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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 December 2005 (01.12.2005)

PCT

(10) International Publication Number
WO 2005/114955 A1

(51) International Patent Classification[7]: H04L 29/06, 12/22

(21) International Application Number: PCT/US2005/017601

(22) International Filing Date: 20 May 2005 (20.05.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/573,591 21 May 2004 (21.05.2004) US

(71) Applicant *(for all designated States except US)*: **COMPUTER ASSOCIATES THINK, INC.** [US/US]; One Computer AssociateS Plaza, Islandia, NY 11749 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GASSOWAY, Paul** [US/US]; 219 Normandy Drive, Norwood, MA 02062 (US).

(74) Agent: **BHAVSAR, Samir, A.**; Baker, Botts, L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

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

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

Published:
— *with international search report*

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.

(54) Title: SYSTEMS AND METHODS OF COMPUTER SECURITY

(57) Abstract: A method for combating malicious programs including monitoring network traffic from one or more devices, analyzing the network traffic to determine the presence of a malicious program in the one or more devices and disabling transmission of the network traffic for those of the one or more devices determined to have the malicious program present.

WO 2005/114955 A1

SYSTEMS AND METHODS OF COMPUTER SECURITY

BACKGROUND

REFERENCE TO RELATED APPLICATION

The present disclosure is based on and claims the benefit of Provisional application Serial No. 60/573,591 filed May 21, 2004, the entire contents of which are herein incorporated by reference.

TECHNICAL FIELD

The present disclosure relates to security and, more specifically, to systems and methods of computer security.

DESCRIPTION OF THE RELATED ART

In today's highly computer dependant environment, computer security is a major concern. The security of computer networks is routinely threatened by computer viruses, Trojan horses, worms and the like. Once computer networks are infected with these malicious programs, the malicious programs may have the ability to damage expensive computer hardware, destroy valuable data, tie up limited computing resources or compromise the security of sensitive information.

Worms can be a particularly catastrophic form of malicious program. Worms can infect a computer network and quickly commandeer network resources to aid in the worm's further propagation. In many cases malicious code, for example worms, propagates so rapidly that network bandwidth can become nearly fully consumed. This consumption of bandwidth can grind network function to a near complete halt threatening the proper function of critical applications. Such a network slowdown can have severe adverse effects even on network systems that are not themselves infected with the malicious program.

After a worm has infected computers and computer networks a destructive payload can then be delivered. Destructive payloads can have many harmful

consequences, for example, valuable hardware and/or data can be destroyed, sensitive information can be compromised and network security measures can be circumvented.

To guard against the risk of malicious programs such as worms, businesses may often employ antivirus programs, intrusion detection systems and intrusion protection systems. Antivirus programs are computer programs that can scan computer systems to detect malicious computer code embedded within infected computer files. Malicious code can then be removed from infected files, the infected files may be quarantined or the infected file may be deleted from the computer system. Intrusion detection systems and intrusion protection systems (IDSs) are systems that can be implemented on a computer network that monitor the computer network to detect anomalous traffic that can be indicative of a potential problem, for example a worm infection. IDSs may be either active or passive. Active IDSs may take affirmative measures to remedy a potential infection when found while passive IDSs may be used to alert a network administrator of the potential problem.

IDSs often attempt to identify the presence of network infection by analyzing packets of data that are communicated over the network. Packets are generally examined and compared with signatures of known malicious programs. When a signature matches a packet, the packet may be indicative of a malicious program infection.

IDSs that rely on signatures for the detection of malicious programs must regularly receive and install updated signatures corresponding newly discovered malicious programs. If no signature has been received and installed for a particular malicious program, the IDS might not be able to identify the malicious program.

Modern malicious programs such as worms are able to spread very quickly from computer network to computer network throughout the world. Unfortunately, they can spread so quickly that they can infect many networks before a signature for detecting the malicious program can be developed, distributed and installed.

It is desired that a method and system be used that can slow down the propagation of malicious programs until a suitable signature can be obtained to combat the malicious program. By slowing down the propagation of malicious programs, it is possible that further infection can be limited and network bandwidth can be maintained.

