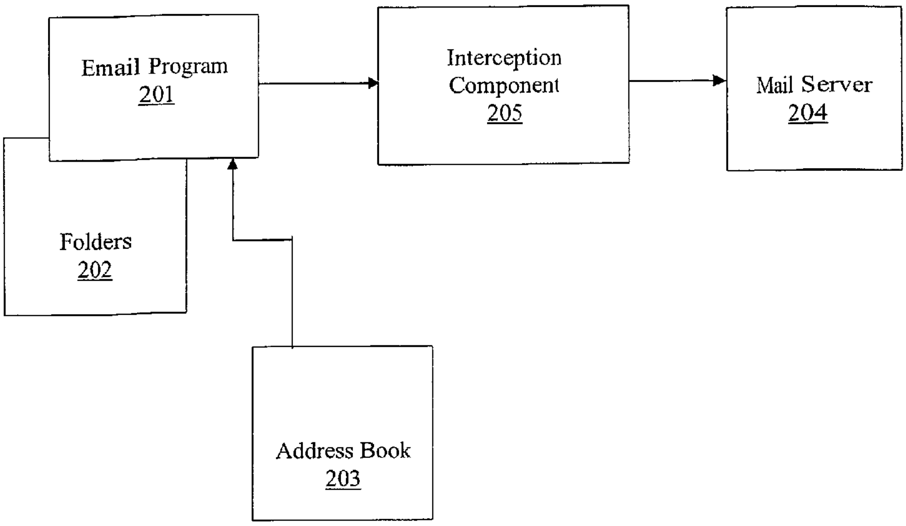
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SYSTEM FOR PREVENTING A COMPUTER VIRUS ACCESSING EMAIL ADDRESSES



(57) Abstract: A system for preventing a computer virus from accessing message addresses is described. The system comprises an interception component that communicates with a messaging client and a messaging server. The interception component receives messages from the server and forwards messages to the client. Before forwarding messages to the client the interception component replaces message addresses with a unique identifier. The interception component also receives messages from the client and forwards messages to the server. Before forwarding messages to the server the interception component replaces a unique identifier with a message addresses. Also described is a system for preventing keyboard sniffer programs from intercepting input and a system for preventing a computer virus from activating a send confirmation of a messaging client.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

"SYSTEM FOR PREVENTING A COMPUTER VIRUS ACCESSING EMAIL ADDRESSES"

FIELD OF THE INVENTION

The field of the invention generally relates to the prevention of the spread of viruses from a computer system receiving a virus, and in particular to a system for preventing a computer virus from accessing message addresses for further replication.

SUMMARY OF THE PRIOR ART

Computer viruses constitute a danger for computer users and in particular companies. Many computer virus protection software programs try to prevent computer systems being infected by scanning incoming and outgoing e-mails for virus patterns. These types of virus protection programs depend upon the virus definition files being kept up to date. When a new virus appears there is a window of opportunity for viruses to spread. In even a few hours viruses can spread rapidly, worldwide.

Many viruses carry their own SMTP commands. That is they send outgoing emails without going through the email program. If a virus operates in this manner, then the only way it can replicate is by cracking the encryption technology such as the standard 128-bit encryption. Part of the encryption formula is the user-defined password this differs on each machine. Therefore, if a hacker-initiated virus breaks the encryption, it theoretically would only do so on one machine.

A problem with conventional anti virus systems that rely on standard 128-bit encryption arises via accessing the password. Keyboard sniffer programs exist that can intercept keyboard entries. It is possible (although quite difficult) for a trojan horse program to wait until the user enters a password, and then to intercept the password. Once the virus knows the password, cracking the encryption would be difficult, but possible. If the encryption were cracked, the virus could replicate through the email program, entering via the password itself. Conventional security systems do not offer any protection against password interception. Therefore, what is needed is a new security method capable of defeating a trojan horse attack that intercepts a user's password.

Another point of failure in a conventional anti virus system occurs when the user clicks a confirmation button when sending emails with attachments that could contain a virus. For example, a virus could duplicate user keystroke actions, and activate the confirmation button itself. Thus, what is needed is a way to ensure that no keystrokes can activate the confirmation (for example, OK buttons can generally be activated by the Enter key in addition to a mouse click). This would ensure that the confirmation can only be activated by a user activated mouse click. Mouse clicks are far more difficult for a virus writer to duplicate.

However, it would be possible for a virus writer to establish the co-ordinates of a confirmation button on a screen, program the mouse to go to that position, and then to generate a mouse click at that position. Thus, what is needed is a method for ensuring that a virus cannot find the position of the email activation button.

SUMMARY OF THE INVENTION

Therefore, what is needed is a system for overcoming the above- mentioned difficulties by interrupting the spread of viruses through the use of messaging software such as e-mail. What is also needed is a system for preventing a computer virus from accessing message addresses.

