

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 September 2003 (04.09.2003)

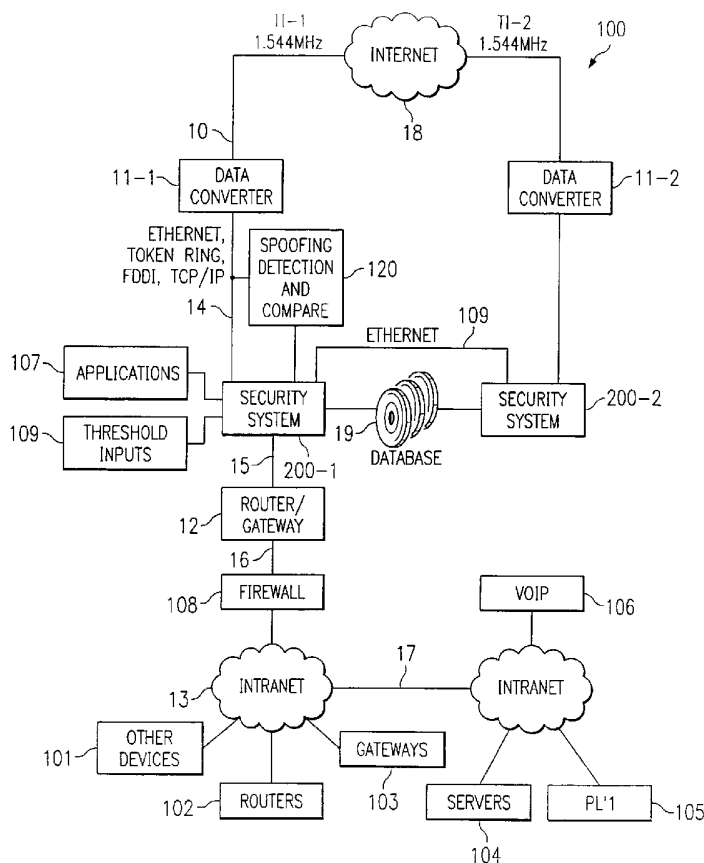
PCT

(10) International Publication Number
WO 03/073724 A3

- (51) International Patent Classification⁷: **H04L 29/06**, 12/56
- (74) Agents: **TANNENBAUM, David, H.** et al.; Fulbright & Jaworski, L.L.P., 2200 Ross Avenue, Suite 2800, Dallas, TX 75201-2784 (US).
- (21) International Application Number: PCT/US03/03623
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
- (22) International Filing Date: 7 February 2003 (07.02.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 10/078,386 20 February 2002 (20.02.2002) US
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant: **DEEP NINES, INC.** [US/US]; 14643 Dallas Parkway, Suite 150, Dallas, TX 75254 (US).
- (72) Inventors: **SHARP, Clifford, F.**; 2553 Via Merano, Del Mar, CA 92014 (US). **DARK, Susan, P.**; 14643 Dallas Parkway, Suite 150, Dallas, TX 75254 (US).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR DETECTING AND ELIMINATING IP SPOOFING IN A DATA TRANSMISSION NETWORK



(57) Abstract: A traffic management system sniffs data arriving at any point in a system. The sniffer operates to extract certain data from each address. This data could be, for example, the IP address data and the physical address data. The extracted data is then used to access different data bases to determine if matches occur. Time stamps, sequencing and other parameters of each piece of data entering a system are used to control data access.

WO 03/073724 A3



Published:

— *with international search report*

(88) Date of publication of the international search report:

18 December 2003

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.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/03623

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 H04L29/06 H04L12/56				
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, INSPEC, COMPENDEX				
C. DOCUMENTS CONSIDERED TO BE RELEVANT				
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
X	ISHIBASHI H ET AL: "A protection method against unauthorized access and address spooling for open network access systems" 2001 IEEE PACIFIC RIM CONFERENCE ON COMMUNICATIONS, COMPUTERS AND SIGNAL PROCESSING. VICTORIA, BC, CANADA, AUG. 26 - 28, 2001, IEEE PACIFIC RIM CONFERENCE ON COMMUNICATIONS, COMPUTERS AND SIGNAL PROCESSING. PACRIM, NEW YORK, NY: IEEE, US, vol. 1 OF 2. CONF. 8, 26 August 2001 (2001-08-26), pages 10-13, XP010560275 ISBN: 0-7803-7080-5	1-5,9-11		
Y	4 Implementation 4.1 Structure of the system 4.2 Detailed behaviour	6-8		
--- -/--				
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.				
<input checked="" type="checkbox"/> Patent family members are listed in annex.				
° Special categories of cited documents :				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none; vertical-align: top;"> <ul style="list-style-type: none"> *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 </td> <td style="width: 50%; border: none; vertical-align: top;"> <ul style="list-style-type: none"> *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 </td> </tr> </table>			<ul style="list-style-type: none"> *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 	<ul style="list-style-type: none"> *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
<ul style="list-style-type: none"> *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 	<ul style="list-style-type: none"> *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 <p style="text-align: center; font-size: 1.2em;">21 August 2003</p>		Date of mailing of the international search report <p style="text-align: center; font-size: 1.2em;">02.09.03</p>		
Name and mailing address of the ISA 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		Authorized officer <p style="text-align: center; font-size: 1.2em;">Bertolissi, E</p>		