SUMMARY

A method for combating malicious programs including monitoring network traffic from one or more devices, analyzing the network traffic to determine the presence of a malicious program in the one or more devices and disabling transmission of the network traffic for those of the one or more devices determined to have the malicious program present.

A system for combating malicious programs including a monitoring unit for monitoring network traffic from one or more devices, an analyzing unit for analyzing the network traffic to determine the presence of a malicious program in the one or more devices and a disabling unit for disabling transmission of the network traffic for those of the one or more devices determined to have the malicious program present.

A computer system including a processor and a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for combating malicious programs, the method including monitoring network traffic from one or more devices, analyzing the network traffic to determine the presence of a malicious program in the one or more devices, and disabling transmission of the network traffic for those of the one or more devices determined to have the malicious program present.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the present disclosure and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

FIG. 1 shows a segment of a computer network according to embodiments of the present disclosure;

FIG. 2 shows a packet analyzer according to embodiments of the present disclosure; and

FIG. 3 illustrates an example of a computer system capable of implementing the method and apparatus of the present disclosure.

DETAILED DESCRIPTION

In describing the preferred embodiments of the present disclosure illustrated in the drawings, specific terminology is employed for sake of clarity. However, the present disclosure is not intended to be limited to the specific terminology so selected, and it is to be understood that each specific element includes all technical equivalents which operate in a similar manner.

Destructive payloads and network slowdowns are principal methods in which malicious programs may be able to inflict substantial harm on computer networks. It is desirable to slow down the propagation of malicious programs across a computer network. By slowing down the propagation of malicious programs, the malicious program's consumption of network bandwidth can be reduced and fewer network systems can be infected by the malicious program thereby reducing a network's exposure to the potential for destructive payloads.

Systems for combating malicious programs such as antivirus programs and IDSs are generally effective in combating malicious programs. However, many of these systems rely on the installation of signatures. Signatures are generally available shortly after the discovery of an unknown malicious program, for example, signatures may be available within hours of the discovery of the unknown malicious program. Unfortunately, the ill effects of malicious programs, for example, network slowdowns associated with bandwidth consumption, can be felt immediately and a substantial amount of damage can accrue within the time required to generate and install new signatures.

Embodiments of the present disclosure seek to slow down the propagation of malicious programs, for example worms, until appropriate signatures can be acquired. Embodiments of the present disclosure help to mitigate the damage caused by unknown malicious programs by disconnecting and/or shutting down devices on the network as they become infected. Devices on the network can be network devices, for example a computer connected to the network, and devices can be network connection devices that can be used for routing network traffic across the network, for example, routers.

Embodiments of the present disclosure attempt to discover the propagation of unknown viruses by monitoring the outbound traffic of data packets from one or more

devices on the network.

Figure 1 shows a segment of a computer network according to embodiments of the present disclosure. Three network devices 10-12, which may be, for example, computers, may be connected to the network by a router 19 thereby forming an isolated network segment called a subnet. The network devices 10-12 communicate with the network by sending and receiving packets of data that conform to the set communications protocols used by the network. For example, TCP/IP protocols are commonly used as communications protocols within a network.

The handling of data over the network is generally performed by multiple network layers, each layer responsible for particular network functions, and each layer utilizing one or more protocols from the set of protocols. The network layers are generally hierarchical, with the top layers handling user interaction and the bottom layers handling network hardware. Each layer is dependant on the layer below it and each layer communicates with the layer above and the layer below. Because protocols may be specific to the hierarchical layer in which they occur, the protocols used by the layers are generally hierarchical as well. For this reason, the set of protocols used can be referred to as the protocol stack 13-15.

A device transmits data by forming a packet at the top layers of the protocol stack using the top layer protocols and the packet may be processed, for example, the packet may be passed down the protocol stack (13-15) until it reaches the bottom layer where it may then be sent through the network adapter (16-18) along the network. The network receives data from the network devices 10-12 via the network adapters 16-18. Packets received from the network may be received by the bottom layer of the protocol stack (13-15) and the packet may be processed by passing the packet up the protocol stack (13-15) until it reaches the top layer where it can be utilized.