In a first aspect the present invention may broadly be said to consist in a system for preventing a computer virus from accessing message addresses, said system comprising an interception component adapted to communicate with a messaging client and a messaging server, said interception component including:

means for receiving messages from said server and forwarding said messages to said client;

means for receiving messages from said client and forwarding the messages to said server;

means for identifying message addresses in messages received from said server;

means for replacing an identified message address in messages received from said server with a corresponding unique identifier;

means for identifying unique identifiers in messages received from said client; and

means for replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server.

In a second aspect the present invention may broadly be said to consist in a system for preventing a computer virus from activating a send confirmation of a messaging client comprising means for preventing keystrokes activating said send confirmation wherein said send confirmation can only be activated by other input means.

In a third aspect the present invention may broadly be said to consist in a system for preventing keyboard sniffer programs from intercepting input via a keyboard comprising:

means for adding randomly generated characters into the keyboard buffer between password keystrokes; and

means for reading said keyboard buffer; and

means for reading the stream of said randomly generated characters and removing said randomly generated characters.

In a fourth aspect the present invention may broadly be said to consist in a method of preventing a computer virus from accessing message addresses, including the steps of:

receiving messages from a messaging server and forwarding said messages to a messaging client;

receiving messages from said client and forwarding the messages to said server;

identifying message addresses in messages received from said server;

replacing an identified message address in messages received from said server with a corresponding unique identifier;

identifying unique identifiers in messages received from said message client; and

replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server.

In a fifth aspect the present invention may broadly be said to consist in a method of preventing a computer virus from activating a send confirmation of a messaging client comprising the step of preventing keystrokes activating said send confirmation wherein said send confirmation can only be activated by other input means.

In a sixth aspect the present invention may broadly be said to consist in a method of preventing keyboard sniffer programs from intercepting input via a keyboard including the steps of:

adding randomly generated characters into the keyboard buffer between password keystrokes; and

reading said keyboard buffer; and

reading the stream of said randomly generated characters and removing said randomly generated characters.

In a seventh aspect the present invention may broadly be said to consist in a system comprising:

an email or messaging server which sends and receives messages including a message address;

an email or messaging interface which replaces said external address with a unique identifier; and

an email or messaging client which sends and receives messages including a unique identifier.

In a eighth aspect the present invention may broadly be said to consist in a system for preventing a computer virus from accessing message addresses, said system comprising an interception component adapted to communicate with a messaging client and a messaging server, said interception component including:

means for receiving messages from said server and forwarding said messages to said client;

means for identifying message addresses in messages received from said server; and

means for replacing an identified message address in messages received from said server with a corresponding unique identifier.

In a ninth aspect the present invention may broadly be said to consist in a system for preventing a computer virus from accessing message addresses, said system comprising an interception component adapted to communicate with a messaging client and a messaging server, said interception component including:

means for receiving messages from said client and forwarding the messages to said server;

means for identifying unique identifiers in messages received from said client; and

means for replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server.

This invention also may be said to consist in the parts, elements and features referred to or indicated in the specification of the application, individually or collectively, and any or all combinations of any two or more of said parts, elements or features, and where specific integers are mentioned herein which have known equivalents in the art to which this invention relates, such known equivalents are deemed to be incorporated herein as if individually set forth.

Brief Description of the Drawings

Figure 1 is a diagrammatic representation of a conventional message client program including message folders and message address book.

Figure 2A is a diagrammatic representation a system for receiving incoming email according to an aspect of present invention.

Figure 2B is a diagrammatic representation a system for sending outgoing email according to an aspect of present invention.

Figure 3 is a diagrammatic representation of the system operating in an environment including a message address server according to an aspect of the present invention.

Figure 4A is a diagrammatic representation of the operation of a conventional Keyboard Buffer.

Figure 4B is a diagrammatic representation of the operation of a Keyboard Buffer when awaiting password input from the keyboard according to an aspect of the present invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

Conventional anti virus software attempts to prevent viruses from entering and leaving the system, by examining incoming and outgoing messages and attempting to identify possible viruses. In contrast, an aspect of the present invention stops viruses from replicating, by preventing viruses from spreading to other systems through the use of message addresses such as e-mail addresses.

Many viruses replicate by using message addresses found on the infected system. Viruses source message addresses in order to replicate. Figure 1 shows a typical prior art message client 100. Viruses source message addresses by checking folders 102 accessed from within messaging programs 101. Folders 102 such as Inbox, Sent box, Outbox, Drafts, are used for storing messages. Message addresses found in the headers of individual messages are used to replicate the virus.

Another source of message addresses for replicating is the address book 103 that stores details of contacts including message addresses. The virus may then proceed to send itself to the located addresses using its own embedded mail daemon.

Referring to Figures 2A and 2B, the software of the present invention includes an interception component 205 as part of an application program that operates on the same environment as the client messaging program 201. The interception component 205 acts as an intermediary between the messaging client 201 and the messaging server 204, encrypting and decrypting message addresses.

During installation, according to an aspect of the invention, an installation component of the application program changes the messaging server settings of the messaging client 201 to refer to the interception component 205 instead of the messaging server 204. With respect to the messaging client 201, the interception component 205 acts as a messaging server. With respect to the messaging server 204, the interception component acts a client messaging program.

