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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/100613 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/IB2006/050554

(22) International Filing Date:
21 February 2006 (21.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05006462.5 24 March 2005 (24.03.2005) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [—/US]; New Orchard Road, Armonk, New York 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RIORDAN, James, F.** [US/CH]; Alte Landstrasse 50, CH-8803 Rüschlikon (CH). **ZAMBONI, Diego, M.** [MX/CH]; Etzelstrasse 33, CH-8820 Wädenswil (CH). **DUPONCHEL, Yann** [FR/CH]; Feldblumenstrasse 18, CH-8134 Adliswil (CH). **RISSMANN, Rüdiger** [DE/CH]; Kronenstrasse 3, CH-8134 Adliswil (CH).

(74) Agents: **KLETT, Peter, M.** et al.; Säumerstrasse 4 / Postfach, CH-8803 Rüschlikon (CH).

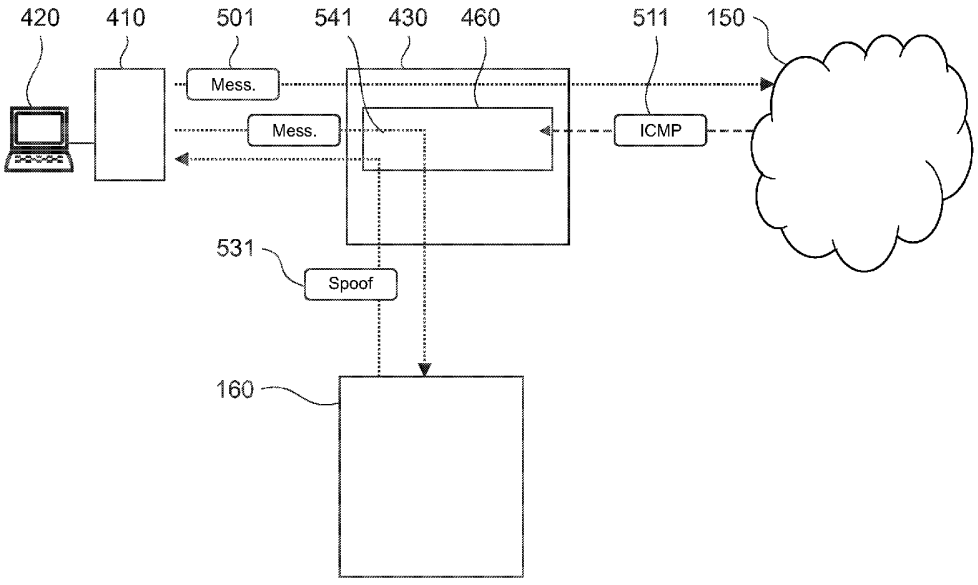
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, 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, LV, 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*

[Continued on next page]

(54) **Title:** NETWORK ATTACK DETECTION



(57) **Abstract:** A method and apparatus are provided for detecting attacks on a data communication network. The apparatus includes a router with a mechanism for monitoring return messages addressed to an originating user system local to the router. The mechanism includes a message checker for identifying a return message of a specified nature and a rerouter for temporarily routing subsequent messages from the originating user system to the intrusion detection sensor.

WO 2006/100613 A1

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

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.

NETWORK ATTACK DETECTION

This invention relates to the field of detecting network attacks and particularly relates to detecting attacks on a data communication network locally to the attack originating user system.

The Internet is a wide area data communication network formed from a plurality of interconnected data networks. In operation, the Internet facilitates data communication between a range of remotely situated data processing systems. Typically, end user data processing systems connected to the Internet are referred to as client data processing systems or simply clients. Similarly, data processing systems hosting web sites and services for access by end users via the Internet are referred to as server data processing systems or simply servers. There is a client-server relationship completed via the Internet between the end user data processing systems and the hosting data processing systems.

The Internet has become an important communication network for facilitating electronically effected commercial interactions between consumers, retailers, and service providers. Access to the Internet is typically provided to such entities via an Internet Service Provider (ISP). Each ISP typically operates an open network to which clients subscribe. Each client is provided with a unique Internet Protocol (IP) address on the network. Similarly, each server on the network is provided with a unique IP address. The network operated by the ISP is connected to the Internet via a dedicated data processing system usually referred to as a router. In operation, the router directs inbound communication traffic from the Internet to specified IP addresses on the network. Similarly, the router directs outbound communication traffic from the network in the direction of specified IP addresses on the Internet.

A problem faced by many people and businesses is the increasing frequency of electronic attacks to the networks they use. Such attacks include computer virus attacks and so-called "worm" attacks. Attacks of this nature introduce significant performance degradation in networks. Infected systems connected to the network typically attempt to spread the infection within the network. Many users do not recognize that their systems are infected.

A known intrusion detection sensor spoofs service interaction with potential attackers. The sensor functions by spoofing the existence of machines and services at otherwise unused IP addresses. As the addresses are otherwise unused, all traffic destined to them is *a priori* suspicious. The sensor spoofs services to determine the intention behind the traffic. The sensor itself offers a virtualization infrastructure that allows individual sensors to be written as if they were running on a single host.

WO 2004/107706 discloses an intrusion detection sensor (IDS) for detecting attacks on a data communication network. The IDS identifies data traffic on the network originating at any assigned address and addressed to any unassigned address, inspects the data traffic so identified for data indicative of an attack and generates an alert signal, if required.

The term "unassigned" is used in this context as covering an address that is not assigned to a physical device other than an apparatus for detecting an intrusion or generating an attack signature. The apparatus that is designed to execute the method disclosed in WO 2004/107706 is the device those "unassigned" addresses are actually assigned to in order to make use of the method. Those addresses are insofar unassigned as they are not assigned to any device that does have another functionality apart from signature generation or intrusion detection.

In the above mentioned IDS, a block of unassigned addresses is designated to the IDS such that the IDS can spoof a response to any data traffic to these unassigned addresses. Also, the IDS may be geographically remote from the originating user system of the data traffic making it difficult to take action against the originating user system.

