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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010269 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB2003/003112

(22) International Filing Date: 17 July 2003 (17.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/202,517 23 July 2002 (23.07.2002) US

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MG only)*: **IBM UNITED KINGDOM LIMITED** [GB/GB]; PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventors: **ARNOLD, William, Carlisle**; 207 Hill Street, Mahopac, NY 10541 (US). **CHESS, David, Michael**; 1744 Lawrence Road, Mohegan Lake, NY 10547 (US). **MORAR, John, Frederick**; 53 Hillside View Road, Mahopac, NY 10541 (US). **SEGAL, Alla**; 48 Park Drive, Mount Kisco, NY 10549 (US). **WHALLEY, Ian, Nicholas**; 203 Charles Colman Boulevard, Pawling, NY 12564-1124 (US). **WHITE, Steve, Richard**; 225 East 57th Street, Apartment 19F, New York, NY 10016 (US).

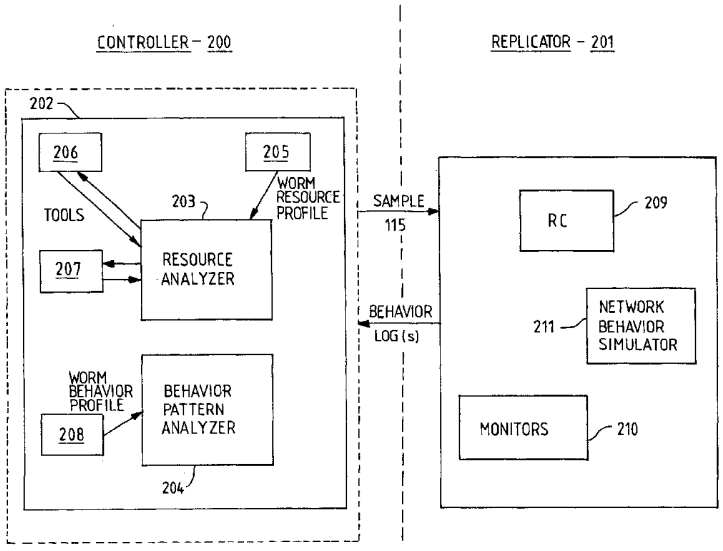
(74) Agent: **LING, Christopher, John**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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, NI, 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.

(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, RO,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR THE AUTOMATIC DETERMINATION OF POTENTIALLY WORM-LIKE BEHAVIOUR OF A PROGRAM



(57) Abstract: A method and system for the automatic determination of the behavioural profile of a program suspected of having worm-like characteristics includes analyzing data processing system resources required by the program and, if the required resources are not indicative of the program having worm-like characteristics, running the program in a controlled non-network environment while monitoring and logging accesses to system resources to determine the behaviour of the program in the non-network environment. A logged record of the observed behaviour is analyzed to determine if the behaviour is indicative of the program having worm-like characteristics. The non-network environment may simulate the appearance of a network to the program, without emulating the operation of the network.

WO 2004/010269 A3

SE, SI, SK, 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:
11 March 2004

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

Interna... ...pplication No
PCT/GB 03/03112

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

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 G06F

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, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 02 06928 A (VCIS INC) 24 January 2002 (2002-01-24) abstract page 1, line 26 page 4, line 5 - line 16 page 6, line 8 - line 15 ---	1,12,18, 19 2-4, 13-15
Y	MARK BURNETT: "Securing Microsoft Services" INTERNET CITATION, 'Online! 22 May 2002 (2002-05-22), XP002264375 Retrieved from the Internet: <URL:http://www.securityfocus.com/infocus/1581 > 'retrieved on 2003-12-09! page 1, paragraph 2 page 2, paragraph 13 page 3, paragraph 1 --- -/--	2-4, 13-15

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

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 December 2003	29/12/2003

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	Kerschbaumer, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/GB 03/03112

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 842 002 A (KLEMMER TIMOTHY J ET AL) 24 November 1998 (1998-11-24) figure 1 column 1, line 40 - line 47 column 4, line 21 - line 36 column 5, line 29 - line 32	1-19
A	US 6 192 512 B1 (CHESS DAVID M) 20 February 2001 (2001-02-20) figure 2 column 4, line 65 -column 5, line 16	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat Application No
PCT/GB 03/03112

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0206928 A	24-01-2002	AU 6982601 A	30-01-2002
		CA 2416066 A1	24-01-2002
		EP 1358526 A2	05-11-2003
		TW 518463 B	21-01-2003
		WO 0206928 A2	24-01-2002
US 5842002 A	24-11-1998	AT 183592 T	15-09-1999
		CA 2191205 A1	07-12-1995
		DE 69511556 D1	23-09-1999
		EP 0769170 A1	23-04-1997
		JP 10501354 T	03-02-1998
		WO 9533237 A1	07-12-1995
US 6192512 B1	20-02-2001	NONE	