The interception component 205 of the present invention comprises an application program running on a computer. The application program has a module to receive messages from a messaging client 201 and a module to send messages to a messaging client 201. To communicate with a messaging server 204 the application program of interception component 205 has modules to send messages to the messaging server 204 and receive messages from the messaging server 204. The messaging client 201 receiving and sending modules and the server 204 receiving and sending modules implement the functionality of standard client and server messaging protocols.

The application program of interception component 205 has a find address module to locate messaging addresses in messages received from the messaging server 204. The find address module passes located addresses to an encrypting module that has both encrypting and decrypting functions. The encrypting module encrypts message addresses and passes the encrypted address back to the find address module as a unique identifier to replace the message address.

A find identifier module is used to locate the unique identifier that has replaced the message address. The find identifier module passes the located identifier to the encrypting module for decrypting, receives a message address from the encrypting module and replaces the unique identifier with the message address. The interception component 205 also has an address book module to monitor the address book 203 of the messaging client 201. This module detects new addresses added to the address book, passes the message address to the encrypting module, receives the encrypted address from the encrypting module and replaces the address in the address book 203 with the encrypted address.

The application program of interception component 205 includes an installation component which uses the scanning modules and encrypting modules to encrypt message addresses in message folders 202 and message addresses in address books 203. The installation component has functions to replace the messaging server settings of the messaging client 201 and store the existing messaging server settings of the client 201 in the application program of interception component 205 for use by the modules that send and receive messages for the messaging server 204.

The application program also includes a scanning module message folder and a message address book scanning module. Each scanning module uses the find address module to locate message addresses and the encrypting module to encrypt any message addresses found.

Referring to Figure 3 a module of the interception component 305 to interface with a messaging address server 306 has functions to interact with both messaging clients 301 and messaging address server 306. The module receives requests for an address from the client 301 and forwards the requests to the server 306. After receiving the message address from server 306 the module passes the address to the encrypting module, receives the encrypted address and forwards the encrypted address to the messaging client 301.

The operation of the system of the present invention in use is described with reference to Fig 3 as follows. After a user composes a new outgoing message, and sends a message, the messaging client 301 forwards the message to the interception component 305. The interception component 305 decrypts the message address data and sends the message onto the messaging server 304.

To receive a new message, a user requests that the messaging client 301 check for new messages, the messaging client 301 requests that the interception component 305 checks with the messaging server 304 if there are new messages. If there are, the interception component 305 downloads the messages, identifies and encrypts the message addresses, and then passes the messages onto the messaging client 301. All message addresses entering the messaging client are thus encrypted.

Messaging clients may be set up to automatically check to see if there are new messages. In this case the messaging client 301 checks for new messages by checking with the interception component 305. The interception component 305 in turn checks with the messaging server 304. If there are new messages the interception component encrypts the addresses and forwards the messages to the client 301 in the same way as if the user had made the request to check for new mail.

As all message addresses entering the messaging client 301 are encrypted, when messages are subsequently saved in the various folders 302 within the messaging client 301, such as the Inbox, they are stored with encrypted message addresses. Message addresses stored in the address book 303 are also stored in an encrypted form as the addresses have been encrypted when messages enter the system.

The address book 303 is where details of contacts are stored, including message addresses. In the case of Microsoft Outlook Express, this is the Windows Address Book (WAB). The interception component monitors all changes to the address book. Whenever a new contact is added, the address book monitoring module of interception component 305 will encrypt the message address.

When the system component is installed for the first time, the installation component encrypts all existing message addresses found in the various folders 303 of the client message program 301, as well as all message addresses found in the address book 303.

The interception component uses an encryption key, unique to each user to prevent viruses from activating the interception component 304 in order to use it to decrypt message addresses. This technique makes it difficult for a virus to duplicate entries from a user.

The interception component can be used with message address servers 306 such as Microsoft Exchange or an LDAP Server. Address servers 306 store public addresses such as those addresses required to locate local users of the system and message addresses located outside the system. When composing a new message, the messaging client 301 may request addresses from a message address server 306, the interception component 305 intercepts the request, makes the request of the message address server 306, receives the address and encrypts the addresses before forwarding onto the messaging client 301. The message is then sent in the normal way with the interception component 305 decrypting the message address before forwarding the message onto the messaging server 304.

An additional safeguard provided by the present invention against keystroke loggers and sniffer programs is shown with reference to Figures 4A and 4B. Referring to Figure 4A, a conventional keyboard buffer 402 receives input data from a keyboard (not shown) over an input line 401. The contents of the buffer are read by a relevant software program over a suitable connection at 403.

Referring to Figure 4B, an aspect of the present invention provides a keyboard buffer scrambling feature that adds randomly-generated characters into the keyboard buffer 402 between the password keystrokes which are input at 401 into keyboard buffer 402 from a keyboard or other or other data entry device. It will be appreciated that this aspect totally defeats keyboard sniffer programs. A Trojan horse program attempting to intercept a user's password only would receive a lot of meaningless characters.

