

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
22 March 2007 (22.03.2007)

PCT

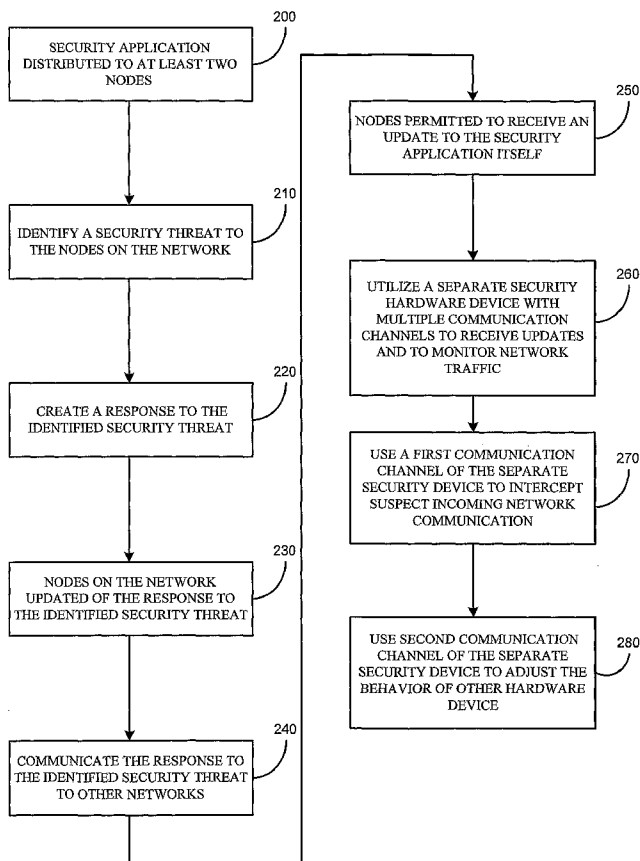
(10) International Publication Number
WO 2007/032967 A1

- (51) International Patent Classification:
H04L 12/22 (2006.01) *G06F 21/20* (2006.01)
- (21) International Application Number:
PCT/US2006/034580
- (22) International Filing Date:
6 September 2006 (06.09.2006)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
11/224,605 12 September 2005 (12.09.2005) US
- (71) Applicant (for all designated States except US): **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).
- (72) Inventors: **FRANK, Alexander**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **DUFFUS, James, S.**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **PHILLIPS, Thomas, G.**; One Microsoft Way, Redmond, Washington 98052-6399 (US).

- (74) Agent: **MICROSOFT CORPORATION**; Attention: Sharon Rydberg(sharonr-21-2029), LCA, International Patent Department, One Microsoft Way, 21/2029, Redmond, WA 98052-6399 (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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: DISTRIBUTED NETWORK SECURITY SERVICE



(57) Abstract: A method and apparatus to distribute a network security service is disclosed. The security software may be distributed across nodes on a network and may use a separate security device that has two channels, one to review network traffic and a second to send updates to other security devices.

WO 2007/032967 A1



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*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

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.

DISTRIBUTED NETWORK SECURITY SERVICE

Background

[0001] As networks continue to grow in use, the importance of having safe and secure networks have increase. Applications to address security concerns have
5 been developed but writers of viruses quickly adjust to avoid the security applications. In addition, virus writers will attack nodes that are supplying security application updates.

Summary

[0002] A method and apparatus to distribute a network security service is
10 disclosed. The security software may be distributed across nodes on a network. The software may observe network traffic and search for possibly malicious communication. If a malicious communication is found, a response may be created and be distributed to other network nodes and additional networks. The method may also use a security device that has first and second communication channel
15 that may spoof suspected malicious nodes and based on the response, may use the second communication channel, which may be secure, to notify other nodes of the threat and possible responses.

Drawings

[0003] Fig. 1 is a block diagram of a computing system that may operate in
20 accordance with the claims;

[0004] Fig. 2 is a method of providing a distributed security system in accordance with the claims;

[0005] Fig. 3 is an illustration of a network that may implement the security method as described in the claims; and

25 [0006] Fig. 4 is an illustration of a peer to peer network that may implement the security method as described in the claims.

Description

[0007] Although the following text sets forth a detailed description of numerous different embodiments, it should be understood that the legal scope of the
30 description is defined by the words of the claims set forth at the end of this patent. The detailed description is to be construed as exemplary only and does not describe

every possible embodiment since describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology developed after the filing date of this patent, which would still fall within the scope of the claims.