It is an aim of the present invention to provide a system for detecting attacks to unused or inaccessible addresses. It is a further aim to provide local reporting of local problems. In addition the detection can be realized transparent to the attacking entity.

According to a first aspect of the present invention there is provided a method for detecting attacks on a data communication network, the method comprising: monitoring return messages addressed to an originating user system; identifying a return message of a specified nature; and temporarily routing subsequent messages from the originating user system to an intrusion detection sensor. The term specified nature is understood as the

message having a specific property or being of a predetermined type. The monitoring means also referred to as message checker works as a filter that checks if the return message has the specific property. If the return message is recognized to have the property the message checker is looking for, the return message is subjected to rerouting. The message checker can hence be seen as a return message type operated switch. The message checker can at the same time check for different specific properties, and perform the rerouting if one or more of those properties are found to be present.

Preferably, the intrusion detection sensor is local to the originating user system, i.e. the intrusion detection sensor is connected to the same network as the originating system. The term network is herein understood as an aggregation of networkable units, the border of the network being represented by border routers or edge routers. Those routers handle the connectivity to other networks. A network can be a subnetwork to a larger network. The intrusion detection sensor may spoof an exchange with the originating user system. In this way, an intrusion detection sensor local to an originating user system of a message sent to an inaccessible address can determine the nature of the originating user system's intent. In other words, the invention allows a detection and reporting of an attack closer to the attacking entity.

The return message may relate to a message sent by the originating user system to a destination address and the step of temporarily routing may reroute to the intrusion detection sensor all subsequent messages that are directed from the originating user system to the destination address.

The specified nature of the return message may indicate that a destination address is inaccessible. For example, the specified nature of the return message may be an Internet Control Message Protocol message indicating a failed connection.

The temporarily routing may be applied for a predetermined period of time, after which normal routing is resumed. The method may also include triggering the temporarily routing if the number of return messages of a specified nature that have been identified as addressed to an originating user system, exceeds a predetermined threshold. This threshold would then be usable to differentiate between harmless traffic and harmful traffic such as spam.

According to a second aspect of the present invention there is provided an apparatus for detecting attacks on a data communication network, the apparatus comprising: a router including a mechanism for monitoring return messages addressed to an originating user system local to the router; and an intrusion detection sensor; wherein the mechanism including: a message tracker for identifying a return message of a specified nature: and means for temporarily routing subsequent messages from the originating user system to the intrusion detection sensor.

Preferably, the intrusion detection sensor is local to the router. The intrusion detection sensor may include means for spoofing an exchange with the originating user system. The intrusion detection sensor may include a virtualization infrastructure with a plurality of virtual sensors each spoofing a service.

According to a third aspect of the present invention there is provided a router comprising: a mechanism for monitoring return messages addressed to an originating user system local to the router; means for identifying a return message of a specified nature: and means for temporarily routing subsequent messages from the originating user system to an intrusion detection sensor.

According to a fourth aspect of the present invention there is provided a data communication system comprising: a plurality of data processing systems in a network; a router local to the data processing systems for routing messages to and from the data processing systems; the router including a mechanism for monitoring return messages addressed to an originating user system in the form of one of the data processing systems local to the router; and an intrusion detection sensor; wherein the mechanism includes: means for identifying a return message of a specified nature: and means for temporarily routing subsequent messages from the originating user system to the intrusion detection sensor.

According to a fifth aspect of the present invention there is provided a computer program element comprising computer program code means which, when loaded in a processor of a data processing system, configures the processor to perform a method comprising the steps of: monitoring return messages addressed to an originating user system; identifying a

return message of a specified nature; and temporarily routing subsequent messages from the originating user system to an intrusion detection sensor.

When a process from an originating user system tries to contact an unused or inaccessible address (for example, behind a firewall), an ICMP (Internet Control Message Protocol) message is returned to the router local to the originating user system telling the originating user system that the destination is not reachable along with some details as to why. This message is intercepted by the router local to the originating user system and all traffic from the originating user system is temporarily routed through the IDS.

Embodiments of the present invention will now be described, by way of examples only, with reference to the accompanying drawings in which:

Figure 1 is a block diagram of a data processing system as known in the prior art;

Figure 2 is a block diagram of a data processing network showing an embodiment of a known intrusion detection sensor;

Figure 3 is a block diagram of known intrusion detection sensor;

Figure 4 is a block diagram of a data processing network in accordance with the present invention;

Figure 5 is a detail of the data processing network of Figure 4 showing re-routing of messages in accordance with the present invention; and

Figure 6 is a flow diagram of the method or re-routing in accordance with the present invention.

Referring first to Figure 1, a data processing system comprises a central processing unit (CPU) 10, an input/output (I/O) subsystem 20, and a memory subsystem 40, all interconnected by a bus subsystem 30. The memory subsystem 40 may comprise random access memory (RAM), read only memory (ROM), and one or more data storage devices such as hard disk drives, optical disk drives, and the like. The I/O subsystem 20 may

comprise: a display; a printer; a keyboard; a pointing device such as a mouse, trackball, or the like; and one or more network connections permitting communication between the data processing system and one or more similar systems and/or peripheral devices via a data communication network. The combination of such systems and devices interconnected by such a network may itself form a distributed data processing system. Such distributed systems may be themselves interconnected by additional data communication networks.

In the memory subsystem 40 is stored data 60 and computer program code 50 executable by the CPU 10. The program code 50 includes operating system software 90 and application software 80. The operating system software 90, when executed by the CPU 10, provides a platform on which the application software 80 can be executed.

Referring now to Figure 2, an example extract of an Internet architecture is shown with an embodiment of an intrusion detection sensor (IDS). In the example architecture two data communication networks 100, 200 are shown. It will be appreciated that this is an example architecture and many different forms of data communication networks may be provided.