As shown in Figure 4B, a continuous stream of random characters are generated from a buffer scrambler 405 that randomly streams data in while someone enters a password to help prevent the password being picked up by a keyboard sniffer program. The buffer scrambler 405 comprises a random number generator, which also can be a cryptographic accelerator or other means for providing a variable and unpredictable stream of random characters that are sent as a data input 401 to the keyboard buffer 402. The contents of the keyboard buffer 402 are then read at 403 by a reader which is coupled with or otherwise has access shown at 407 to the random character stream provided by buffer scrambler 405. The reader 403 deletes the random characters inserted in the input data 401 from the contents of keyboard buffer 402.

By comparing the random characters with the contents of keyboard buffer 402, the reader 403 is able to reconstruct original (correct) input data 401 from the keyboard. Unauthorized software (such as keyboard buffer sniffer software) is able to access reader 403, but cannot determine the random character stream at 405 and is therefore unable to determine the input data 401.

In addition to replacing email addresses with identifiers the system on startup checks that files that could alter a message just before a message leaves the system are unchanged. The system does this by comparing the checksum of critical files with a stored checksum of those files.

As a further means to prevent viruses utilizing a messaging client to send out email the present invention modifies the messaging client to prevent the message send confirmation being activated by keystrokes. In addition the present invention replaces any button confirmation with a graphic confirmation. As a further protection the graphic confirmation is moved to a different location either at each login or each time a user prepares an email to send. This prevents a virus writer from establishing the coordinates of the graphic and programming the mouse to go to that position. The email client is modified by the installation component of the present system.

While the invention has been described in connection with what are presently considered to be the most practical and preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments, but rather is intended to cover various modifications and equivalent arrangements which are included with the scope of the claims.

For example, the features of the invention are compatible with WAP or any mobile device enabling standard. Thus, an equivalent arrangement can be accomplished by implementing the keyboard buffer scrambling feature as well as other features described above in a PDA, cell phone or other computing device. Accordingly, persons of ordinary skill in this field are to understand that all such equivalent arrangements are to be included within the scope of the claims.

CLAIMS:

1. A system for preventing a computer virus from accessing message addresses, said system comprising an interception component adapted to communicate with a messaging client and a messaging server, said interception component including:

means for receiving messages from said server and forwarding said messages to said client;

means for receiving messages from said client and forwarding the messages to said server;

means for identifying message addresses in messages received from said server;

means for replacing an identified message address in messages received from said server with a corresponding unique identifier;

means for identifying unique identifiers in messages received from said client; and

means for replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server.

2. A system for preventing a computer virus from accessing message addresses as claimed in claim 1 including:

means for identifying message addresses in stored mail of said messaging client and/or any address books of said client or client system; and

means for replacing an identified message address with a unique identifier in said stored mail and/or said any address books.

3. A system for preventing a computer virus from accessing message addresses as claimed in claim 1 or claim 2 including:

means for identifying unique identifiers in stored mail of said messaging client and/or any address books of said client or client system; and

means for replacing an identified unique identifier with a message address in said stored mail and/or said any address books.

4. A system for preventing a computer virus from accessing message addresses as claimed in anyone of claims 1 to 3 wherein:

said means for replacing an identified message address in messages received from said server with a corresponding unique identifier includes on encrypting engine; and

said means for replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server includes a decrypting engine.

5. A system for preventing a computer virus from accessing message addresses as claimed in claim 2 or claim 4 wherein said means for replacing an identified message address with a unique identifier in said stored mail and/or said any address books includes an encrypting engine.

6. A system for preventing a computer virus from accessing message addresses as claimed in anyone of claims 3 to 5 wherein said means for replacing an identified unique identifier with a message address in said stored mail and/or said any address books includes a decrypting engine.

7. A system for preventing a computer virus from accessing message addresses as claimed in anyone of claims 1 to 6 including:

means for reconfiguring the message server settings of said messaging client to point to said interception component; and

means for storing original message server settings, wherein said original message server setting are accessible by said interception component.

8. A system for preventing a computer virus from accessing message addresses as claimed in any one of claims 1 to 7 including means for monitoring one or more address books, said means for monitoring including:

means for identifying message addresses added to an address book; and

means for replacing an identified message address with a unique identifier in said address books.

9. A system for preventing a computer virus from accessing message addresses as claimed in claim 8 wherein said means for replacing an identified message address with a unique identifier in said address books includes an encrypting engine.

10. A system for preventing a computer virus from accessing message addresses as claimed in anyone of claims 4 to 9 wherein:

said encrypting engine; and

said decrypting engine,

include means for receiving a unique user identifier from a messaging client user

11. A system for preventing a computer virus from accessing message addresses as claimed in claim 10 wherein said means for receiving a unique identifier from a messaging client user includes means for preventing keyboard sniffer programs from intercepting input comprising:

means for adding randomly generated characters into the keyboard buffer between password keystrokes; and

means for reading said keyboard buffer; and

means for reading the stream of said randomly generated characters and removing said randomly generated characters.