5 [0008] It should also be understood that, unless a term is expressly defined in this patent using the sentence “As used herein, the term ‘ _____ ’ is hereby defined to mean...” or a similar sentence, there is no intent to limit the meaning of that term, either expressly or by implication, beyond its plain or ordinary meaning, and such term should not be interpreted to be limited in scope based on any statement made
10 in any section of this patent (other than the language of the claims). To the extent that any term recited in the claims at the end of this patent is referred to in this patent in a manner consistent with a single meaning, that is done for sake of clarity only so as to not confuse the reader, and it is not intended that such claim term be limited, by implication or otherwise, to that single meaning. Finally, unless a claim
15 element is defined by reciting the word “means” and a function without the recital of any structure, it is not intended that the scope of any claim element be interpreted based on the application of 35 U.S.C. § 112, sixth paragraph.

[0009] Fig. 1 illustrates an example of a suitable computing system environment
100 on which a system for the steps of the claimed method and apparatus may be
20 implemented. The computing system environment 100 is only one example of a suitable computing environment and is not intended to suggest any limitation as to the scope of use or functionality of the method of apparatus of the claims. Neither should the computing environment 100 be interpreted as having any dependency or requirement relating to any one or combination of components illustrated in the
25 exemplary operating environment 100.

[0010] The steps of the claimed method and apparatus are operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the methods
30 or apparatus of the claims include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems,

microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0011] The steps of the claimed method and apparatus may be described in the
5 general context of computer-executable instructions, such as program modules,
being executed by a computer. Generally, program modules include routines,
programs, objects, components, data structures, etc. that perform particular tasks or
implement particular abstract data types. The methods and apparatus may also be
practiced in distributed computing environments where tasks are performed by
10 remote processing devices that are linked through a communications network. In a
distributed computing environment, program modules may be located in both local
and remote computer storage media including memory storage devices.

[0012] With reference to Fig. 1, an exemplary system for implementing the steps
of the claimed method and apparatus includes a general purpose computing device
15 in the form of a computer 110. Components of computer 110 may include, but are
not limited to, a processing unit 120, a system memory 130, and a system bus 121
that couples various system components including the system memory to the
processing unit 120. The system bus 121 may be any of several types of bus
structures including a memory bus or memory controller, a peripheral bus, and a
20 local bus using any of a variety of bus architectures. By way of example, and not
limitation, such architectures include Industry Standard Architecture (ISA) bus,
Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video
Electronics Standards Association (VESA) local bus, and Peripheral Component
Interconnect (PCI) bus also known as Mezzanine bus.

25 [0013] Computer 110 typically includes a variety of computer readable media.
Computer readable media can be any available media that can be accessed by
computer 110 and includes both volatile and nonvolatile media, removable and
non-removable media. By way of example, and not limitation, computer readable
media may comprise computer storage media and communication media.

30 Computer storage media includes both volatile and nonvolatile, removable and
non-removable media implemented in any method or technology for storage of

information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by computer 110. Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0014] The system memory 130 includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) 132. A basic input/output system 133 (BIOS), containing the basic routines that help to transfer information between elements within computer 110, such as during start-up, is typically stored in ROM 131. RAM 132 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 120. By way of example, and not limitation, Fig. 1 illustrates operating system 134, application programs 135, other program modules 136, and program data 137.

[0015] The computer 110 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, Fig. 1 illustrates a hard disk drive 140 that reads from or writes to non-removable, nonvolatile magnetic media, a magnetic disk drive 151 that reads from or writes to a removable, nonvolatile magnetic disk 152, and an optical disk drive 155 that reads from or writes to a removable, nonvolatile optical disk 156 such as a CD

ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that can be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like.

5 The hard disk drive 141 is typically connected to the system bus 121 through a non-removable memory interface such as interface 140, and magnetic disk drive 151 and optical disk drive 155 are typically connected to the system bus 121 by a removable memory interface, such as interface 150.

[0016] The drives and their associated computer storage media discussed above and illustrated in Fig. 1, provide storage of computer readable instructions, data structures, program modules and other data for the computer 110. In Fig. 1, for example, hard disk drive 141 is illustrated as storing operating system 144, application programs 145, other program modules 146, and program data 147. Note that these components can either be the same as or different from operating
15 system 134, application programs 135, other program modules 136, and program data 137. Operating system 144, application programs 145, other program modules 146, and program data 147 are given different numbers here to illustrate that, at a minimum, they are different copies. A user may enter commands and information into the computer 20 through input devices such as a keyboard 162 and pointing
20 device 161, commonly referred to as a mouse, trackball or touch pad. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 120 through a user input interface 160 that is coupled to the system bus, but may be connected by other interface and bus structures, such as a parallel
25 port, game port or a universal serial bus (USB). A monitor 191 or other type of display device is also connected to the system bus 121 via an interface, such as a video interface 190. In addition to the monitor, computers may also include other peripheral output devices such as speakers 197 and printer 196, which may be connected through an output peripheral interface 190.