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 03/03623

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>URUPOJ KANLAYASIRI, SURASAK SANGUANPONG AND YUEN: "Detecting Denial of Service using BENEF Model:" INTERNATIONAL WORKSHOP ON ASIA PACIFIC, 'Online! February 2001 (2001-02), XP002240231 Tokyo, Japan Retrieved from the Internet: <URL:http://anreg.cpe.ku.ac.th/pub/benef-ivs2001.pdf> 'retrieved on 2003-05-07! 2.2 Overall system 3 Feature Selector 4 Pre-Detector 5.1 Network Information ---</p>	1-5,9-11
X	<p>S. WHALEN: "An Introduction to ARP Spoofing" INTERNET PUBLICATION, 'Online! June 2001 (2001-06), XP002240206 Retrieved from the Internet: <URL:http://packetstormsecurity.nl/papers/protocols/intro_to_arp_spoofing.pdf> 'retrieved on 2003-05-06! Introduction Defenses ---</p>	1-5,9-11
Y	<p>DAEMON9 / ROUTE / INFINITY: "IP-spoofing Demystified " PHRACK MAGAZINE (ONLINE), VOLUME SEVEN, ISSUE FORTY-EIGHT, FILE 14 OF 18, 'Online! June 1996 (1996-06), XP002240268 Retrieved from the Internet: <URL:http://www.phrack.org/phrack/48/P48-14> 'retrieved on 2003-05-07! Sequence Numbers & Acknowledgements (and other flags) ---</p>	6-8
X	<p>JP 08 186569 A (TOSHIBA CORP) 16 July 1996 (1996-07-16) abstract paragraph '0001! - paragraph '0012! ---</p>	1-5
A	<p>DATAMATION: "Sleuth9" DATAMATION, 'Online! 25 January 2002 (2002-01-25), XP002240287 Retrieved from the Internet: <URL:http://products.datamation.com/security/security/1011891069.html> 'retrieved on 2003-05-07! the whole document ---</p>	1-11
L	<p>US 2002/131366 A1 (DARK SUSAN PITTMAN ET AL) 19 September 2002 (2002-09-19) the whole document ---</p>	12-25

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 03/03623

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 222 856 B1 (ALAM BILAL ET AL) 24 April 2001 (2001-04-24) abstract column 1, line 10 -column 3, line 36 column 4, line 14 -column 5, line 54 column 6, line 56 -column 7, line 67 ---	12-25
X	US 5 799 002 A (KRISHNAN MURALI R) 25 August 1998 (1998-08-25) abstract column 2, line 46 -column 3, line 36 column 4, line 34 -column 6, line 60 ---	12-25
X	WO 00 11841 A (COLEMAN TREVOR JOHN ;KNIGHT RICHARD JOHN (GB); MADGE NETWORKS LTD) 2 March 2000 (2000-03-02) abstract page 2, line 20 -page 3, line 21 page 4, line 27 -page 5, line 34 page 11, line 18 - line 29 -----	12-14,18

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 03/03623

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-11

A traffic management system and a data network monitoring system for determining spoofing

2. Claims: 12-25

A Method and a data flow control system for temporary storing certain packets upon attainment of a certain packet flow volume

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 03/03623

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 08186569 A	16-07-1996	NONE	
US 2002131366 A1	19-09-2002	WO 0210039 A2 US 2003110394 A1 AU 6137901 A EP 1282954 A2 WO 0189146 A2	12-12-2002 12-06-2003 26-11-2001 12-02-2003 22-11-2001
US 6222856 B1	24-04-2001	US 5799002 A US 6343085 B1	25-08-1998 29-01-2002
US 5799002 A	25-08-1998	US 6222856 B1	24-04-2001
WO 0011841 A	02-03-2000	EP 1106003 A1 WO 0011841 A1 WO 0011848 A1 WO 0011842 A1	13-06-2001 02-03-2000 02-03-2000 02-03-2000