12 A system for preventing a computer virus from accessing message addresses as claimed in anyone of claims 1 to 11 including means for preventing keystrokes activating a send confirmation of a messaging client wherein said send confirmation can only be activated by other input means.

13 A system for preventing a computer virus from accessing message addresses as claimed in claim 12 wherein said send confirmation is a button and including means for replacing said message send confirmation button with a graphic.

14. A system for preventing a computer virus from accessing message addresses as claimed in claim 13 including means for moving said graphical randomly.

15. A system for preventing a computer virus from accessing message addresses as claimed in anyone of claims 12 to 14 wherein said send confirmation is activated by a mouse.

16. A system for preventing a computer virus from activating a send confirmation of a messaging client comprising means for preventing keystrokes activating said send confirmation wherein said send confirmation can only be activated by other input means.

17 A system for preventing a computer virus from activating a send confirmation of a messaging client as claimed in claim 16 wherein said send confirmation is a button and including means for replacing said message send confirmation button with a graphic.

18 A system for preventing a computer virus from activating a send

confirmation of a messaging client as claimed in claim 17 including means for moving said graphical randomly.

19. A system for preventing a computer virus from activating a send confirmation of a messaging client as claimed in anyone of claims 16 to 18 wherein said send confirmation is activated by a mouse.

20. A system for preventing keyboard sniffer programs from intercepting input via a keyboard comprising:

means for adding randomly generated characters into the keyboard buffer between password keystrokes; and

means for reading said keyboard buffer; and

means for reading the stream of said randomly generated characters and removing said randomly generated characters.

21. A computer program comprising program instructions which when loaded into a computer constitute the processing means of any of claims 1 to 20

22. A method of preventing a computer virus from accessing message addresses, including the steps of:

receiving messages from a messaging server and forwarding said messages to a messaging client;

receiving messages from said client and forwarding the messages to said server;

identifying message addresses in messages received from said server;

replacing an identified message address in messages received from said server with a corresponding unique identifier;

identifying unique identifiers in messages received from said message client; and replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server.

23. A method of preventing a computer virus from accessing message addresses as claimed in claim 22 including the steps of:

identifying message addresses in stored mail of said messaging client and/or any address books of said client or client system; and

replacing an identified message address with a unique identifier in said stored mail and/or said any address books.

24. A method of preventing a computer virus from accessing message addresses as claimed in claim 22 or claim 23 including the steps of:

identifying unique identifiers in stored mail of said messaging client and/or any address books of said client or client system; and

replacing an identified unique identifier with a message address in said stored mail and/or said any address books.

25. A method of preventing a computer virus from accessing message addresses as claimed in anyone of claims 22 to 24 wherein:

replacing an identified message address in messages received from said server with a corresponding unique identifier includes the step of encrypting said message address; and

replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server includes the step of decrypting said unique identifier.

26. A method of preventing a computer virus from accessing message addresses as claimed in claim 23 or claim 25 wherein said step of replacing an

identified message address with a unique identifier in said stored mail and/or said any address books includes the step of encrypting said message address.

27. A method of preventing a computer virus from accessing message addresses as claimed in anyone of claims 24 to 26 wherein step of replacing an identified unique identifier with a message address in said stored mail and/or said any address books includes the step of decrypting said unique identifier.

28. A method of preventing a computer virus from accessing message addresses as claimed in anyone of claims 22 to 27 including the steps of:

reconfiguring the message server settings of said messaging client; and

storing original message server settings, wherein said original message server setting are used when

receiving messages from said messaging server; and

forwarding message to said server.

29. A method of preventing a computer virus from accessing message addresses as claimed in any one of claims 22 to 28 including the step of monitoring one or more address books, said step of monitoring including the steps of:

identifying message addresses added to an address book; and

replacing an identified message address with a unique identifier in said address books.

30. A method of preventing a computer virus from accessing message addresses as claimed in claim 29 wherein said step of replacing an identified message address with a unique identifier in said address books includes the step of encrypting said message address.

31. A method of preventing a computer virus from accessing message addresses as claimed in anyone of claims 25 to 30 wherein said steps of:

encrypting said message address; and

decrypting said unique identifier

include the step of receiving a unique user identifier from a messaging client user

32. A method of preventing a computer virus from accessing message addresses as claimed in claim 31 wherein said steps of receiving a unique identifier from a messaging client user includes the step of preventing keyboard sniffer programs from intercepting input including the steps of:

adding randomly generated characters into the keyboard buffer between password keystrokes; and

reading said keyboard buffer; and

reading the stream of said randomly generated characters and removing said randomly generated characters.

33. A method of preventing a computer virus from accessing message addresses as claimed in anyone of claims 22 to 32 including the steps of preventing keystrokes activating a send confirmation of a messaging client wherein said send confirmation can only be activated by other input means.