Figure 2 shows a first data communication network 100 with a plurality of addresses 110 for assignment to data processing systems 120 in the first network 100 and a second data communication network 200 having a plurality of addresses 210 for assignment to data processing systems 220 in the second network 200. The networks 100, 200 may be in the form of Internet service installations having a plurality of assignable Internet Protocol (IP) addresses 110, 210. The networks 100, 200 are each connected to the Internet 150 via a router 130, 230.

The routers 130, 230 may be implemented in the form of a data processing system as herein before described with reference to Figure 1 dedicated by appropriate programming to the task to route communication traffic in the form of data packets between the Internet 150 and the network 100, 200 to which the router 130, 230 is connected based on IP address data specified in the data packets.

In the first data communication network 100, there are IP addresses 110 assigned to systems 120 belonging to users of the Internet service. Each system 120 may be a data processing system as herein before described with reference to Figure 1. A second group

140 of the IP addresses on the network 100 are free. More specifically, the second group 140 of IP addresses are not assigned to user systems. An intrusion detection sensor (IDS) 160 is connected to the network 100. The IDS 160 is also connected to the router 130.

A process 240, such as a worm or other attack, may originate from a user system 220 on the second data communication network 200. The process 240 may be addressed to a wide selection of addresses on other networks 100. If the process 240 is addressed to an unassigned address such as one of the second group 140 of IP addresses on the first network 100 which are unassigned to user systems, the process 240 is routed to the IDS 160 which spoofs replies to the process 240 and raises an alarm.

An example internal architecture of an IDS 160 is shown in more detail in Figure 3. Other forms of IDS are known and may be used in the present invention. The IDS 160 operates by spoofing the existence of machines and services at otherwise unused IP addresses. Because the IP addresses are otherwise unused, all traffic destined to these addresses is *a priori* suspicious. The IDS 160 spoofs services, rather than merely recording attempted connections, to determine the intention behind the traffic.

The IDS 160 is built on top of a security-hardened machine that offers no real services beyond restricted login. The IDS 160 offers a virtualization infrastructure 310 that allows individual sensors 311-315 to be operated as if they were running on a single host. It also provides a logging infrastructure 320 based on a relational database 330 that allows correlation and analysis of the copious data produced by the number of virtual sensors 311-315. The services offered by the virtual sensors 311-315 may include Hypertext Transfer Protocol (HTTP), Microsoft's Distributed Component Object Model, Structured Query Language, and Windows file sharing and printing (SMB).

With reference to Figure 4, in an example embodiment of the present invention, there is provided a first data communication network 400 with a user system 420 with an IP address 410 from which originates a process 440 such as a malicious worm process. The process 440 may be addressed to a range of IP addresses 510 of user systems 520 across other networks, for example the second network 500 shown in Figure 4.

The process 440 may be addressed to IP addresses 540 which are unused or inaccessible, for example, behind a firewall. If this is the case, an ICMP (Internet Control Message Protocol) message is returned from the router 530 local to the inaccessible address which in this example is the router 530 of the second network 500. The ICMP message is addressed to the originating user system 420 of the process 440 indicating that the destination is not reachable, together with some details as to why.

A mechanism is provided to capture the ICMP message at the router 430 local to the originating user system 420. The ICMP message tells the router 430 local to the originating user system 420 that all traffic from the originating user system 420 to the destination should be given to or routed through a local intrusion detection sensor (IDS) 160. The local IDS 160 can then interact with the originating user system 420 to determine the root cause of the attempted connection.

Each network 400, 500 has its router 430, 530 which manages the traffic across the Internet 150. The routers open the IP packets of data to read the destination address, calculate the best route, and then send the packet toward its final destination. If the destination is on the same network as the sending computer, the router sends the packet directly to the destination computer. If the packet is going to a destination outside the local network, the router instead sends the packet to another router closer to the destination. That router in turn sends the packet to a closer router until the packet reaches its final destination.

The routers 430, 530 have two or more physical ports: input ports and output ports. When an input port receives a packet, a software routine called a routing process is run. This process looks inside the header information in the IP packet and finds the address to which the data is being sent. It then compares this address against an internal database, called a routing table, which has detailed information about the ports to which packets with various IP addresses should be sent. Based on what it finds in the router table, the router sends the packet to a specific output port which sends the data to the next router or to the destination itself.

The operation of the Internet is monitored by the routers and when a connection cannot be completed, the event is reported by the ICMP (Internet Control Message Protocol). Various different types of ICMP messages are defined and each message type is encapsulated in an IP packet. For example, a "Destination Unreachable" message is used when the subnet or a router cannot locate the host destination, and a "Network Unreachable" message is used when the network of the destination cannot be located.

Referring to Figure 5, in an example embodiment of the present invention, a rerouting mechanism 460, also referred to as rerouter, in the router 430 identifies the nature of messages being returned to the IP addresses 410 local to the router 430. An originating user system 420 with an originating IP address 410 sends a message 501 to a destination address. If a return message 511 is identified by the mechanism 460 as being an ICMP message indicating an unreachable destination, the mechanism 460 sets up a temporary route 541 to direct traffic addressed to the unreachable destination from the originating IP address 410 to an IDS 160 local to the router 430. The mechanism 460 can herefor comprise a message checker that is able to analyze the nature of the intercepted return message 511 and identify those that are of a specified nature. This identification works like a filter that does not affect the return messages that are not of the specified nature. The other messages 511 are re-routed by a rerouter to the IDS 160. The rerouter need not be a separate hardware device. It can be a functionality of the router 430 that reroutes the return messages 511 in accordance with a policy. The router 430 can run one or more policies to determine the nature of redirection and re-routing. For example, the redirection may only take place if the number of return messages 511 of the monitored type exceeds a predetermined threshold. The temporary route 541 may be timed to last for a predetermined period of time, for example 30 seconds.