30 [0017] The computer 110 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 180. The

remote computer 180 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer 110, although only a memory storage device 181 has been illustrated in Fig. 1. The logical connections depicted
5 in Fig. 1 include a local area network (LAN) 171 and a wide area network (WAN) 173, but may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0018] When used in a LAN networking environment, the computer 110 is
10 connected to the LAN 171 through a network interface or adapter 170. When used in a WAN networking environment, the computer 110 typically includes a modem 172 or other means for establishing communications over the WAN 173, such as the Internet. The modem 172, which may be internal or external, may be connected to the system bus 121 via the user input interface 160, or other appropriate
15 mechanism. In a networked environment, program modules depicted relative to the computer 110, or portions thereof, may be stored in the remote memory storage device. By way of example, and not limitation, Fig. 1 illustrates remote application programs 185 as residing on memory device 181. It will be appreciated that the network connections shown are exemplary and other means of establishing a
20 communications link between the computers may be used.

[0019] Fig. 2 may be an illustration of a method of providing a distributed network security service. The method may be applied to a network as broad as the Internet as an illustrated in Fig. 3 or as narrow as a peer to peer network illustrated in Fig. 4. At block 200, a security application may be distributed to at least two
25 nodes (300, 310 in Fig. 3 or 400, 410 in Fig. 4) on a network. Distributed computing is a powerful concept where a single application is split into parts which operate on separate computing devices. In this way, a single computing device does not become bogged down running the entire application. In addition, as the application is spread over numerous computing devices, there is no single point of
30 failure (or single point to attack) for the application. The various application parts can be stored in a redundant manner on a plurality of computing devices further

ensuring that if one computing device fails or is subject to attack, the other nodes on the network can execute the distributed application. A variety of manners of distributing the single application are known and may be appropriate in view of the claims.

5 [0020] At block 210, the security application may identify a security threat to the nodes on the network. Security threats are only too well known and the variety of security threats continues to grow. Common threats include viruses, worms and attempts to take control of a user's computer. Modern security programs can identify security threats based on a variety of factors such as file names, traffic
10 similar to previously created viruses, malformed packets, sending address, etc.

[0021] At block 220, the security application may create a response to the identified security threat. There are a variety of possible responses, such as blocking traffic from a malicious node 320 (Fig. 3) 420 (Fig. 4), replicating executable programs that address the threat, replicating policy updates, replicating
15 signature updates, or replicating security profiles. Other responses may include reducing the privilege for any similar traffic from the originating subnet of the identified security threat and/or reducing privilege for any similar traffic with their own subnet. Yet a further response may be to create a plurality of security levels and adjusting the level of security based on an analysis of the suspect nodes and
20 suspect messages.

[0022] At block 230, other nodes on the network may be updated of the response to the identified security threat. For example, referring to Fig. 3, device1 310 which may execute the security application, may inform device2 315 of the response to the security threat. Similarly, in Fig. 4, device1 410 may inform
25 device2 415 of the response to the security threat. If the response is to block a particular malicious node 320 (Fig. 3) 420 (Fig. 4), the response may spread from device 310 410 to device 315 415 and the communication from the malicious node may be effectively blocked.

[0023] At block 240, the method may communicate the response to the identified
30 security threat to other networks. For example, in Fig. 4, node2 405 may be a member of several peer to peer networks. Node2 405 may take the response to the

identified security threat and distribute it to other nodes on the additional peer to peer networks of which it is a part. In addition, at block 250, the nodes may be permitted to receive an update to the security application itself. As with any program, bugs may be located or the code may be improved over time. Block 250
5 may allow the code to be updated over time.

[0024] At block 260, the method may utilize a separate security hardware device with a first communication channel and a second communication channel where the security hardware receives network communications on the first channel before determining whether to forward the network communications to the computer.
10 Referring to Fig. 3, the device 310 may sit between an internet service provider ("ISP") 325 and a home device 300 that is accessing the internet. Referring to Fig. 4, the device 410 may also sit between a node 410 and a peer to peer network 425. The device may have a first communication channel to communicate with the network, and a second channel to communicate with other security devices. For
15 example, referring to Fig. 3, the first communication channel 330 may sit between the ISP1 325 and home1 300 and the second communication channel 335 may communicate with other security devices such as security device 315. The second communication channel 335 may be a secure communication channel and the second communication channel may be used to communicate updates to the
20 security application and security responses. The second communication channel 335 may be a completely separate wired channel or may be a virtually separate channel such as a virtual private network.