34. A method of preventing a computer virus from accessing message addresses as claimed in claim 33 wherein said send confirmation is a button and including the step of replacing said message send confirmation button with a graphic.

35. A method of preventing a computer virus from accessing message addresses as claimed in claim 34 including the steps of moving said graphical randomly.

36. A method of preventing a computer virus from accessing message addresses as claimed in anyone of claims 33 to 35 wherein said send confirmation is activated by a mouse.

37. A method of preventing a computer virus from activating a send confirmation of a messaging client comprising the step of preventing keystrokes activating said send confirmation wherein said send confirmation can only be activated by other input means.

38. A method of preventing a computer virus from activating a send confirmation of a messaging client as claimed in claim 37 wherein said send confirmation is a button and including the step of replacing said message send confirmation button with a graphic.

39. A method of preventing a computer virus from activating a send confirmation of a messaging client as claimed in claim 38 including the step of moving said graphical randomly.

40. A method of preventing a computer virus from activating a send confirmation of a messaging client as claimed in anyone of claims 37 to 39 wherein said send confirmation is activated by a mouse.

41. A method of preventing keyboard sniffer programs from intercepting input via a keyboard including the steps of:

adding randomly generated characters into the keyboard buffer between password keystrokes; and

reading said keyboard buffer; and

reading the stream of said randomly generated characters and removing said randomly generated characters.

42. A computer program comprising program instructions for causing a computer to perform the process of any of claims 22 to 41.

43. A system comprising:

an email or messaging server which sends and receives messages including a message address;

an email or messaging interface which replaces said external address with a unique identifier; and

an email or messaging client which sends and receives messages including a unique identifier.

44. A system for preventing a computer virus from accessing message addresses, said system comprising an interception component adapted to communicate with a messaging client and a messaging server, said interception component including:

means for receiving messages from said server and forwarding said messages to said client;

means for identifying message addresses in messages received from said server; and

means for replacing an identified message address in messages received from said server with a corresponding unique identifier.

45. A system for preventing a computer virus from accessing message addresses, said system comprising an interception component adapted to communicate with a messaging client and a messaging server, said interception component including:

means for receiving messages from said client and forwarding the messages to said server;

means for identifying unique identifiers in messages received from said client; and

means for replacing an identified unique identifier with a corresponding message address before sending the message received from said client to said server.

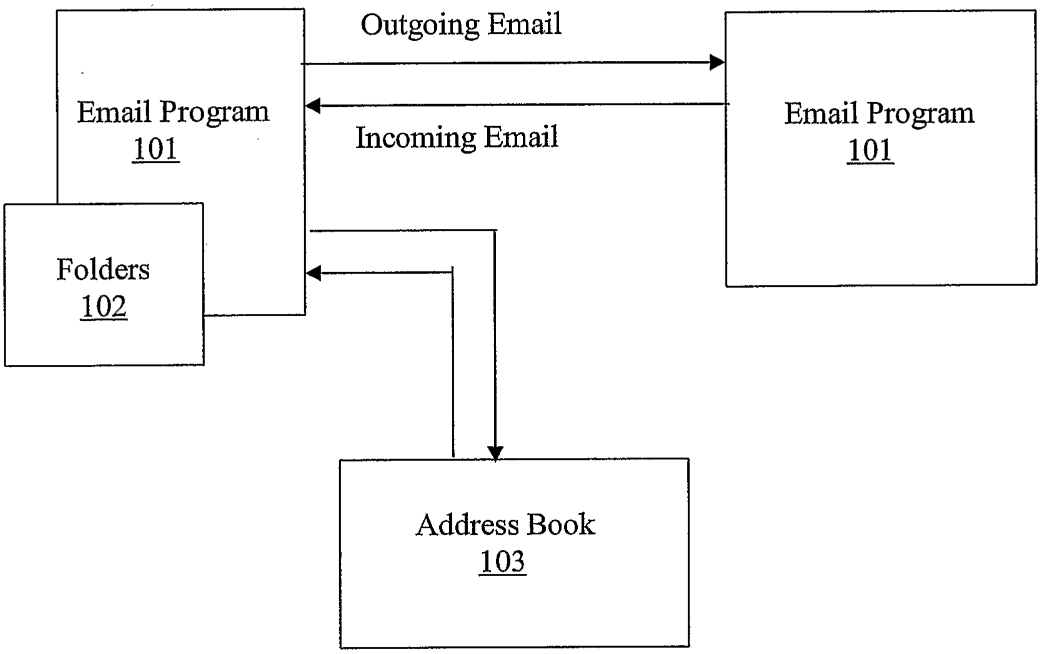

Outgoing Email
Email Program
101
Incoming Email
Email Program
101
Folders
102
Address Book
103