Embodiments of the present disclosure seek to analyze the data sent from the devices 10-12 so that the presence of a malicious program infection can be discovered. Copies of the outbound packets (e.g., packets being sent by network devices 10-12 across the network) may be analyzed by an analyzer (Fig. 2) which can be connected to the network at any location or within any subnet. Copies of the outbound packets can be monitored by the analyzer at any stage in their transmission. For example, packets can be

monitored by the analyzer as they exit the devices 10-12 via the network adapters 16-18. According to an embodiment of the present disclosure, packets may be monitored by the analyzer after the packets have been formed by the protocol stacks 13-15 and before they are received by the network adapters 16-18. According to another embodiment, packets may be monitored by the analyzer after the packets emerge from the router 19. Packets may be analyzed at multiple locations. Figure 1 shows packets being monitored by the analyzer after formation and prior to entering network adapters 16-18 and as they emerge from the router 19. According to various embodiments of the present disclosure, the analyzer examines packets but does not filter them.

After packets are received by the analyzer they may be analyzed to identify a potential infection by a malicious program. Figure 2 shows a packet analyzer according to an embodiment of the present disclosure. Packets that enter the analyzer may be sent to a packet queue 20. The packet queue 20 receives incoming packets and can store them along with the time of the packets' entry. The packet queue 20 may be used as a buffer to hold packets temporarily until the packet checker 21 is ready to analyze the next packet in the queue 20. In the event that the queue 20 is full when a new packet comes in, that new packet may be discarded and not analyzed.

The packet checker 21 analyzes packets and attempts to ascertain if the packets are indicative of a malicious program infection. There are many possible ways in which the packet checker can make this determination and any of these may be utilized by various embodiments of the present disclosure. According to an embodiment of the present disclosure, the packet checker 21 employs a model conformity approach to analyzing packets.

The model conformity approach makes use of the fact that devices infected by a malicious program often utilize as much of the network's resources as possible to propagate the malicious program. This utilization is often very different from the way the device normally utilizes network resources. The model conformity approach to packet analysis compares the packets from a given device with a model that has been developed to represent the normal usage of that given device to ascertain if usage has substantially changed. For example, the packet checker 21 might keep track of the number of packets sent by a given device in a given hour and compare that to the model

that represents the normal number of packets sent in a given hour. When the observed rate of sent packets exceeds the model by a margin specified in the model, the packet checker 21 has discovered a potential malicious program infected device.

The model used by the model conformity approach may be determined based on historic values observed by the packet checker 21. For example, the model used may be an average number of packets sent in an hour (an hourly usage rate) as determined over the past month of observation. The margin that may be used in comparing the observed usage against the normal usage model may also be determined based on historic observations. For example, the margin may be a specific number of standard deviations departure from the historically observed average. For example, if the observed rate deviates from the average by 4 or more standard deviations, the packet checker 21 may determine that a malicious program has been detected.

The model conformity approach may use fixed models/margins or dynamic models/margins that are based on historic observations. For example, the model might be predetermined by the network administrator. According to other embodiments of the present disclosure, the model conformity approach may start out using predetermined models/margins but then modify the fixed models and/or margins as historic statistics are ascertained by the packet checker 21.

The model conformity approach need not be limited to analyzing statistics concerning the number of packets observed. Embodiments of the present disclosure may also analyze the form of the packets collected and compare it to the model form for packets from that given device. For example, the packet checker 21 might examine such factors as the size of the packet, the recipient address of the packet, the time of day the packet is being sent, etc. and use that information to ascertain potential malicious activity.

The model conformity approach may use any level of complexity in analyzing the packets and comparing properties of those packets to the model. The model conformity approach may use statistical analysis to analyze packets and compare them with models. For example, statistical comparisons can be used to gauge the degree of similarity between the observed factors and the model. For example, linear regression may be used to determine if the observed usage deviates substantially from the normal usage as indicated by the model thereby indicating a malicious program infection.