[0025] Referring to Fig. 2, at block 270, the method may use the separate security device to intercept suspect incoming network communication from a suspect node,
25 spoof a response to the suspect node and based on the suspect node's reply to the response, determining the response to the identified security threat. For example, referring to Fig.3, device2 315 may suspect that some network traffic from ISP2 340 may be malicious such as from the malicious node 320. As mentioned previously, suspect network communication may be indicated by monitoring a
30 computer of the subnet network for virus-like traffic and malformed packets. Before communicating the network traffic to home2 305, the security device 315

may send a response to the suspect malicious node 320 to test the node, such as offering to malicious node 320 access to something desirable. If the malicious node 320 acts on the offer, the security device 315 can determine that the suspected malicious node 320 truly is malicious. The security device 315 may then determine an appropriate response. There are a variety of possible responses, such as blocking traffic from the malicious node 320, replicating executable programs, replicating policy updates, replicating signature updates, or replicating security profiles. Other responses may include reducing the privilege for any similar traffic from the originating subnet of the identified security threat, reducing privilege for any similar traffic with their own subnet. Yet a further response may be to create a plurality of security levels and adjusting the level of security based on an analysis of the suspect nodes and suspect messages.

[0026] At block 280, the second communication channel may be used to adjust the behavior of other hardware device 310. The method may allow network computers to opt in to execute part of the distributed security application. If a network computer does opt in, the user may be forbidden from accessing the distributed security application.

[0027] Although the forgoing text sets forth a detailed description of numerous different embodiments, it should be understood that the scope of the patent is defined by the words of the claims set forth at the end of this patent. The detailed description is to be construed as exemplary only and does not describe every possible embodiment because describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology developed after the filing date of this patent, which would still fall within the scope of the claims.

[0028] Thus, many modifications and variations may be made in the techniques and structures described and illustrated herein without departing from the spirit and scope of the present claims. Accordingly, it should be understood that the methods and apparatus described herein are illustrative only and are not limiting upon the scope of the claims.

CLAIMS

1. A method of providing a distributed network security service comprising:
distributing a security application to at least two nodes on a network to be operated in a distributed manner on the network;
identifying a security threat to the nodes on the network;
creating a response to the identified security threat; and
updating other nodes on the network of the response to the identified security threat.
2. The method of claim 1, further comprising communicating the response to the identified security threat to other networks.
3. The method of claim 1, further comprising allowing the nodes to receive an update to the security application.
4. The method of claim 1, further comprising using a separate security hardware device with a first communication channel and a second communication channel wherein the security hardware receives network communications on the first channel before determining whether to forward the network communications to the computer.
5. The method of claim 4, further comprising:
using the separate security device to intercept suspect incoming network communications from a suspect node,
spoofing a response to the suspect node; and
based on the suspect node's reply to the response, determining the response to the identified security threat.
6. The method of claim 4, further comprising using the second communication channel to adjust the behavior of the hardware devices.
7. The method of claim 5, wherein the second communication channel is a secure communication channel.
8. The method of claim 5, wherein updates to the security application comprise replicating executable programs, policy, signature or profile updates implemented on the originating network subnet on other networks subnets.

9. The method of claim 5, further comprising creating a response by reducing the privilege for any similar traffic from the originating subnet of the identified security threat
10. The method of claim 5, further comprising creating a response by reducing privilege for any similar traffic with their own subnet.
11. The method of claim 5, further comprising creating a response by blocking transmissions from a source of malicious messages.
12. The method of claim 5, further comprising creating a plurality of security levels and adjusting the level of security based on an analysis of the suspect nodes and suspect messages.
13. The method of claim 1, further comprising monitoring a computer of the subnet network for virus-like traffic and malformed packets.
14. The method of claim 1, further comprising storing redundant parts of the distributed security application on additional nodes.
15. The method of claim 1, further allowing network computers to opt in to execute part of the distributed security application.
16. The method of claim 14, further comprising not permitting the user of the computer to access the distributed security application.
17. A tangible computer readable medium comprising computer executable instructions for providing a distributed network security service comprising computer executable instructions for:
 - distributing a security application to at least two nodes on a network to be operated in a distributed manner on the network;
 - intercepting suspect incoming network communications from a suspect node,
 - identifying a security threat to the nodes on the network;
 - spoofing a response to the suspect node;
 - based on the suspect node's reply to the response, determining the response to the identified security threat; and
 - updating other nodes on the network of the response to the identified security threat.

18. The tangible computer readable medium of claim 17, further comprising using a separate security hardware device with a first communication channel and a second communication channel wherein the security hardware receives network communications on the first channel before determining whether to forward the network communications to the computer.

19. A computer system comprising a memory, a processor, an input device and an output device wherein the processor is adapted to execute computer instructions for providing a distributed network security service, the computer executable instructions comprising instructions for:

distributing a security application to at least two nodes on a network to be operated in a distributed manner on the network;

using a separate security hardware device with a first communication channel and a second communication channel wherein the security hardware receives network communications on the first channel before determining whether to forward the network communications to the computer system;

using the security device to:

intercept suspect incoming network communications from a suspect node,

identify a security threat to the nodes on the network;

spoof a response to the suspect node; and

based on the suspect node's reply to the response, determining the response to the identified security threat; and

updating other nodes on the network of the response to the identified security threat.