In response to the message 501 an ICMP message 511 is returned by a remote router in the Internet 150 to the router 430 local to the originating user system 420. The mechanism 460 intercepts the ICMP message 511. Since the return message 511 is identified to be of a specified nature, namely here indicating an unreachable destination, the mechanism 460 will perform a rerouting so that all traffic from the originating user system 420 to the destination is given to or routed through the local IDS 160. The mechanism 460 sets up a temporary route 541 so that any subsequent messages sent from the originating IP address 410 to the inaccessible address are re-routed to the IDS 160. The IDS 160 can spoof an

exchange 531 with the originating user system 420 by pretending to be the inaccessible address. The IDS 160 can then determine the nature of the attempted contact by the originating user system 420 to the inaccessible address and, if the attempted contact is malicious an alarm can be raised locally within the same router network.

Figure 6 shows a flow diagram of the process 600 of the mechanism 460 at the router 430. The process 600 involves the mechanism 460 monitoring 610 return messages 511 addressed to an originating user system, identifying 620 a return message 511 of a specified nature and temporarily routing 630 subsequent messages from the originating user system 420 to the intrusion detection sensor 160. The IDS 160 can be a sensor as described herein before, spoofing replies to the originating user system 420.

In addition to all the advantages of a conventional IDS, this mechanism more precisely delivers alarms more locally hence reducing the need for a redistribution architecture. This directly addresses the problem of efficiently detecting infected machines in the local network, which is valuable information for the local network administrators, instead of detecting remote infected systems, about which the local network administrator can do nothing. So the invention allows a detection of an intrusion closer to the intruder, thereby allowing a network administrator who is in charge of the domain that includes the intruder to react to the intrusion by an appropriate action. The closer the intrusion detection is located to the intruder the better the administrator is able to perform such action.

Another advantage is that every unused or inaccessible address in existence across different networks will result in a returned ICMP message 511. Therefore, unused addresses do not need to be assigned to an IDS. The mechanism relies on the returned ICMP messages 511 indicating that the destination address is inaccessible.

The present invention is typically implemented as a computer program product, comprising a set of program instructions for controlling a computer or similar device. These instructions can be supplied preloaded into a system or recorded on a storage medium such as a CD-ROM, or made available for downloading over a network such as the Internet or a mobile telephone network.

The invention can also be realized by a servicing entity offering a service to a serviced entity, also referred to as client system. This service can be one or more of the following: Installation of the device or system according to the invention in or for an environment of the serviced entity, deployment of the infrastructure usable to perform thereon, in particular deployment or integration of computing infrastructure, comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of performing the method according to the invention. In the context of this invention, the servicing entity can equip a client system against intrusion from an originating user system. Thereby the servicing entity can either provide efficient detection of infected machines in the serviced entity's network or detect infected machines that attack the serviced entitie's network. The equipment method can comprise the steps of: connecting an intrusion detection sensor 160 to a router 430, providing the router 430 with a capability to monitor 610 return messages 511 addressed to an originating user system 420, identify 620 a return message 511 of a specified nature, and temporarily route 630 subsequent messages from the same originating user system 420 to said intrusion detection sensor 160. The IDS 160 can be equipment owned or leased by the servicing entity. In particular, the servicing entity could use this IDS 160 for several serviced entities at the same time, hence sharing this resource. This has the advantage that an update performed on the IDS 160 with respect to intrusion detectability performance, has its impact on all connected serviced entities. Another advantage is that this service can be realized transparent to the serviced entity.

Improvements and modifications can be made to the foregoing without departing from the scope of the present invention.

CLAIMS

1. A method for detecting attacks on a data communication network, the method comprising:

monitoring (610) return messages (511) addressed to an originating user system (420);

identifying (620) a return message (511) of a specified nature; and

temporarily routing (630) subsequent messages from the same originating user system (420) to an intrusion detection sensor (160).

2. A method as claimed in claim 1, wherein the intrusion detection sensor (160) is selected to be arranged local to the originating user system (420).

3. A method as claimed in claim 1 or claim 2, further comprising the intrusion detection sensor (160) spoofing an exchange with the originating user system (420).

4. A method as claimed in any one of claims 1 to 3, wherein the return message (511) relates to a message (501) sent by the originating user system (420) to a destination address and the step of temporarily routing (630) is applied to all subsequent messages from the originating user system (420) to the destination address.

5. A method as claimed in any one of the preceding claims, wherein the specified nature of the return message (511) is selected to indicate that a destination address is inaccessible.

6. A method as claimed in any one of the preceding claims, wherein the specified nature of the return message (511) is selected to comprise an Internet Control Message Protocol message indicating a failed connection.

7. A method as claimed in any one of the preceding claims, wherein the temporarily routing (630) is applied for a predetermined period of time.

8. A method as claimed in any one of the preceding claims, further comprising triggering the temporarily routing (630) if a number of return messages (511) of a specified nature have been identified as being addressed to an originating user system (420), said number exceeding a predetermined threshold.

9. An apparatus for detecting attacks on a data communication network, the apparatus comprising:

a router (430) including a mechanism (460) for monitoring return messages (511) addressed to an originating user system (420) local to the router (430); and

an intrusion detection sensor (160);

wherein the mechanism (460) includes:

a message checker for identifying a return message (511) of a specified nature: and

a rerouter for temporarily routing subsequent messages from the originating user system (420) to the intrusion detection sensor (160).

10. An apparatus as claimed in claim 9, wherein the intrusion detection sensor (160) is local to the router (430).

11. An apparatus as claimed in claim 9 or claim 10, wherein the intrusion detection sensor (160) is designed to spoof an exchange with the originating user system (420).

12. An apparatus as claimed in claim 11, wherein the intrusion detection sensor (160) includes a virtualization infrastructure with a plurality of virtual sensors (310-315) each spoofing a service.

13. An apparatus as claimed in any one of claims 9 to 12, wherein the return message (511) relates to a message (500) sent by the originating user system (420) to a destination address and the rerouter is operative on all subsequent messages from the originating user system (420) to the destination address.