Where statistics are used to compare observed usage against normal usage, statistics used to characterize the packets and the models may be, for example, overall averages, for example, the average rate of packet sending, or the statistics used may relate to a given time or day of the week or year. Multiple statistics can be combined to create a multifaceted model that can be used to compare observed packets in any number of ways to determine if there is a substantial deviation between observed usage and normal usage.

The model conformity approach may use artificial intelligence to determine if there is a substantial deviation. For example, neural networks and/or Bayesian analysis may be used to determine if there is a substantial deviation between observed usage and normal usage.

The model conformity approach may be used to generate a deviation score. This score represents the degree of deviation between the observed usage and normal usage. The score can be checked against an acceptable score to ascertain if a malicious program may be present. By modifying the score, the sensitivity of the approach can be adjusted.

Other approaches for determining if the packets are indicative of a malicious program infection may be used. For example, heuristic recognition approaches may be used to recognize characteristics indicative of malicious program infection. Heuristic recognition scans may be able to intelligently estimate whether packets evidence a malicious program infection. This technique relies on programmed logic, called heuristics, to make its determinations.

For example, the packet checker 21 can monitor packet traffic at multiple subnets to detect a sudden, unusual and/or large proliferation of similar packets. Such proliferation may be indicative of a malicious program infection.

When the packet checker has determined that particular devices or connections have become infected with a malicious program, the disabler 22 sends instructions to the infected devices instructing them to stop sending packets thereby disabling the transmission of packets. For example, where a device, for example a computer, has been determined to be infected, the disabler 22 may send instructions for that computer to power down or to otherwise remove itself from the network, for example by deactivating its network adapter. For example, where a device, for example a router, has been determined to be responsible for transmitting infected packets onto the network, the

disabler 22 may send instructions for that router to power down or to otherwise stop routing packets. Alternatively, the disabler may remove an infected device from the network by revoking network authentication. The disabler may notify a network administrator that an infected device has been detected, and suggest that the network administrator take the infected machine offline until a signature is available to detect the particular infection on the machine so that the infection can be removed.

After the disabler 22 has disabled the devices believed to be infected with a malicious program, those disabled devices may no longer be able to propagate the malicious program. Therefore, the spread of the malicious program can be, at the very least, slowed down and possibly stopped. Additionally, network bandwidth can be protected so that those devices that remain uninfected might still be able to function normally on the network.

Disabled devices may then be enabled after appropriate remedial measures have been taken or it has otherwise been determined that those devices no longer pose a risk to the network. For example, a network administrator might enable the disabled devices after a signature has been obtained and incorporated into an antivirus program thereby removing the malicious program from the disabled devices. For example, the network administrator may determine that there was no malicious program infection and the disabling had not been necessary.

Fig. 3 depicts an example of a computer system which may implement methods and systems of the present disclosure. The systems and methods of the present disclosure may be implemented in the form of a software application running on a computer system, for example, a mainframe, personal computer (PC), handheld computer, server, etc. The software application may be stored on a recording media locally accessible by the computer system and accessible via a hard wired or wireless connection to a network, for example, a local area network, or the Internet.

The computer system referred to generally as system 100 may include, for example, a central processing unit (CPU) 102, random access memory (RAM) 104, a printer interface 106, a display unit 108, a local area network (LAN) data transmission controller 110, a LAN interface 112, a network controller 114, an internal buss 116, and one or more input devices 118, for example, a keyboard, mouse etc. As shown, the

system 100 may be connected to a data storage device, for example, a hard disk, 120 via a link 122.

What is claimed is:

1. A method for combating malicious programs, the method comprising:

monitoring network traffic from one or more devices;

analyzing said network traffic to determine the presence of a malicious program in said one or more devices; and

disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present.

2. The method of claim 1, wherein analyzing said network traffic to determine the presence of a malicious program in said one or more devices comprises:

comparing observed network traffic for a device to a normal network traffic model for said device; and

determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model.