FIGURE 1

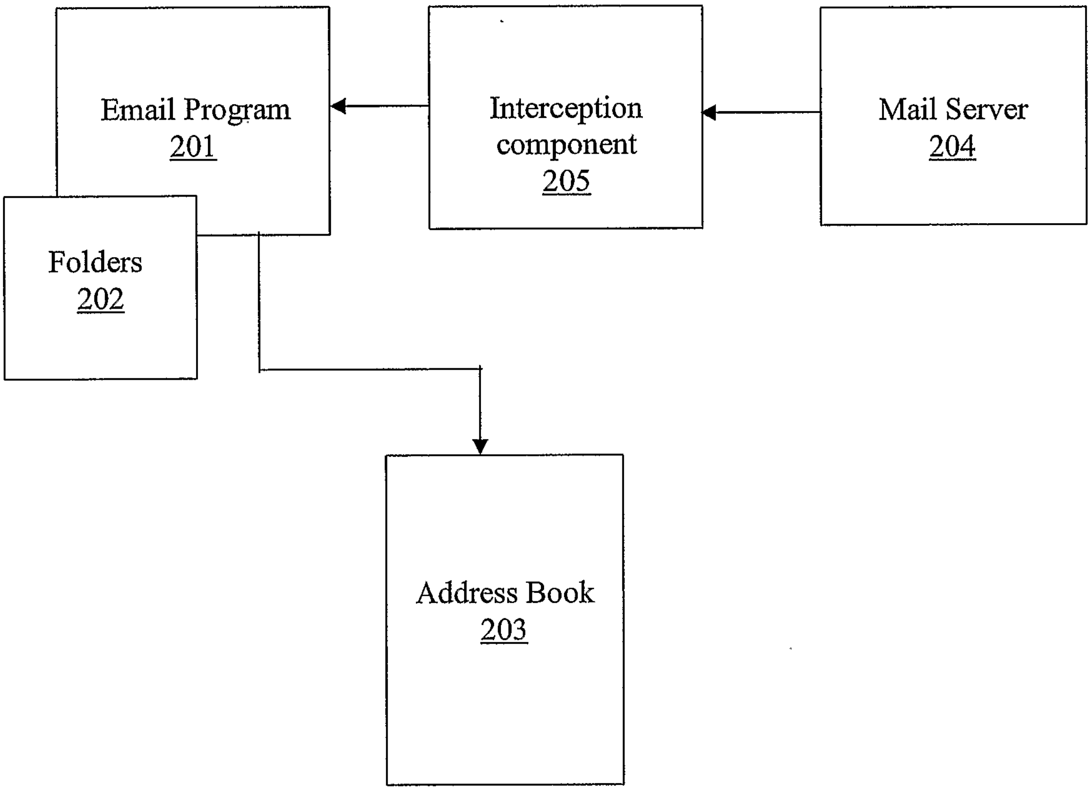

Email Program
201
Interception component
205
Mail Server
204
Folders
202
Address Book
203

Fig. 2A

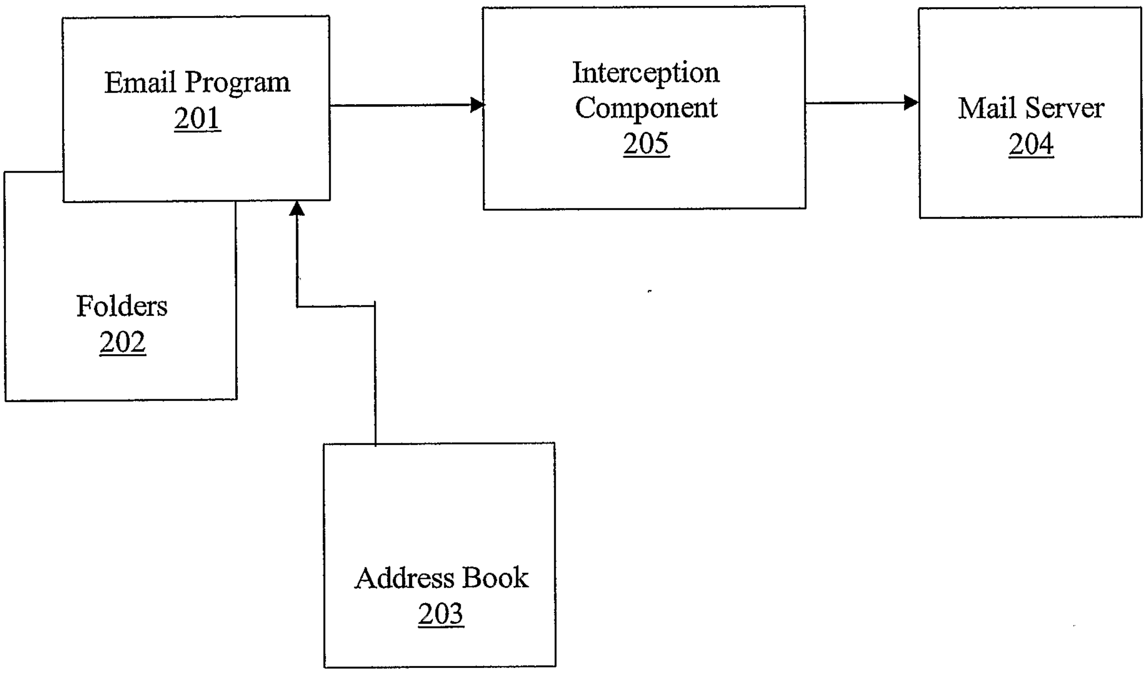

Email Program
201
Interception Component
205
Mail Server
204
Folders
202
Address Book
203