20. The computer system of claim 19, further comprising instructions for allowing network computers to opt in to execute part of the distributed security application; and

not permitting the user of the network computer to access the distributed security application.

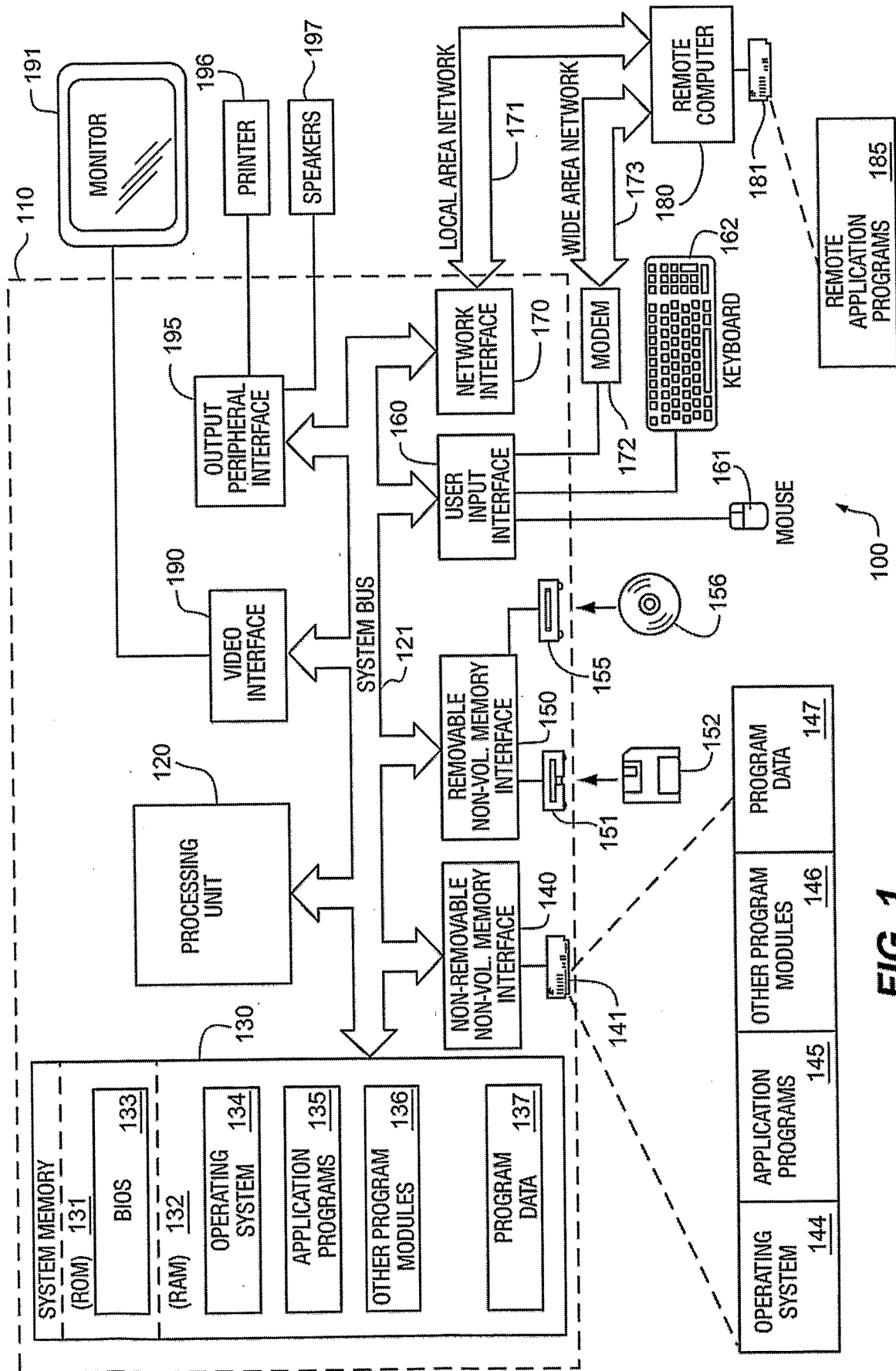


FIG. 1

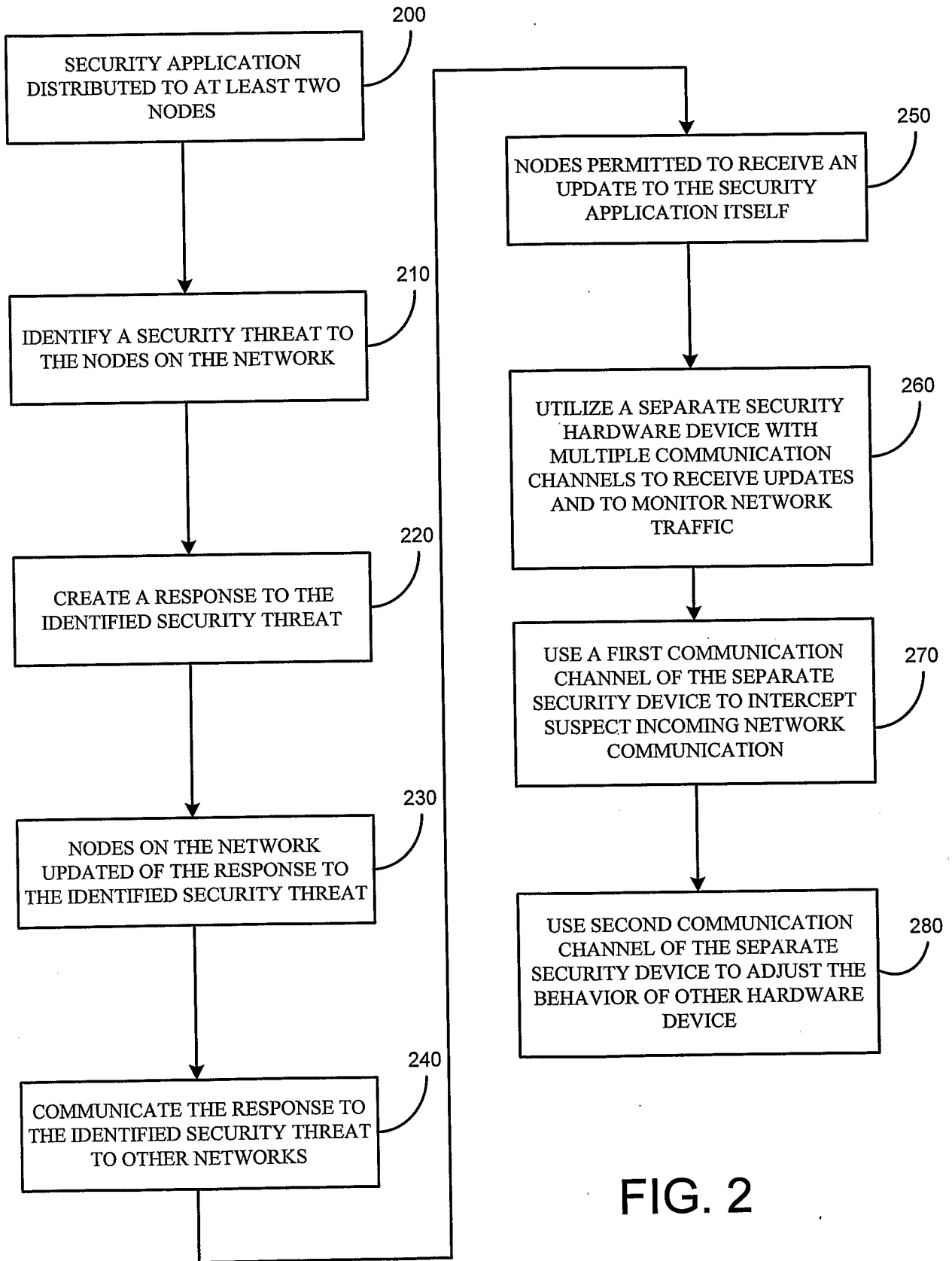


FIG. 2

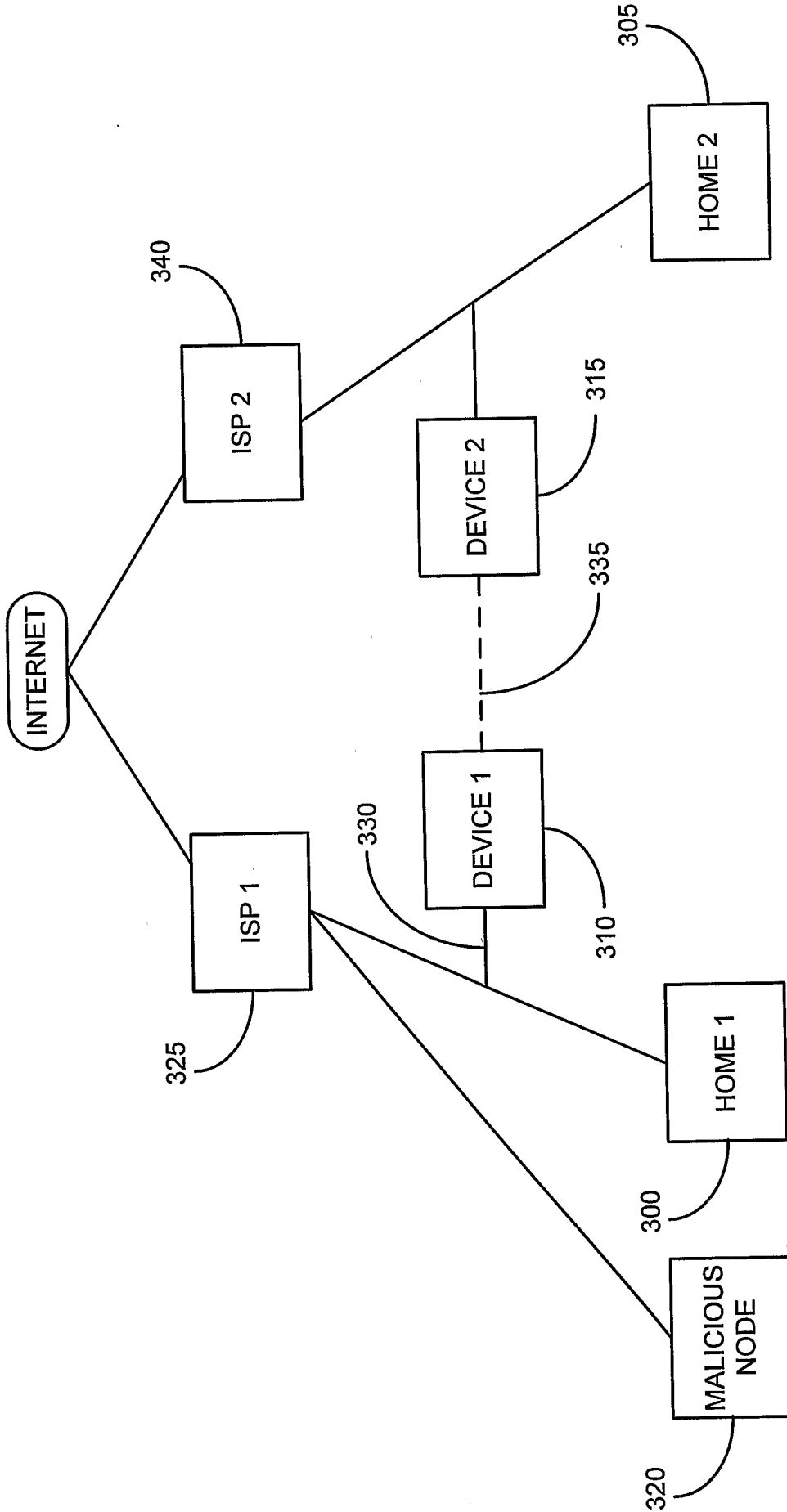


FIG. 3

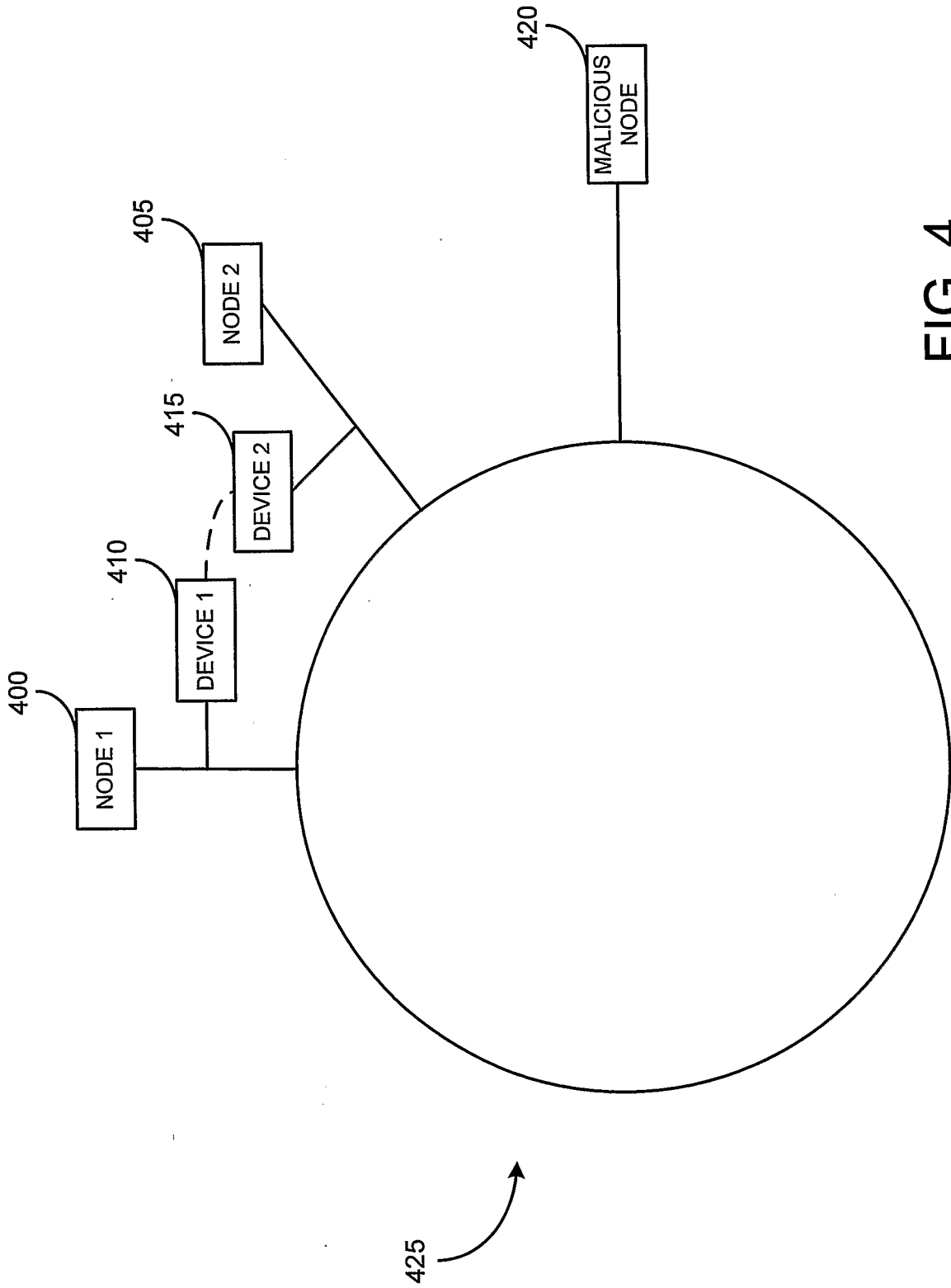


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2006/034580**A. CLASSIFICATION OF SUBJECT MATTER****H04L 12/22(2006.01)i, G06F 21/20(2006.01)i**

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)