3. The method of claim 2, wherein statistical analysis is used to compare and determine.

4. The method of claim 2, wherein artificial intelligence is used to compare and determine.

5. The method of claim 2, wherein determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model comprises ascertaining if said observed network traffic deviates from said normal network traffic model by at least a determined margin.

6. The method of claim 5, wherein said determined margin is predetermined and fixed.

7. The method of claim 5, wherein said determined margin is determined based on historic values observed by monitoring network traffic.

8. The method of claim 5, wherein said determined margin is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

9. The method of claim 2, wherein said normal network traffic model is predetermined and fixed.

10. The method of claim 2, wherein said normal network traffic model is determined based on historic values observed by monitoring network traffic.

11. The method of claim 2, wherein said normal network traffic model is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

12. The method of claim 1, wherein disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises powering down said those of said one or more devices determined to have said malicious program present.

13. The method of claim 1, wherein disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises removing from said network said those of said one or more devices determined to have said malicious program present.

14. A system for combating malicious programs comprising:

a monitoring unit for monitoring network traffic from one or more devices;

an analyzing unit for analyzing said network traffic to determine the presence of a malicious program in said one or more devices; and

a disabling unit for disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present.

15. The system of claim 14, wherein analyzing said network traffic to determine the presence of a malicious program in said one or more devices comprises:

a comparing unit for comparing observed network traffic for a device to a normal network traffic model for said device; and

a determining unit for determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model.

16. The system of claim 15, wherein statistical analysis is used to compare and determine.

17. The system of claim 15, wherein artificial intelligence is used to compare and determine.

18. The system of claim 15, wherein determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model comprises ascertaining if said observed network traffic deviates from said normal network traffic model by at least a determined margin.

19. The system of claim 18, wherein said determined margin is predetermined and fixed.

20. The system of claim 18, wherein said determined margin is determined based on historic values observed by monitoring network traffic.

21. The system of claim 18, wherein said determined margin is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

22. The system of claim 15, wherein said normal network traffic model is predetermined and fixed.

23. The system of claim 15, wherein said normal network traffic model is determined based on historic values observed by monitoring network traffic.

24. The system of claim 15, wherein said normal network traffic model is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

25. The system of claim 14, wherein disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises powering down said those of said one or more devices determined to have said malicious program present.

26. The system of claim 14, wherein disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises removing from said network said those of said one or more devices determined to have said malicious program present.

27. A computer system comprising:

a processor; and

a program storage device readable by the computer system, embodying a program of instructions executable by the processor to perform method steps for combating malicious programs, the method comprising:

monitoring network traffic from one or more devices;

analyzing said network traffic to determine the presence of a malicious program in said one or more devices; and

disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present.

28. The computer system of claim 27, wherein analyzing said network traffic to determine the presence of a malicious program in said one or more devices comprises:

comparing observed network traffic for a device to a normal network traffic model for said device; and

determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model.

29. The computer system of claim 28, wherein statistical analysis is used to compare and determine.

30. The computer system of claim 28, wherein artificial intelligence is used to compare and determine.

31. The computer system of claim 28, wherein determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model comprises ascertaining if said observed network traffic deviates from said normal network traffic model by at least a determined margin.

32. The computer system of claim 31, wherein said determined margin is predetermined and fixed.

33. The computer system of claim 31, wherein said determined margin is determined based on historic values observed by monitoring network traffic.

34. The computer system of claim 31, wherein said determined margin is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

35. The computer system of claim 28, wherein said normal network traffic model is predetermined and fixed.

36. The computer system of claim 28, wherein said normal network traffic model is determined based on historic values observed by monitoring network traffic.

37. The computer system of claim 28, wherein said normal network traffic model is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

38. The computer system of claim 27, wherein disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises powering down said those of said one or more devices determined to have said malicious program present.

39. The computer system of claim 27, wherein disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises removing from said network said those of said one or more devices determined to have said malicious program present.

