(19) World Intellectual Property Organization International Bureau





(43) International Publication Date 21 March 2002 (21.03.2002)

PCT

(10) International Publication Number WO 02/023805 A3

(51) International Patent Classification7: 29/06

H04L 12/26.

(21) International Application Number: PCT/GB01/04107

(22) International Filing Date:

13 September 2001 (13.09.2001)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

0022485.7

13 September 2000 (13.09.2000) GB

(71) Applicant (for all designated States except US): KARAKORAM LIMITED [CY/CY]; 1C. Pantelides Avenue, 1010 Nicosia (CY),

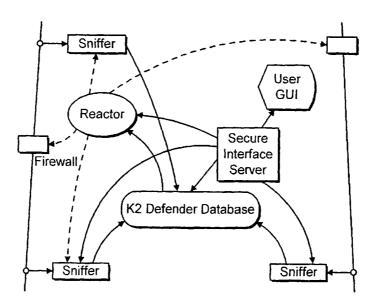
- (72) Inventors: and
- (75) Inventors/Applicants (for US only): TRIULZI, Arrigo,

Giangaleazzo, Bodo [IT/GB]; 23 Lurline Gardens, London SW11 4DB (GB). JOUBERT, Adriaan, Wolfgang [DE/CY]; 22 Andrea Kalvou Street, 2546 Ilioupolis Dali (CY).

- (74) Agents: BUTLER, Michael, John et al.; Frank B. Dehn & Co., 179 Queen Victoria Street, London EC4V 4EL (GB).
- (81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), 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, PH, PL, PT, RO, RU, SD, SE, SG,SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: MONITORING NETWORK ACTIVITY



(57) Abstract: A system for analysing network traffic, particularly to detect suspect packets and identify attacks or potential attacks. Data packets which meet defined criteria are detected and their details forwarded to a database server where the details are stored so as to be accessible for use in analysis in conjunction with the details of other detected packets. Packet detection uses a tap and a packet factory which creates a packet for analysis consisting of the received packet and a unique identifier. A series of adapters are used to apply functions to different parts of the packets, to detect those meeting the criteria.



02/023805 A3



patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (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

(88) Date of publication of the international search report: 18 July 2002

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

Ir ational Application No PCT/GB 01/04107

		PC1/6	aB 01/0410/		
A. CLASSI IPC 7	IFICATION OF SUBJECT MATTER H04L12/26 H04L29/06				
	o International Patent Classification (IPC) or to both national cl	assification and IPC			
	SEARCHED ocumentation searched (classification system followed by class	sification symbols)			
IPC 7	H04L	, .			
<u>.</u>					
Documenta	tion searched other than minimum documentation to the exten	t that such documents are included in the	e fields searched		
Clastropia	data base consulted during the international search (name of d	ata base and, where practical sparch to	rme ueod)		
	ternal, WPI Data, PAJ	ara base and, where practical, search te	ms useu)		
LIO III	ternar, wir baca, Tho				
C. DOCUM	ENTS CONSIDERED TO BE RELEVANT				
Category °	Citation of document, with indication, where appropriate, of	the relevant passages	Relevant to claim No.		
χ	WO 00 05852 A (RAYTHEON CO)		1,2,4,		
^	3 February 2000 (2000-02-03)		14,15,		
			17,19, 21,25,		
			27,34		
A			3,5-13, 16,18,		
			20,		
			22-24,		
	abstract		26,28-33		
	page 2, line 28 - line 31				
	page 3, line 3 - line 6 page 3, line 25 - line 32				
	page 7, line 1 - line 12				
	page 7, line 20 - line 36 page 8, line 12 - line 19				
	page 8, line 24 - line 34				
	page 11, line 8 - line 34	-/			
V Furti	her documents are listed in the continuation of box C.	γ Patent family members a	are listed in annex		
	ategories of cited documents :				
·	ent defining the general state of the art which is not	"T" later document published after or priority date and not in cor	iflict with the application but		
consid	dered to be of particular relevance document but published on or after the international	cited to understand the princi invention	, , ,		
filing d "L" docume	ent which may throw doubts on priority claim(s) or	cannot be considered novel of	"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		
citation	is cited to establish the publication date of another n or other special reason (as specified)		lve an inventive step when the		
other r			ne or more other such docu- ng obvious to a person skilled		
	ent published prior to the international filing date but nan the priority date claimed		'&' document member of the same patent family		
Date of the	actual completion of the international search	Date of mailing of the internal	tional search report		
2	May 2002	13/05/2002			
Name and n	mailing address of the ISA	Authorized officer	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) 340-2040, 1x: 31 631 epo 111, Fax: (+31-70) 340-3016	Lai, C	Lai, C		

2

INTERNATIONAL SEARCH REPORT

In itional Application No PCT/GB 01/04107

	ation) DOCUMENTS CONSIDERED TO BE RELEVANT Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Category °	Спанон от document, with indication, where appropriate, or the relevant passages	Figure 10 damino.
	page 12, line 18 - line 23 page 20, line 33 -page 21, line 19 claims 1-3,5,7,8,11,15,17	
X A	US 5 835 726 A (DOGON GIL ET AL) 10 November 1998 (1998–11–10)	1,2,25 3-24, 26-34
	abstract column 2, line 37 - line 61 column 3, line 64 -column 4, line 21 column 6, line 28 - line 54 column 9, line 18 - line 49 column 13, line 5 - line 29	
Χ	EP 0 910 197 A (LUCENT TECHNOLOGIES INC)	1,2,25
Α	21 April 1999 (1999-04-21)	3-24, 26-34
	abstract page 2, line 35 -page 3, line 7 page 5, line 55 -page 6, line 51 page 7, line 50 -page 8, line 10	

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

In tional Application No
PCT/GB 01/04107

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0005852	A	03-02-2000	AU BR EP NO WO	5080599 A 9912193 A 1097554 A1 20010338 A 0005852 A1	14-02-2000 25-09-2001 09-05-2001 05-03-2001 03-02-2000
US 5835726	A	10-11-1998	US AU CA EP WO JP NO CA DE DE EP JP	5606668 A 6135696 A 2197548 A1 0807347 A2 9700471 A2 10504168 T 970611 A 2138058 A1 69425038 D1 69425038 T2 0658837 A2 8044642 A	25-02-1997 15-01-1997 03-01-1997 19-11-1997 03-01-1997 14-04-1998 15-04-1997 16-06-1995 03-08-2000 08-03-2001 21-06-1995 16-02-1996
EP 0910197	Α	21-04-1999	US EP JP	6154775 A 0910197 A2 11167538 A	28-11-2000 21-04-1999 22-06-1999