IPC8: G06F 15/00, 15/173, 11/30; H04L 9/00, 9/32, 29/06, 12/56.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Patents and applications for inventions since 1975Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, eKIPASS(KIPO internal)**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2004-0065674 A (KWON, CHANG HOON.) 23 July 2004 See abstract; fig. 1; claims 1, 2, 5, 11-15.	1, 3, 5, 6, 8, 11, 12, 13, 14, 16-20
X	WO03032571 A1 (MOTOROLA CO., LTD.) 17 April 2003 See page 3 line 16 - page 4 line 2, page 4 line 27 - page 5 line 2.	2, 4
X	KR 10-2005-0026624 A (LEE, SANG JOON.) 15 March 2005 See abstract; figs. 8, 9, 26, 27; claims 19, 26-31.	1, 3, 5, 6, 8, 11, 13, 14, 16-20
X	US 2003-0200464 A1 (YARON KIDRON) 23 October 2003 See abstract; claims 1, 4.	5, 6, 11, 13, 14, 16
X	US 2004-0093513 A1 (CRAIG CANTRELL. et al.) 13 May 2004 See abstract; claims 2, 4, 6, 8, 9, 11, 13, 64, 68.	5, 11, 13, 16

 Further documents are listed in the continuation of Box C. See patent family 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 application or patent 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 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

14 FEBRUARY 2007 (14.02.2007)

Date of mailing of the international search report

14 FEBRUARY 2007 (14.02.2007)

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer

YANG, CHAN HO

Telephone No. 82-42-481-5689



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2006/034580

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR2004065674 A	23.07.2004	None	
W003032571 A1	17.04.2003	CN1685657A FI20040514A0 JP17506736 KR1020040045815 US20030074582A1	19.10.2005 07.04.2004 03.03.2005 02.06.2004 17.04.2003
KR2005026624 A	15.03.2005	None	
US2003200464 A1	23.10.2003	AU2003223656A1 BR200309288A CA2480475A1 CN1647483A EP01495616A1 IL164609A0 JP17523539 KR1020040101490 US2003200464A1 W003090426A1	03.11.2003 09.02.2005 30.10.2003 27.07.2005 12.01.2005 18.12.2005 04.08.2005 02.12.2004 23.10.2003 30.10.2003
US2004093513 A1	13.05.2004	AU2003290674A1 CN1720459A EP01558937A2 JP18506853 KR1020050086441 US20040093513A1 US2005028013A1 US2005044422A1 W02004045126A2	03.06.2004 11.01.2006 03.08.2005 23.02.2006 30.08.2005 13.05.2004 03.02.2005 24.02.2005 27.05.2004