39. A computer recording medium including computer executable code for combating malicious programs, the computer executable code comprising:

code for monitoring network traffic from one or more devices;

code for analyzing said network traffic to determine the presence of a malicious program in said one or more devices; and

code for disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present.

40. The computer recording medium of claim 39, wherein said code for analyzing said network traffic to determine the presence of a malicious program in said one or more devices comprises:

code for comparing observed network traffic for a device to a normal network traffic model for said device; and

code for determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model.

41. The computer recording medium of claim 40, wherein statistical analysis is used to compare and determine.

42. The computer recording medium of claim 40, wherein artificial intelligence is used to compare and determine.

43. The computer recording medium of claim 40 wherein said code for determining that a malicious program is present when said observed network traffic deviates substantially from said normal network traffic model comprises code for ascertaining if said observed network traffic deviates from said normal network traffic model by at least a determined margin.

44. The computer recording medium of claim 43, wherein said determined margin is predetermined and fixed.

45. The computer recording medium of claim 43, wherein said determined margin is determined based on historic values observed by monitoring network traffic.

46. The computer recording medium of claim 43, wherein said determined margin is initially predetermined and is subsequently modified based on historic values observed by monitoring network traffic.

47. The computer recording medium of claim 40, wherein said normal network traffic model is predetermined and fixed.

48. The computer recording medium of claim 40, wherein said normal network traffic model is determined based on historic values observed by monitoring network traffic.

49. The computer recording medium of claim 40, wherein said normal network traffic model is initially predetermined and is subsequently modified based on historic

values observed by monitoring network traffic.

50. The computer recording medium of claim 39, wherein said code for disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises code for powering down said those of said one or more devices determined to have said malicious program present.

51. The computer recording medium of claim 39, wherein said code for disabling transmission of said network traffic for those of said one or more devices determined to have said malicious program present comprises code for removing from said network said those of said one or more devices determined to have said malicious program present.