FIGURE 2 B

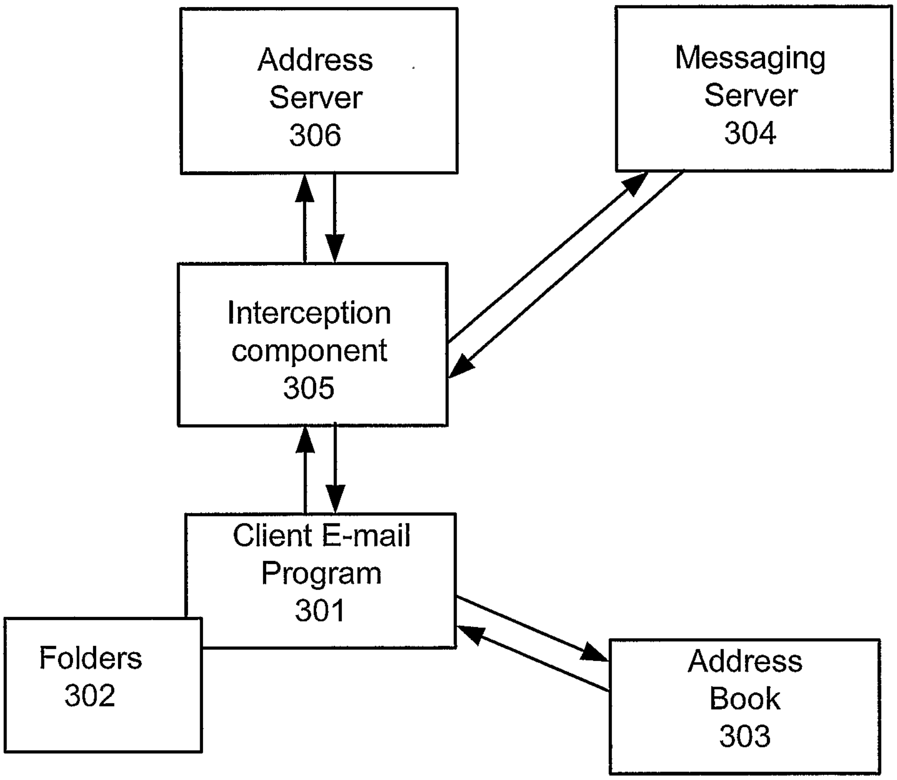

Address
Server
306
Messaging
Server
304
Interception
component
305
Client E-mail
Program
301
Folders
302
Address
Book
303

Figure 3

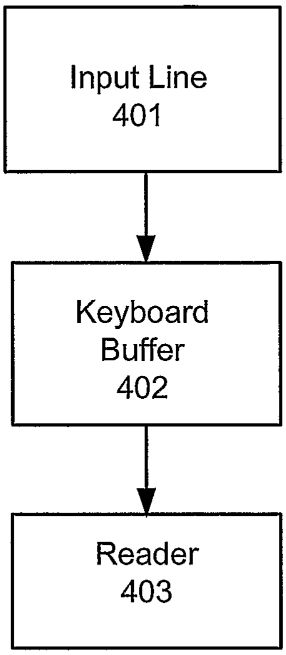


Figure 4A

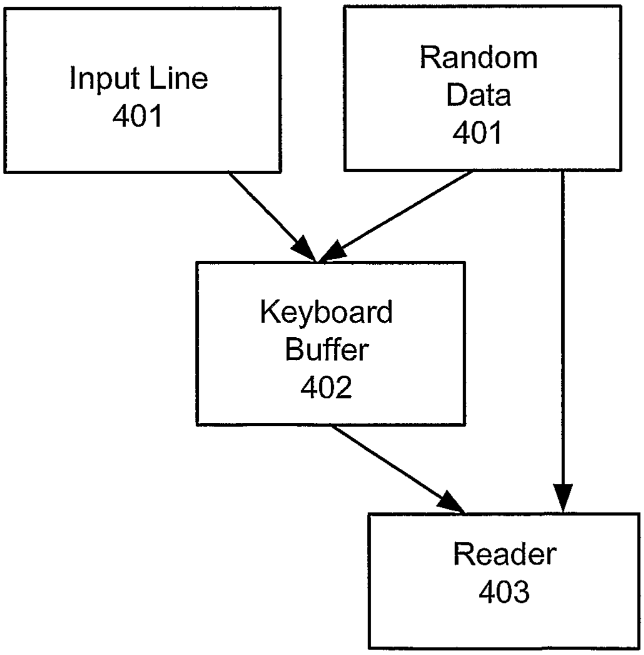


Figure 4B