14. An apparatus as claimed in any one of claims 9 to 13, wherein the specified nature of the return message (511) indicates that a destination address is inaccessible.

15. An apparatus as claimed in any one of claims 9 to 14, wherein the specified nature of the return message (511) is an Internet Control Message Protocol message indicating a failed connection.

16. An apparatus as claimed in any one of claims 9 to 15, wherein the rerouter is active for a predetermined period of time.

17. An apparatus as claimed in any one of claims 9 to 16, wherein the rerouter includes a determinator for determining whether a number of return messages (510) of a specified nature that have been identified addressed to an originating user system (420) exceeds a predetermined threshold.

18. A router (430) comprising:
a mechanism (460) for monitoring return messages (511) addressed to an originating user system (420) local to the router (430);
a message checker for identifying a return message (511) of a specified nature: and
a rerouter for temporarily routing subsequent messages from the originating user system (420) to an intrusion detection sensor (160).

19. A data communication system comprising:
- a plurality of data processing systems in a network;
- a router (430) local to the data processing systems for routing messages to and from the data processing systems;
the router (430) including a mechanism (460) for monitoring return messages (511) addressed to an originating user system (420) in the form of one of the data processing systems local to the router (430);
- an intrusion detection sensor (160);
wherein the mechanism (460) includes:
a message checker for identifying a return message (510) of a specified nature: and
a rerouter for temporarily routing subsequent messages from the originating user system (420) to the intrusion detection sensor (160).

20. A computer program element comprising computer program code means which, when loaded in a processor of a data processing system, configures the processor to perform a method comprising the steps of:

monitoring (610) return messages (511) addressed to an originating user system (420);

identifying (620) a return message (510) of a specified nature; and

temporarily routing (630) subsequent messages from the originating user system (420) to an intrusion detection sensor (160).

21. A computer program element as claimed in claim 20, wherein the return message (511) relates to a message (501) sent by the originating user system (420) to a destination address and the step of temporarily routing is performed for all subsequent messages from the originating user system (420) to the destination address.

22. A computer program element as claimed in claim 20 or claim 21, wherein the specified nature of the return message (511) indicates that a destination address is inaccessible.

23. A computer program element as claimed in any one claims 20 to 22, wherein the specified nature of the return message (511) is an Internet Control Message Protocol message indicating a failed connection.

24. A computer program element as claimed in any one of claims 20 to 23, wherein the temporarily routing (630) is for a predetermined period of time.

25. A computer program element as claimed in any one of claims 20 to 24, wherein the method includes triggering the temporarily routing (630) if the number of return messages (511) of a specified nature that have been identified as addressed to an originating user system (420) exceeds a predetermined threshold.

26. A method of equipping a client system against intrusion from an originating user system (420) comprising the steps of:

connecting an intrusion detection sensor (160) to a router (430),

providing the router (430) with a capability to

- monitor (610) return messages (511) addressed to the originating user system (420),
- identify (620) a return message (511) of a specified nature, and
- temporarily route (630) subsequent messages from the same originating user system (420) to said intrusion detection sensor (160).