FIG. 1

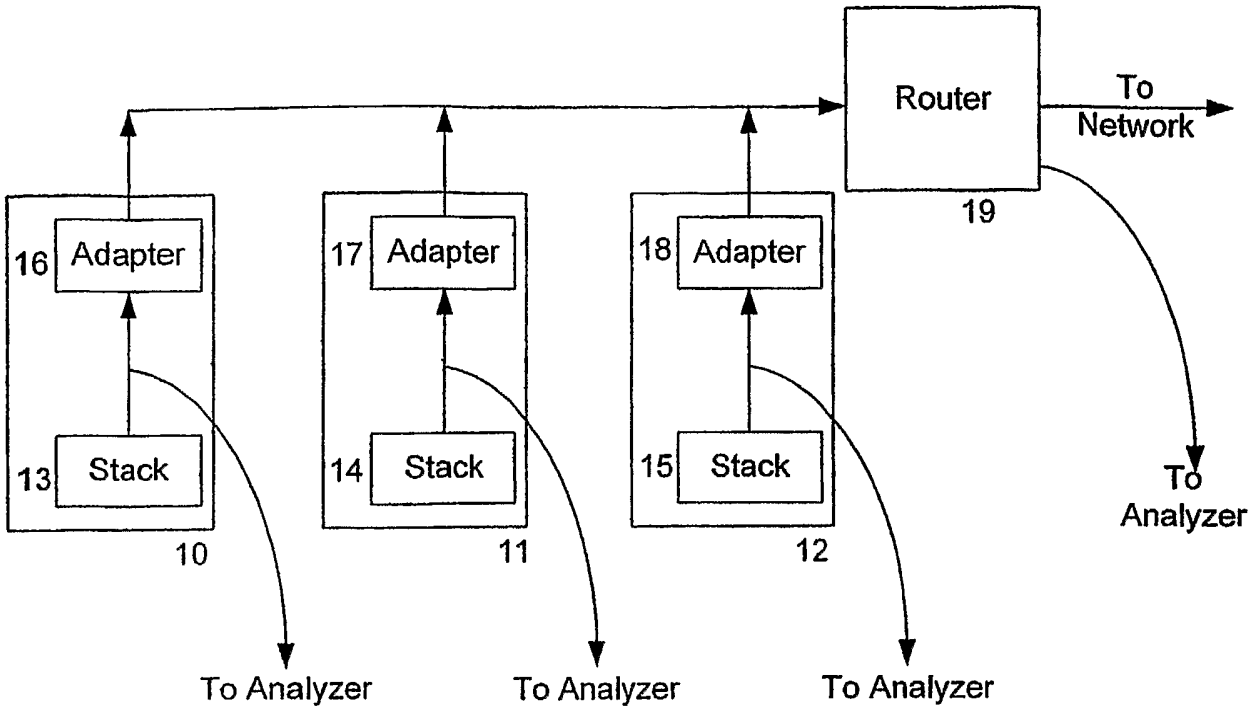

Router
To Network
19
16 Adapter
17 Adapter
18 Adapter
13 Stack
14 Stack
15 Stack
10
11
12
To Analyzer
To Analyzer
To Analyzer
To Analyzer

FIG. 2

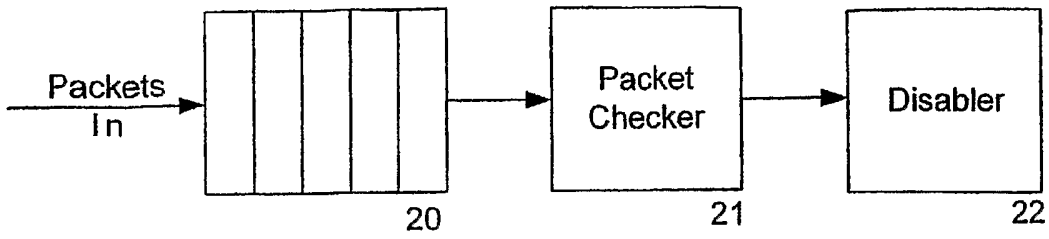
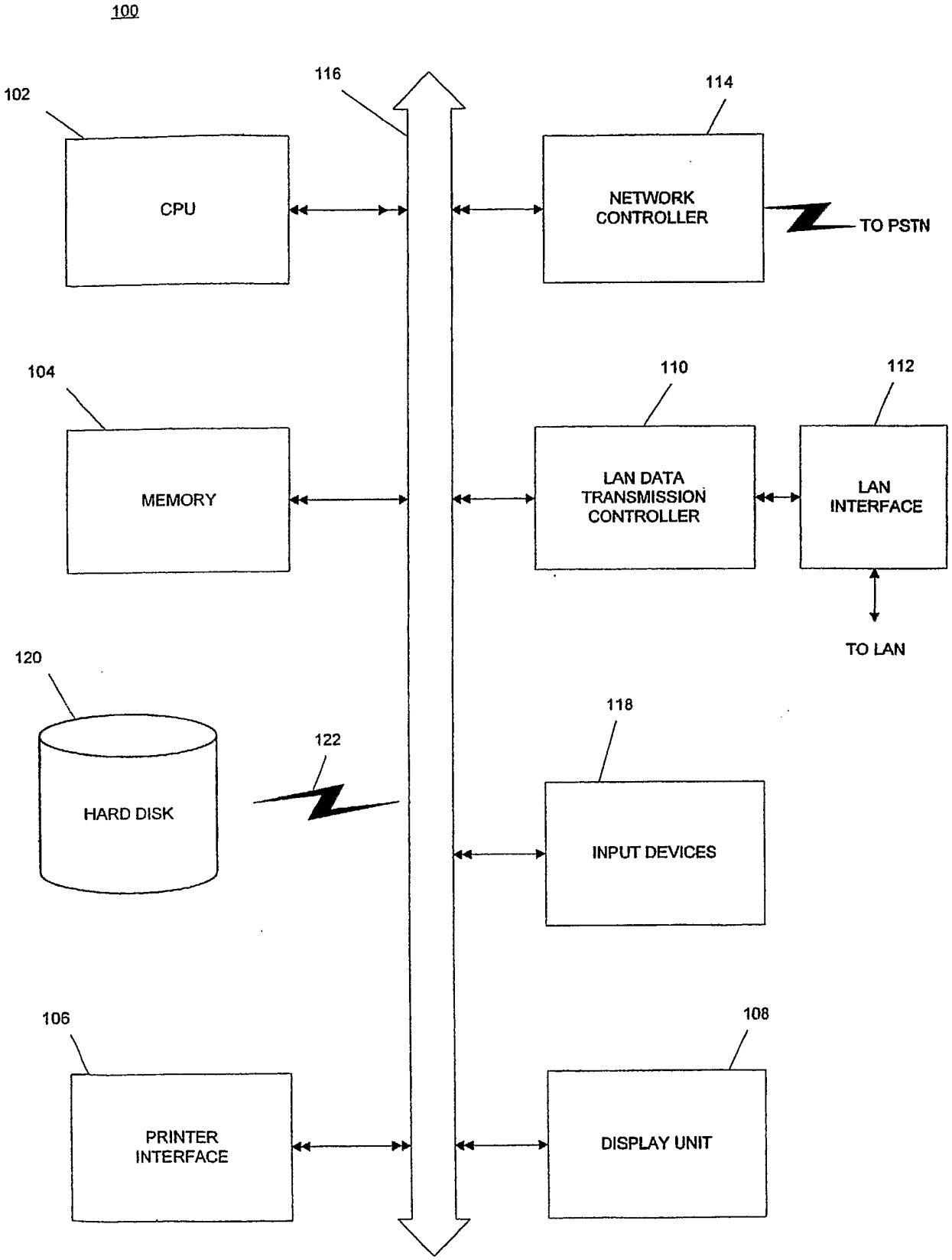


