(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).

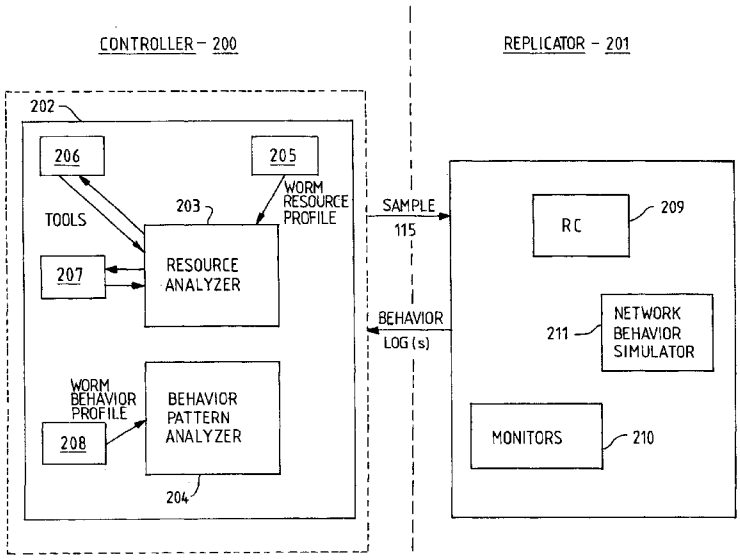
(74) Agent: **LING, Christopher, John**; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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.