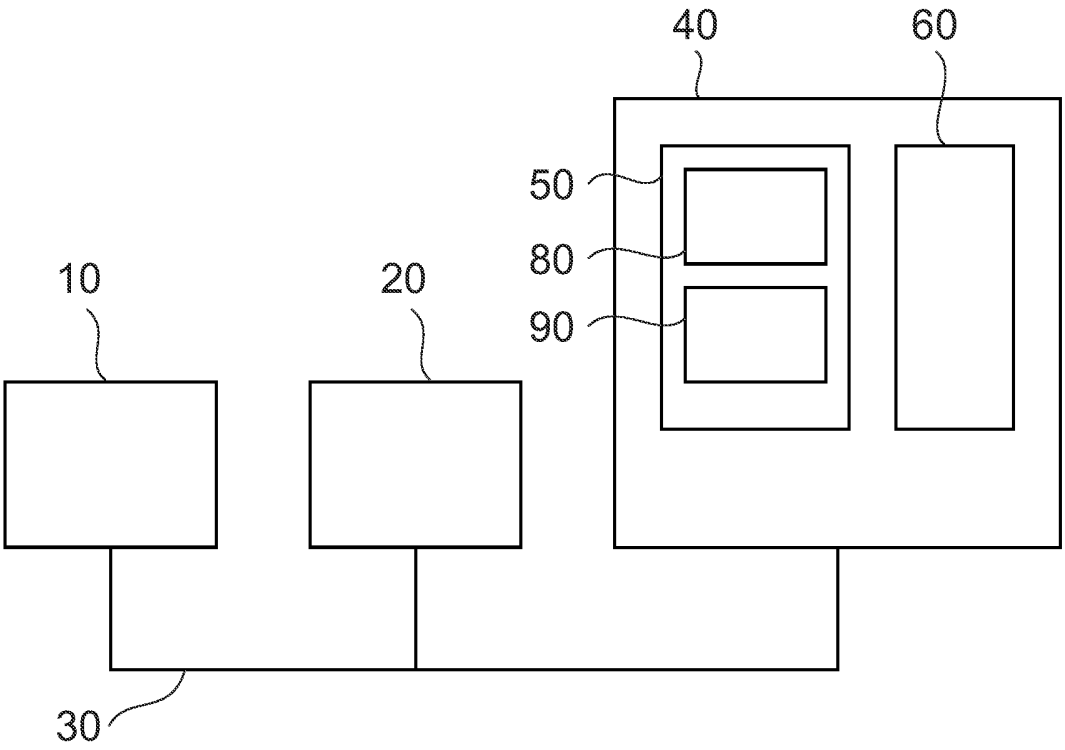


Fig. 1

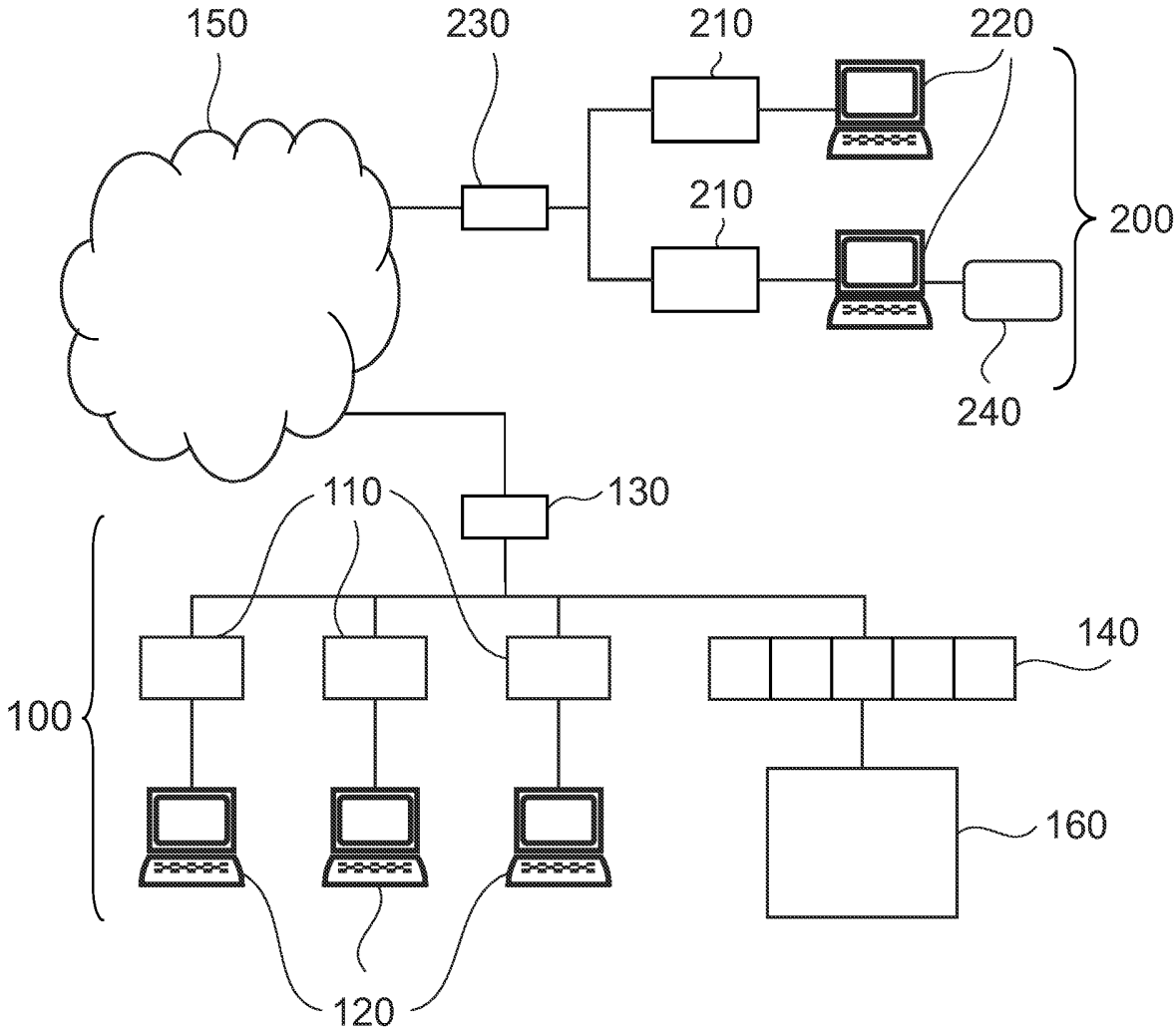


Fig. 2

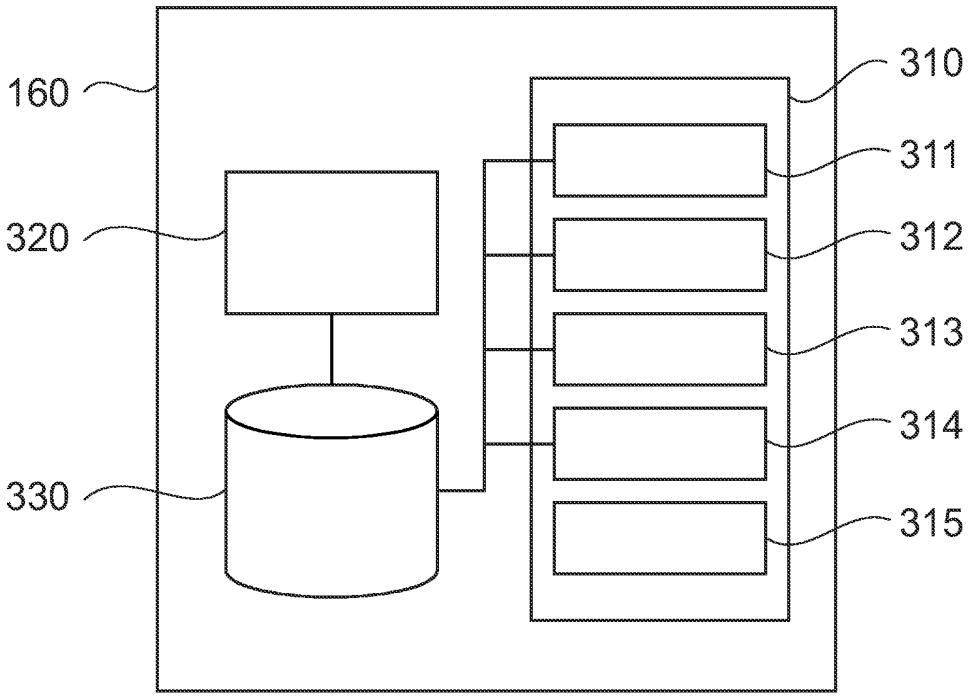


Fig. 3

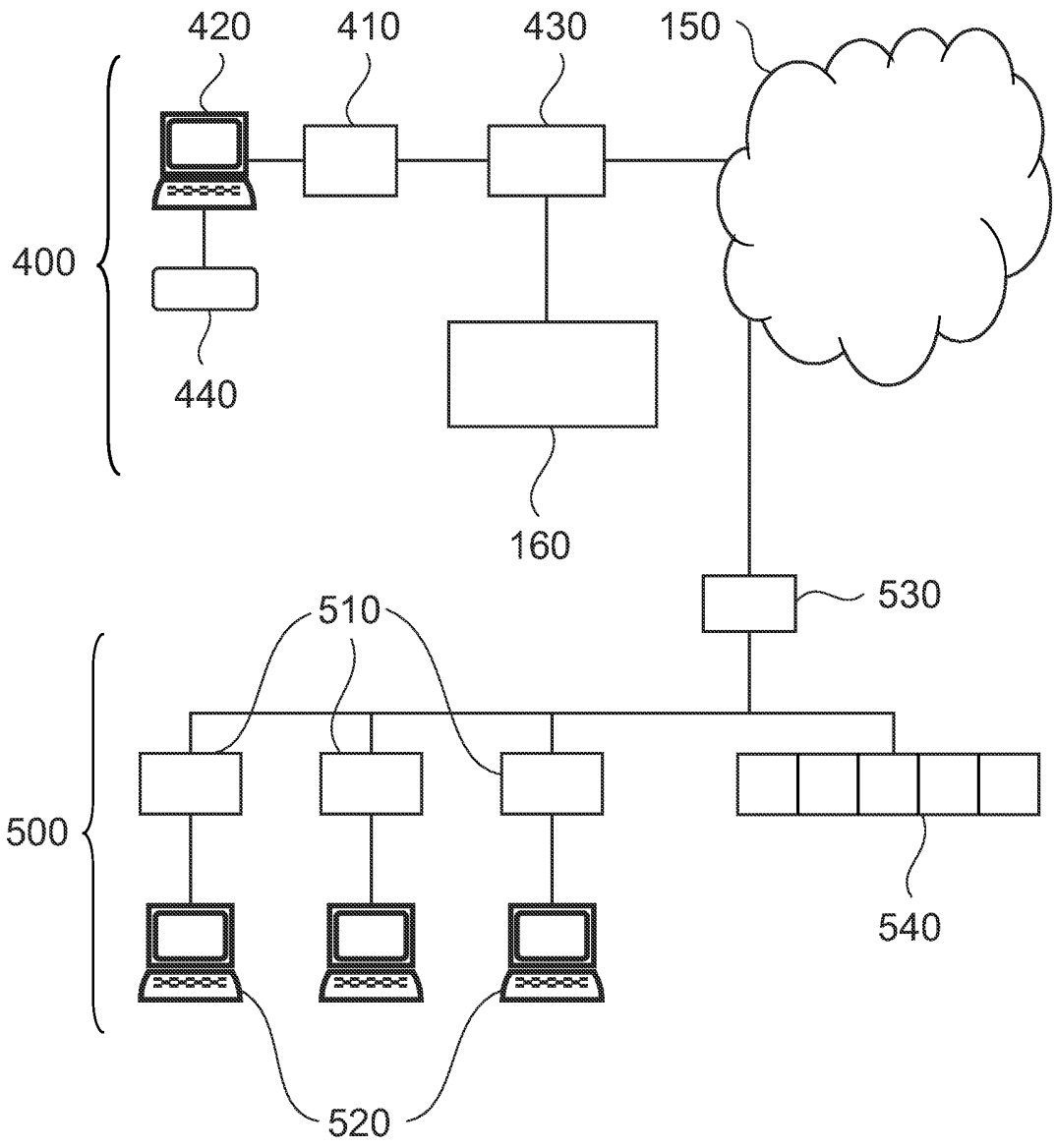


Fig. 4

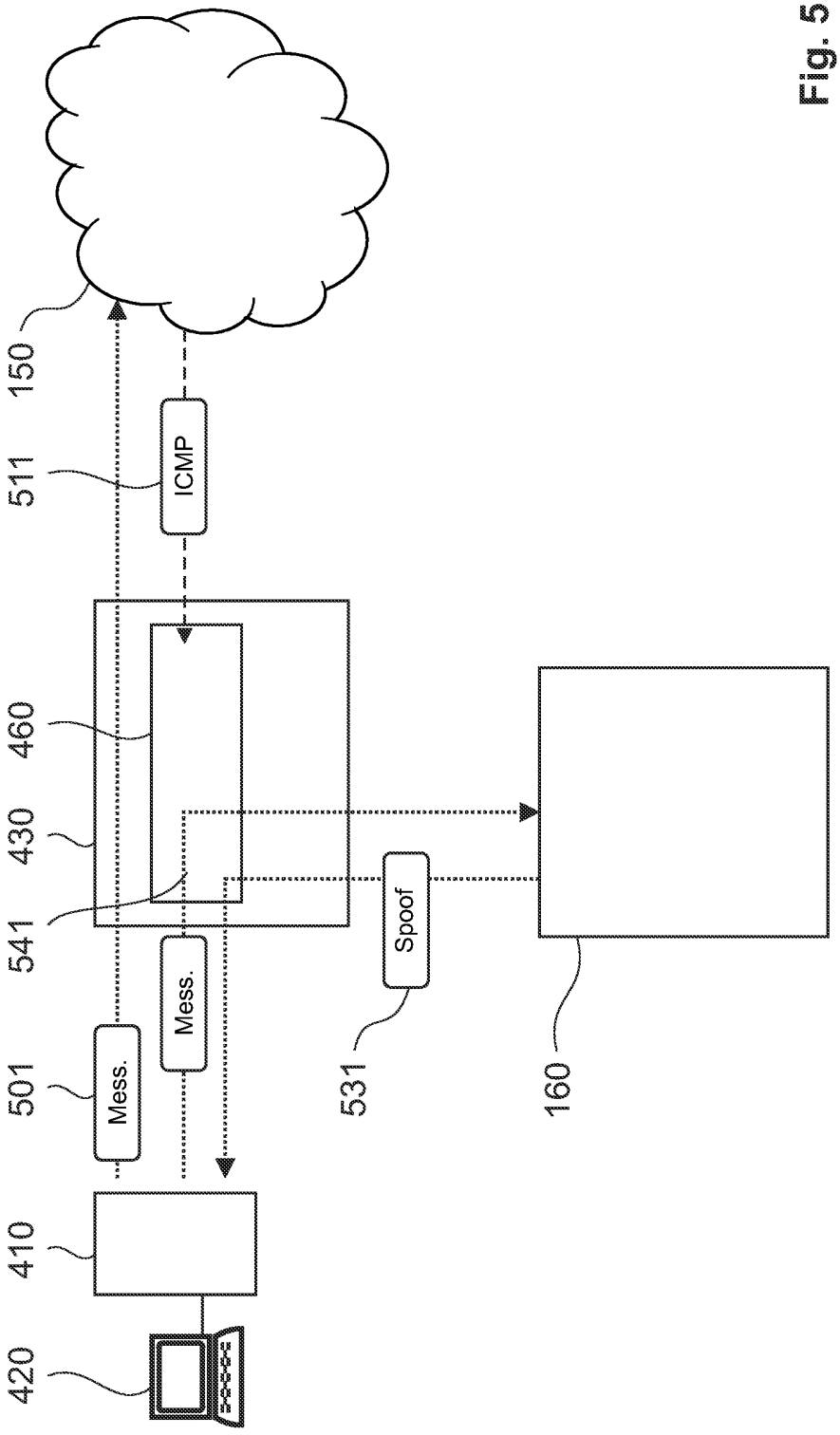


Fig. 5

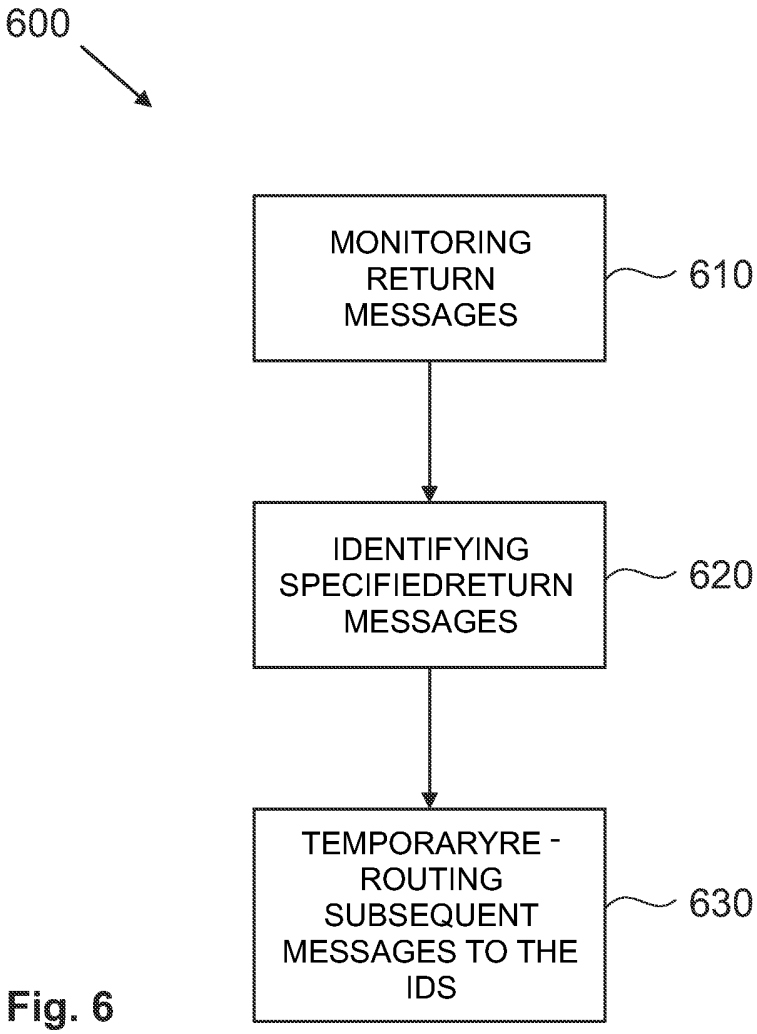

600
MONITORING RETURN MESSAGES
610
IDENTIFYING SPECIFIEDRETURN MESSAGES
620
TEMPORARYRE - ROUTING SUBSEQUENT MESSAGES TO THE IDS
630

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2006/050554

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 H04L29/06

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)
G06F 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 2005/015370 A (TELECOM ITALIA S.P.A; ABENI, PAOLO) 17 February 2005 (2005-02-17) page 7, line 21 - page 13, line 19 figures 1-5	1,2,4, 8-10,13, 17-20, 25,26
X	EP 1 330 095 A (STONESOFT CORPORATION) 23 July 2003 (2003-07-23) paragraph [0028] - paragraph [0042]; figure 2	1,9, 18-20,26
A	WO 2004/107706 A (INTERNATIONAL BUSINESS MACHINES CORPORATION; RIORDAN, JAMES, F) 9 December 2004 (2004-12-09) the whole document	1-26

☐ 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 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
7 August 2006	14/08/2006

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	Horn, M.P.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2006/050554

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005015370 A	17-02-2005	AU 2003279517 A1	25-02-2005
EP 1330095 A	23-07-2003	AT 322790 T	15-04-2006
		US 2003140140 A1	24-07-2003
WO 2004107706 A	09-12-2004	AU 2003280126 A1	21-01-2005
		AU 2003280190 A1	21-01-2005
		WO 2004107707 A1	09-12-2004