FIG. 3


100
102
CPU
116
114
NETWORK CONTROLLER
TO PSTN
104
MEMORY
110
LAN DATA TRANSMISSION CONTROLLER
112
LAN INTERFACE
TO LAN
120
HARD DISK
122
118
INPUT DEVICES
106
PRINTER INTERFACE
108
DISPLAY UNIT

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/017601

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/090426 A (COMPUTER ASSOCIATES THINK, INC) 30 October 2003 (2003-10-30) page 15, line 10 - page 17, line 21 page 20, line 11 - page 21, line 5	1-51
X	WO 03/055148 A (ESPHION LIMITED; BRENDEL, JUERGEN) 3 July 2003 (2003-07-03) page 5, line 1 - page 6, line 9 page 14, lines 3-20 page 15, lines 13-24	1-51
X	US 2003/110396 A1 (LEWIS LUNDY M ET AL) 12 June 2003 (2003-06-12) paragraphs '0015!, '0018!, '0019!, '0065! - '0067!, '0094!, '0123!, '0132! - '0134!	1-51

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 September 2005	14/09/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Lázaro, M.L.

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/37755 A (ASTA NETWORKS, INC) 10 May 2002 (2002-05-10) page 3, lines 7-22 page 7, line 9 - page 8, line 11 page 9, line 31 - page 10, line 8	1-51
X	US 2004/047356 A1 (BAUER BLAINE D) 11 March 2004 (2004-03-11) abstract paragraph '0011!	1-51

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2005/017601

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03090426 A	30-10-2003	AU 2003223656 A1	03-11-2003
		BR 0309288 A	09-02-2005
		CA 2480475 A1	30-10-2003
		EP 1495616 A1	12-01-2005
		WO 03090426 A1	30-10-2003
		US 2003200464 A1	23-10-2003
WO 03055148 A	03-07-2003	NZ 516346 A	24-09-2004
		AU 2002358361 A1	09-07-2003
		WO 03055148 A1	03-07-2003
		US 2005125195 A1	09-06-2005
US 2003110396 A1	12-06-2003	NONE	
WO 0237755 A	10-05-2002	AU 3395702 A	15-05-2002
		WO 0237755 A2	10-05-2002
US 2004047356 A1	11-03-2004	NONE	